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.2 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.
The second mapping table does the same type of mapping as the first table but it follows the chronological order of the policy. In some instances, there is no mapping between HUD's policy and NIST SP 800-53. In these cases, the table will map to newer regulations or to best practices.

2 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 Section Number	Control Name	NIST 800-53 Control #	ISO/IEC 17799	NIST 800-26	GAO FISCAM
Access Control					
5.2a					
5.4.3a	Access Control Policy and Procedures	AC-1	9.1.1		
			9.4.1		
			15		
			16.1.5a		
			5.1d		
			5.1e		
			5.2a		

5.2b
5.2eAccount ManagementAC-2
AC-2 (1)
AC-2 (3)
AC-2 (4)9.2.1
9.2.26.1.8
15.1.1
15.1.4
15.1.8
15.2.2
16.1.3
16.1.5
16.2.12AC-2.1
AC-2.2
AC-3.2
SP-4.1
4.6.5a
5.4.3aAccess and Information Flow ControlAC-3
AC-3 (1)9.2.4
9.4.6
9.4.815.1.1
16.1.1
16.1.2
16.1.3
16.1.7
16.1.9
16.2.7
16.2.10
16.2.11
16.2.15AC-2
AC-3.2
5.4.3bInformation Flow EnforcementAC-49.4.6
9.4.85.2c
4.1.3aSeparation of DutiesAC-58.1.46.1.1
6.1.2
6.1.3
15.2.1
16.1.2
17.1.5SD-1.2
3.1e
5.2cLeast PrivilegeAC-69.2.216.1.2
16.1.3
17.1.5AC-3.2
5.2.1a
5.2.1bUnsuccessful Logon AttemptsAC-79.5.215.1.14AC-3.2
5.2.3a
5.2.3b
5.2.3cSystem Use NotificationAC-89.5.216.2.13
17.1.9AC-3.2
Optional
ControlPrevious Logon NotificationAC-99.5.2AC-3.2
5.2.2bConcurrent Session ControlAC-104.6.1a
4.6.1bSession LockAC-1116.1.4AC-3.2
5.2.2aSession TerminationAC-129.5.716.1.4
16.2.6AC-3.2
5.3dSupervision and Review Access Control AC-13
AC-13 (1)9.2.47.1.10

11.2.2
16.1.10
17.1.6
17.1.7AC-4
AC-4.3
SS-2.2
5.2fPermitted Actions without Identification or AuthenticationAC-14
AC-14 (1)16.2.124.3bAutomated MarkingAC-155.2.28.2.4
16.1.6AC-3.2
Optional ControlAutomated LabelingAC-165.2.216.1.6AC-3.2
5.4.1a
5.4.1b
5.4.1c
5.4.1d
5.5.1cRemote AccessAC-17
AC-17 (1)
AC-17 (2)
AC-17 (3)9.4.3
9.4.416.2.12
16.2.4
16.2.8AC-3.2
4.5.1a
4.5.1b
4.5.1c
4.5.1d
5.5.1cWireless Access Restrictions
AC-18 (2Optional ControlAC-18
AC-18 (1)5.5.1d
5.4.3g
5.4.3hAccess Control for Portable and Mobile SystemsAC-19
AC-19 (1)9.5.1
9.8.17.3.1
7.3.24.6.4a
4.6.4b
4.6.4cPersonally-Owned Information SystemsAC-207.2.5
7.3.1
9.8.110.2.13Awareness and Training
4.1.4aSecurity Awareness and Training Policy and
ProceduresAT-1134.1.4cSecurity AwarenessAT-26.3.1
9.8.1
11.1.4
12.1.413.1.4
13.1.54.1.4b
4.1.4cSecurity TrainingAT-34.2.2
6.2.1
6.3.1
8.3.1
9.8.113.1
13.1.54.1.4e
4.1.4hSecurity Training Records AT-413.1.2Audit and Accountability
5.3aAudit and Accountability Policy and ProceduresAU-1175.3a
5.3c
5.3iAuditable Events
AU-2 (2Optional ControlAU-2
AU-2 (1)
AU-2 (2)11.1.217.1.1
17.1.2

17.1.45.3a
5.3iContent of Audit RecordsAU-3
AU-3 (1)
AU-3 (2)9.7.217.1.15.3eAudit Storage CapacityAU-49.7.25.3f
5.3gAudit ProcessingAU-5
AU-5 (1)9.7.25.3d
5.3iAudit Monitoring, Analysis, and Reporting
AU-6 (2Optional ControlAU-6
AU-6 (1)9.7.217.1.15.3hAudit Reduction and Report GenerationAU-7
AU-7 (1)17.1.2
17.1.75.3jTime StampsAU-89.7.35.3bProtection of Audit Information
AU-9 (1Optional ControlAU-912.3.217.1.3
17.1.4Optional ControlNon-repudiationAU-1010.3.415.1.2
17.1.15.3cAudit RetentionAU-1110.7.1
12.1.317.1.4Certification, Accreditation, and Security Assessments
3.10a
3.10b
3.10c
3.10dC&A and Security Assessment Policy and ProceduresCA-12
43.10fSecurity AssessmentCA-24.1.72.1.1
2.1.2
2.1.3
2.1.4SP-5.1
3.10hInformation System ConnectionsCA-31.1.1
3.2.9
4.1.2
4.1.8
12.2.3CC-2.1
3.10a
3.10bSecurity CertificationCA-43.2.3
3.2.5
4.1.1
4.1.6
11.2.8
12.2.5CC-2.1
3.10ePlan of Action and MilestonesCA-51.2.3
2.2.1
4.2.1SP-5.1 SP-5.2
3.10a
3.10b
3.10cSecurity AccreditationCA-64.1.1
4.1.7
4.1.8
12.2.53.10gContinuous MonitoringCA-79.7.2
12.2.110.2.1Configuration Management
3.8a
4.6.4b
4.6.5a
4.6.5e
4.6.5iConfiguration Management Policy and ProceduresCM-13.8aBaseline
ConfigurationCM-2
CM-2 (1)
CM-2 (2)1.1.1
10.1.4
10.2.7
10.2.8
10.2.9CC-2.3

CC-3.1
SS-1.2
3.8bConfiguration Change ControlCM-3
CM-3 (1)8.1.2
10.4.1
10.5.110.2.2
10.2.3
10.2.10
10.2.11SS-3.2
CC-2.2
3.8dMonitoring Configuration ChangesCM-48.1.210.2.1
10.2.4SS-3.1
SS-3.2
CC-2.1
3.8eAccess Restrictions for ChangeCM-5
CM-5 (1)6.1.3
6.1.4
10.1.1
10.1.4
10.1.5SD-1.1
SS-1.2
SS-2.1
3.8f
3.10gConfiguration SettingsCM-6
CM-6 (1)10.2.65.4.3cLeast FunctionalityCM-7
CM-7 (1)9.4.210.3.1Contingency Planning
3.6aContingency Planning Policy and ProceduresCP-13.1.19.3.6bContingency
PlanCP-2
CP-2 (1)11.1.34.1.4
9.1.1
9.2
9.2.1
9.2.2
9.2.3
9.2.10
12.1.8SC-3.1
SC-1.1
3.6d
3.6eContingency TrainingCP-3
CP-3 (1)11.1.3
11.1.49.3.2SC-2.3
3.6eContingency Plan TestingCP-4 (1)
CP-4 (2)11.1.54.1.4
9.3.3SC-3.1
3.6cContingency Plan UpdateCP-511.1.59.3.1
9.3.3
10.2.12SC-2.1
SC-3.1
3.6fAlternate Storage SitesCP-6
CP-6 (1)
CP-6 (2)
CP-6 (3)8.4.19.2.4
9.2.5
9.2.7
9.2.9SC-2.1
SC-3.1
3.6gAlternate Processing SitesCP-7

CP-7 (1)
CP-7 (2)
CP-7 (3)
CP-7 (4)11.1.49.1.3
9.2.4
9.2.5
9.2.7
9.2.9SC-2.1
SC-3.1
3.6h
3.5cTelecommunications ServicesCP-8
CP-8 (1)
CP-8 (2)
CP-8 (3)
CP-8 (4)11.1.44.7.3a
4.7.3b
4.7.3c
4.7.3d
4.7.3e
4.7.3fInformation System BackupCP-9 (1)
CP-9 (2)
CP-9 (3)8.4.19.2.6
9.2.9
12.1.9SC-2.1
3.6iInformation System Recovery and ReconstitutionCP-10
CP-10 (1)11.4.19.2.8SC-2.1
Identification and Authentication
5.1aIdentification and Authentication Policy and
ProceduresIA-111.2.35.1.1aUser Identification and AuthenticationIA-2
IA-2 (1)9.5.315.15.1.2aDevice Authentication and Application
AuthenticationIA-39.4.4
9.5.1
9.8.116.2.75.1a
5.1bIdentifier ManagementIA-49.5.315.1.1
15.2.2
16.1.5
15.1.8AC-2.1
AC-3.2
SP-4.1
5.1b
5.1.3a
5.1.3b
5.1.3c
5.1.3d
5.1.3e
5.1.3f
5.1.3g
5.1.3h
5.1.3i
5.1.3j
5.1.1bAuthenticator ManagementIA-515.1.7
15.1.10
15.1.11
15.1.12
15.1.13AC-3.2
5.1.3gAuthenticator FeedbackIA-65.1.1a
5.5.1c

5.5.2f
5.5.2gCryptographic Module AuthenticationIA-716.1.7Incident Response
4.7.1aIncident Response Policy and Procedures IR-13.1.1144.7.1eIncident
Response TrainingIR-2
IR-2 (1)
IR-2 (2)6.3.114.1.4SP-3.4
4.7.1fIncident Response TestingIR-3
IR-3 (1)4.7.1aIncident HandlingIR-4
IR-4 (1)8.1.314.1.1
14.1.2
14.1.6SP-3.4
4.7.1dIncident MonitoringIR-5
IR-5 (1)8.1.314.1.34.7.1i
4.7.1g
4.7.1hIncident ReportingIR-6
IR-6 (1)8.1.314.1.1
14.1.2
14.1.3
14.2.1
14.2.34.7.1a
4.7.1jIncident Response AssistanceIR-7
IR-7 (1)8.1.1
14.1.1SP-3.4
Maintenance
4.6.5bSystem Maintenance Policy and ProceduresMA-18.1.1104.6.5b
4.6.5cPeriodic MaintenanceMA-2
MA-2 (1)
MA-2 (2)7.2.410.1.1
10.1.3
10.2.1SS-3.1
4.6.5dMaintenance ToolsMA-310.1.3
11.2.44.6.5f
4.6.5j
4.6.5kRemote MaintenanceMA-4
MA-4 (1)
MA-4 (2)9.4.510.1.1SS-3.1
4.6.5gMaintenance PersonnelMA-57.2.410.1.1
10.1.3SS-3.1
4.6.5hTimely MaintenanceMA-69.1.2SC-1.2
Media Protection
4.3aMedia Protection Policy and ProceduresMP-18.6.184.3a
4.3lMedia AccessMP-2
MP-2 (1)8.6.18.2.1
8.2.2
8.2.3
8.2.6
8.2.74.3bMedia LabelingMP-38.2.5
8.2.6
10.2.94.3cMedia StorageMP-48.6.3
12.3.17.1.4
8.2.1
8.2.2
8.2.9AC-3.1
4.3kMedia TransportMP-58.7.28.2.2
8.2.44.3d
4.3e
4.3f

4.3h
4.3iMedia SanitizationMP-68.6.13.2.11
3.2.12
3.2.13
8.2.8
8.2.9AC-3.4
4.3i
4.3jMedia Destruction and DisposalMP-77.2.6
8.6.23.2.11
3.2.12
3.2.13
8.2.10AC-3.4
Physical and Environmental Protection
4.2.1aPhysical and Environmental Protection Policy and
ProceduresPE-174.2.2b
4.2.2cPhysical Access AuthorizationsPE-27.1.1
7.1.2AC-3.1
4.2.2a
4.2.2d
4.2.2ePhysical Access ControlPE-37.1.2
7.1.57.1.1
7.1.2
7.1.5
7.1.6AC-3.1
Optional ControlAccess Control for Transmission
MediumPE-47.2.24.2.2fAccess Control for Display
MediumPE-57.2.14.2.2gMonitoring Physical AccessPE-6
PE-6 (1)
PE-6 (2)7.2.37.1.9AC-4
4.2.1b
4.2.1cVisitor ControlPE-7
PE-7 (1)7.1.27.1.7AC-3.1
4.2.1bAccess LogsPE-8
PE-8 (1)7.1.27.1.9AC-4
4.2.2hPower Equipment and Cabling
PE-9 (1Optional ControlPE-97.2.37.1.16SC-2.2
4.2.2iEmergency ShutoffPE-107.2.24.2.2k
4.2.2lEmergency Power
PE-11 (2Optional ControlPE-11 (1)7.2.27.1.18SC-2.2
4.2.2mEmergency LightingPE-127.2.24.2.2n
4.2.2o
4.2.2pFire ProtectionPE-13
PE-13 (1)
PE-13 (2)7.2.17.1.12SC-2.2
4.2.2qTemperature and Humidity ControlsPE-147.1.14
7.1.15SC-2.2
4.2.2rWater Damage ProtectionPE-157.2.17.1.17SC-2.2
4.2.2sDelivery and RemovalPE-167.1.57.1.3
7.1.11AC-3.1
4.2.1dAlternate Work SitePE-179.8.2Planning
3.1bSecurity Planning Policy and ProceduresPL-153.1bSystem Security
PlanPL-25.1.1
5.1.2SP-2.1
3.1bSystem Security Plan UpdatePL-35.2.1SP-2.1
4.1.1a
4.1.1b
4.1.1cRules of BehaviorPL-44.1.33.1dPrivacy Impact

AssessmentPL-512.1.4Personnel Security
3.1.1aPersonnel Security Policy and ProceduresPS-164.1aPosition
CategorizationPS-26.1.1
6.1.2SD-1.2
4.1b
4.1c
4.1dPersonnel ScreeningPS-36.1.26.2.1
6.2.2
6.2.3
6.2.4SP-4.1
4.1.5aPersonnel TerminationPS-46.1.7SP-4.1
4.1.5aPersonnel TransferPS-56.1.7SP-4.1
4.1.1a
4.1.1b
4.1.1c
4.1.2a
4.1.2bAccess AgreementsPS-66.1.36.1.5
6.2.2SP-4.1
3.3a
3.3dThird-Party Personnel SecurityPS-74.2.26.2.2SP-4.1
3.11a
3.11b
3.11cPersonnel SanctionsPS-86.3.5
9.2.16.1.5Risk Assessment
3.9aRisk Assessment Policy and ProceduresRA-113.1.1aSecurity
CategorizationRA-25.2.11.1.3
3.1.1SP-1
AC-1.1
AC-1.2
3.9aRisk AssessmentRA-3INTRO1.1.2
1.1.4
1.1.5
1.1.6
1.2.1
1.2.3
4.1.7
7.1.13
7.1.19SP-1
3.9bRisk Assessment UpdateRA-4INTRO1.1.2SP-1
5.4.2cVulnerability Scanning
RA-5 (3Optional ControlRA-5
RA-5 (1)
RA-5 (2)10.3.2
14.2.1System and Services Acquisition
3.2a
3.2bSystem and Services Acquisition Policy and ProceduresSA-133.2a
3.2bAllocation of ResourcesSA-28.2.13.1.2
3.1.3
3.1.53.2c
3.7aLife Cycle SupportSA-33.13.2d
3.3a
3.3bAcquisitionsSA-410.1.13.1.6
3.1.7
3.1.9
3.1.11
3.1.124.7.2aInformation System DocumentationSA-5
SA-5 (1)

SA-5 (2)8.6.43.2.2
3.2.3
3.2.4
3.2.8
12.1.6CC-2.1
4.6.2a
4.6.2bSoftware Usage RestrictionsSA-612.1.210.2.10
10.2.13SS-3.2
SP-2.1
4.6.3aUser Installed SoftwareSA-710.4.110.2.10SS-3.2
3.7bSecurity Design PrinciplesSA-83.2.13.3b
3.3c
3.3dOutsourced Information System ServicesSA-94.2.112.2.33.8hDeveloper Configuration ManagementSA-1010.5.1
10.5.2 CM-3
3.8iDeveloper Security TestingSA-1110.5.1
10.5.23.2.1
3.2.2
10.2.5
12.1.5CM-3
System and Communications Protection
4.4System and Communications Policy and ProceduresSC-13.7cApplication PartitioningSC-2DOD ControlSecurity Function IsolationSC-3DOD ControlInformation Remnants
*Media sanitization is covered in Section 4.3SC-43.2.12AC-3.4
5.4.4dDenial of Service Protection
SC-5 (1) (2Optional ControlsSC-58.1.3DOD ControlResource PrioritySC-69.1.3
11.2.7SC-1.3
5.4.3b
5.4.3d
5.4.3e
5.4.3f
5.4.4a
5.4.4bBoundary ProtectionSC-7
SC-7 (1)9.4.616.2.2
16.2.7
16.2.8
16.2.9
16.2.10
16.2.11
16.2.14AC-3.2
4.4.1a
5.5.1cTransmission IntegritySC-8
SC-8 (1)8.7.311.2.1
11.2.4
11.2.9
16.2.14AC-3.2
4.4.1b
5.5.1cTransmission ConfidentialitySC-9
SC-9 (1)5.2.2aNetwork DisconnectSC-1016.2.6AC-3.2
5.1.3h
Optional ControlTrusted PathSC-115.5.1bCryptographic Key Establishment and ManagementSC-1210.3.516.1.7
16.1.85.5.1aUse of Validated CryptographySC-1316.1.7
16.1.85.4.4ePublic Access ProtectionsSC-148.7.616.3.15.7aCollaborative ComputingSC-15Optional ControlTransmission of Security ParametersSC-165.2.2

8.7.116.1.6AC-3.2
5.2.2bPublic Key Infrastructure CertificatesSC-1710.3.55.4.4aMobile CodeSC-185.7bVoice Over Internet ProtocolSC-19System and Information Integrity
4.7.1c
5.6a
5.6bSystem and Information Integrity Policy and ProceduresSI-111.4.7.1cFlaw Remediation
SI-2 (1) (2Optional Controls but have been included in policy as a best practiceSI-2
SI-2 (1)
SI-2 (2)10.4.110.3.2
11.1.1
11.1.2
11.2.2
11.2.7SS-2.2
5.6aMalicious Code ProtectionSI-3
SI-3 (1)
SI-3 (2)8.3.111.1.1
11.1.24.7.1b
5.4.2a
5.4.2b
5.6aIntrusion Detection Tools and Techniques
SI-4 (1) (2Optional Controls but have been included in policy as a best practice.
SI-4 (3) (4Optional ControlsSI-4
SI-4 (1)
SI-4 (2)9.7.211.2.5
11.2.64.7.1b
5.6aSecurity Alerts and AdvisoriesSI-514.1.1
14.1.2
14.1.5SP-3.4
3.10g
4.7.1cSecurity Functionality Verification
SI-6 (2Optional ControlSI-6
SI-6 (1)11.2.1
11.2.2SS-2.2
3.8gSoftware and Information IntegritySI-710.2.1
10.2.2
10.2.411.2.1
11.2.45.6cSpam and Spyware Protection
SI-8 (1) (2Optional Controls but have been included in policy as a best practice.SI-8
SI-8 (1)
SI-8 (2)4.1.2a
4.1.2bInformation Input RestrictionsSI-910.2.1SD-1
4.7.4aInformation Input Accuracy, Completeness, and ValiditySI-10
SI-10 (1)4.7.4bError HandlingSI-114.3a
4.3gInformation Output Handling and RetentionSI-12HUD Information Technology Security Policy to NIST 800-53 Mapping

HUD Policy Section NumberControl NameNIST
800-53 Control #ISO/IEC 17799NIST
800-26GAO FISCAMOther
Management Policies
3.1aBasic RequirementsFISMA -2004
A.3.d, e, f
3.1bBasic RequirementsPL-15

PL-25.1.1
5.1.2SP-2.1
PL-35.2.1SP-2.1
3.1cBasic RequirementsBest Practice
NIST SP 800-18
3.1dBasic RequirementsPL-512.1.4
3.1eBasic RequirementsAC-69.2.216.1.2
16.1.3
17.1.5AC-3.2HIPPA
3.1.1aInformation and Information System CategorizationRA-25.2.11.1.3
3.1.1SP-1
AC-1.1
AC-1.2
3.1.1bInformation and Information System CategorizationBest Practice
FIPS 199
3.2aCapital Planning and Investment ControlSA-13
SA-28.2.13.1.2
3.1.3
3.1.5
3.2bCapital Planning and Investment ControlSA-13
SA-28.2.13.1.2
3.1.3
3.1.5
3.2cCapital Planning and Investment ControlFISMA-2004
A.2.b, A.3.g
3.2dCapital Planning and Investment ControlFISMA 2004
A.3.g
3.3aContractors and Outsourced OperationsPS-74.2.26.2.2SP-4.1
SA-410.1.13.1.6
3.1.7
3.1.9
3.1.11
3.1.12
3.3bContractors and Outsourced OperationsSA-410.1.13.1.6
3.1.7
3.1.9
3.1.11
3.1.12
SA-94.2.112.2.3
3.3cContractors and Outsourced OperationsSA-94.2.112.2.3
3.3dContractors and Outsourced OperationsPS-74.2.26.2.2SP-4.1FISMA-2004
A.2.c, A.3.a, b
SA-94.2.112.2.3
3.4aPerformance Measures and MetricsBest Practice
3.4bPerformance Measures and MetricsBest Practice
3.4cPerformance Measures and MetricsNIST SP 800-35
3.5aCritical Infrastructure ProtectionPDD-63
3.5bCritical Infrastructure ProtectionPDD-63
3.5cCritical Infrastructure ProtectionCP-8PDD-63
3.6aInformation Technology Contingency PlanningCP-13.1.19
3.6bInformation Technology Contingency PlanningCP-2
CP-2 (1)11.1.34.1.4
9.1.1
9.2
9.2.1

9.2.2
9.2.3
9.2.10
12.1.8SC-3.1
SC-1.1FISMA-2004
A.2.d
3.6cInformation Technology Contingency PlanningCP-511.1.59.3.1
9.3.3
10.2.12SC-2.1
SC-3.1
3.6dInformation Technology Contingency PlanningCP-3
CP-3 (1)11.1.3
11.1.49.3.2SC-2.3
3.6eInformation Technology Contingency PlanningCP-3
CP-3 (1)11.1.3
11.1.49.3.2SC-2.3FISMA-2004
A.2.e
CP-4 (1)
CP-4 (2)11.1.54.1.4
9.3.3SC-3.1
3.6fInformation Technology Contingency PlanningCP-6
CP-6 (1)
CP-6 (2)
CP-6 (3)8.4.19.2.4
9.2.5
9.2.7
9.2.9SC-2.1
SC-3.1
3.6gInformation Technology Contingency PlanningCP-7
CP-7 (1)
CP-7 (2)
CP-7 (3)
CP-7 (4)11.1.49.1.3
9.2.4
9.2.5
9.2.7
9.2.9SC-2.1
SC-3.1
3.6hInformation Technology Contingency PlanningCP-8
CP-8 (1)
CP-8 (2)
CP-8 (3)
CP-8 (4)11.1.4
3.6iInformation Technology Contingency PlanningCP-10
CP-10 (1)11.4.19.2.8SC-2.1
3.7aSystem Development Life CycleSA-33.1FISMA
3.7bSystem Development Life CycleSA-83.2.1
3.7cSystem Development Life CycleSC-2
3.8aConfiguration ManagementCM-1
CM-2
CM-2 (1)
CM-2 (2)1.1.1
10.1.4
10.2.7
10.2.8
10.2.9CC-2.3
CC-3.1

SS-1.2
3.8bConfiguration ManagementCM-3
CM-3 (1)8.1.2
10.4.1
10.5.110.2.2
10.2.3
10.2.10
10.2.11SS-3.2
CC-2.2
3.8cConfiguration ManagementBest Practice
3.8dConfiguration ManagementCM-48.1.210.2.1
10.2.4SS-3.1
SS-3.2
CC-2.1
3.8eConfiguration ManagementCM-5
CM-5 (1)6.1.3
6.1.4
10.1.1
10.1.4
10.1.5SD-1.1
SS-1.2
SS-2.1
3.8fConfiguration ManagementCM-6
CM-6 (1)10.2.6FISMA-2004
D.1, D.2
3.8gConfiguration ManagementSI-710.2.1
10.2.2
10.2.411.2.1
11.2.4
3.8hConfiguration ManagementSA-1010.5.1
10.5.2CM-3
3.8iConfiguration ManagementSA-1110.5.1
10.5.23.2.1
3.2.2
10.2.5
12.1.5CM-3
3.9aRisk Management and Risk AssessmentRA-11
RA-3INTRO1.1.2
1.1.4
1.1.5
1.1.6
1.2.1
1.2.3
4.1.7
7.1.13
7.1.19SP-1
3.9bRisk Management and Risk AssessmentRA-4INTRO1.1.2SP-1
3.9cRisk Management and Risk AssessmentOMB guidance OMB-04-04,
E-Authentication Guidance for Federal Agencies
FISMA-2004
A.3.h
3.10aCertification and AccreditationCA-12
4
CA-43.2.3
3.2.5
4.1.1
4.1.6

11.2.8
12.2.5CC-2.1
CA-64.1.1
4.1.7
4.1.8
12.2.5
3.10bCertification and AccreditationCA-12
4
CA-43.2.3
3.2.5
4.1.1
4.1.6
11.2.8
12.2.5CC-2.1
CA-64.1.1
4.1.7
4.1.8
12.2.5
3.10cCertification and AccreditationCA-12
4FISMA-2004
A.2.a
CA-64.1.1
4.1.7
4.1.8
12.2.5
3.10dCertification and AccreditationCA-12
4
3.10eCertification and AccreditationCA-51.2.3
2.2.1
4.2.1SP-5.1 SP-5.2
3.10fCertification and Accreditation
SI-6 (1) (2TBDCA-24.1.72.1.1
2.1.2
2.1.3
2.1.4SP-5.1FISMA-2004
A.2.c
3.10gCertification and AccreditationCA-79.7.2
12.2.110.2.1
CM-6 (1)10.2.6
SI-611.2.1
11.2.2SS-2.2
3.10hCertification and AccreditationCA-31.1.1
3.2.9
4.1.2
4.1.8
12.2.3CC-2.1
3.10iCertification and AccreditationHUD Policy
3.10jCertification and AccreditationHUD Policy
3.11aIncidents, Violations, and Disciplinary ActionPS-86.3.5
9.2.16.1.5
3.11bIncidents, Violations, and Disciplinary ActionPS-86.3.5
9.2.16.1.5
3.11cIncidents, Violations, and Disciplinary ActionPS-86.3.5
9.2.16.1.5
Operational Policies
4.1aPersonnelPS-26.1.1
6.1.2SD-1.2

4.1bPersonnelPS-36.1.26.2.1
6.2.2
6.2.3
6.2.4SP-4.1
4.1cPersonnelPS-36.1.26.2.1
6.2.2
6.2.3
6.2.4SP-4.1
4.1dPersonnelPS-36.1.26.2.1
6.2.2
6.2.3
6.2.4SP-4.1
4.1ePersonnelHUD Policy
4.1fPersonnelHUD Policy
4.1.1aRules of BehaviorPL-44.1.3
PS-66.1.36.1.5
6.2.2SP-4.1
4.1.1bRules of BehaviorPL-44.1.3
PS-66.1.36.1.5
6.2.2SP-4.1
4.1.1cRules of BehaviorPL-44.1.3
PS-66.1.36.1.5
6.2.2SP-4.1
4.1.2aAccess to Sensitive InformationPS-66.1.36.2.2SP-4.1
SI-912.2.1
12.2.2SD-1
4.1.2bAccess to Sensitive InformationPS-66.1.36.1.5
6.2.2SP-4.1
SI-912.2.1
12.2.2 SD-1
4.1.3aSeparation of Duties PolicyAC-58.1.46.1.1
6.1.2
6.1.3
15.2.1
16.1.2
17.1.5SD-1.2OMB A-130 Appendix III
4.1.4aTraining and AwarenessAT-113
4.1.4bTraining and AwarenessAT-34.2.2
6.2.1
6.3.1
8.3.1
9.8.113.1
13.1.5
4.1.4cTraining and AwarenessAT-34.2.2
6.2.1
6.3.1
8.3.1
9.8.113.1
13.1.5FISMA-2004
G.1.b
AT-26.3.1
9.8.1
11.1.4
12.1.413.1.4
13.1.5
4.1.4dTraining and AwarenessAT-3 13.1.5 FISMA-2004
G.1.b

4.1.4eTraining and AwarenessAT-413.1.2FISMA-2004
G.1.b, d, e, f
4.1.4fTraining and AwarenessAT-4HUD Policy
4.1.4gTraining and AwarenessBest Practice
4.1.4hTraining and AwarenessAT-413.1.2FISMA 2004
G.1.a, b, c, d
4.1.5aSeparation from DutyAC-2 (1)
AC-2 (3)
AC-2 (4)9.2.1
9.2.26.1.8
15.1.1
15.1.4
15.1.8
15.2.2
16.1.3
16.1.5
16.2.12AC-2.1
AC-2.2
AC-3.2
SP-4.1
PS-46.1.7SP-4.1
PS-56.1.7SP-4.1
4.2.1aGeneral Physical AccessPE-1
PE-37
4.2.1bGeneral Physical AccessPE-7
PE-7 (1)7.1.27.1.7AC-3.1
PE-8
PE-8 (1)7.1.27.1.9AC-4
4.2.1cGeneral Physical AccessPE-7
PE-7 (1)7.1.27.1.7AC-3.1
4.2.1dGeneral Physical AccessPE-179.8.2
4.2.1eGeneral Physical AccessBest Practice
4.2.2aFacilities Housing Information Technology AssetsPE-37.1.2
7.1.57.1.1
7.1.2
7.1.5
7.1.6AC-3.1
4.2.2bFacilities Housing Information Technology AssetsPE-27.1.1
7.1.2AC-3.1
4.2.2cFacilities Housing Information Technology AssetsPE-27.1.1
7.1.2AC-3.1
4.2.2dFacilities Housing Information Technology AssetsPE-37.1.2
7.1.57.1.1
7.1.2
7.1.5
7.1.6AC-3.1
4.2.2eFacilities Housing Information Technology AssetsPE-37.1.2
7.1.57.1.1
7.1.2
7.1.5
7.1.6AC-3.1
4.2.2fFacilities Housing Information Technology AssetsPE-57.2.1
4.2.2gFacilities Housing Information Technology AssetsPE-6
PE-6 (1)
PE-6 (2)7.2.37.1.9AC-4
4.2.2hFacilities Housing Information Technology
AssetsPE-97.2.37.1.16SC-2.2

4.2.2iFacilities Housing Information Technology AssetsPE-107.2.2
4.2.2jFacilities Housing Information Technology AssetsSC-2.2
4.2.2kFacilities Housing Information Technology AssetsPE-11
(1)7.2.27.1.18SC-2.2
4.2.2lFacilities Housing Information Technology AssetsPE-11 (1)
7.2.27.1.18SC-2.2
4.2.2mFacilities Housing Information Technology AssetsPE-127.2.2
4.2.2nFacilities Housing Information Technology AssetsPE-13
PE-13 (1)
PE-13 (2)7.2.17.1.12SC-2.2
4.2.2oFacilities Housing Information Technology AssetsPE-13
PE-13 (1)
PE-13 (2)7.2.17.1.12SC-2.2
4.2.2pFacilities Housing Information Technology AssetsPE-13
PE-13 (1)
PE-13 (2)7.2.17.1.12SC-2.2
4.2.2qFacilities Housing Information Technology AssetsPE-147.1.14
7.1.15SC-2.2
4.2.2rFacilities Housing Information Technology
AssetsPE-157.2.17.1.17SC-2.2
4.2.2sFacilities Housing Information Technology
AssetsPE-167.1.57.1.3
7.1.11AC-3.1
4.3aMedia ControlsMP-18.6.18
MP-2
MP-2 (1)8.6.18.2.1
8.2.2
8.2.3
8.2.6
8.2.7
SI-1210.7.3
12.2.4
4.3bMedia ControlsMP-38.2.5
8.2.6
10.2.9
AC-155.2.28.2.4
16.1.6AC-3.2
4.3cMedia ControlsMP-48.6.3
12.3.17.1.4
8.2.1
8.2.2
8.2.9AC-3.1
4.3dMedia ControlsMP-68.6.13.2.11
3.2.12
3.2.13
8.2.8
8.2.9AC-3.4
4.3eMedia ControlsMP-68.6.13.2.11
3.2.12
3.2.13
8.2.8
8.2.9AC-3.4
4.3fMedia ControlsMP-68.6.13.2.11
3.2.12
3.2.13
8.2.8
8.2.9AC-3.4

4.3gMedia ControlsSI-1210.7.3
12.2.4
4.3hMedia ControlsMP-68.6.13.2.11
3.2.12
3.2.13
8.2.8
8.2.9AC-3.4
4.3iMedia ControlsMP-68.6.13.2.11
3.2.12
3.2.13
8.2.8
8.2.9AC-3.4
MP-77.2.6
8.6.23.2.11
3.2.12
3.2.13
8.2.10AC-3.4
4.3jMedia ControlsMP-77.2.6
8.6.23.2.11
3.2.12
3.2.13
8.2.10AC-3.4
4.3kMedia ControlsMP-58.7.28.2.2
8.2.4
4.3lMedia ControlsMP-2
MP-2 (1)8.6.18.2.1
8.2.2
8.2.3
8.2.6
8.2.7
4.4Data CommunicationsSC-1
4.4.1aTelecommunications Protection TechniquesSC-8
SC-8 (1)8.7.311.2.1
11.2.4
11.2.9
16.2.14AC-3.2
4.4.1bTelecommunications Protection TechniquesSC-9
SC-9 (1)
4.5.1aWireless Local Area NetworksAC-18
AC-18 (1)
4.5.1bWireless Local Area NetworksAC-18
AC-18 (1)
4.5.1cWireless Local Area NetworksAC-18
AC-18 (1)
4.5.1dWireless Local Area NetworksAC-18
AC-18 (1)
4.6.1aWorkstationsAC-1116.1.4AC-3.2
4.6.1bWorkstationsAC-1116.1.4AC-3.2
4.6.2aCopyrighted SoftwareSA-612.1.210.2.10
10.2.13SS-3.2
SP-2.1
4.6.2bCopyrighted SoftwareSA-612.1.210.2.10
10.2.13SS-3.2
SP-2.1
4.6.3aUser-Installed Software/DownloadsSA-710.4.110.2.10SS-3.2
4.6.4aPersonally-Owned Equipment and SoftwareAC-207.2.5
7.3.1

9.8.110.2.13
4.6.4bPersonally-Owned Equipment and SoftwareCM-1
AC-207.2.5
7.3.1
9.8.110.2.13
4.6.4cPersonally-Owned Equipment and SoftwareAC-207.2.5
7.3.1
9.8.110.2.13
4.6.5aHardware and Software MaintenanceCM-1
AC-3
AC-3 (1)9.2.4
9.4.6
9.4.815.1.1
16.1.1
16.1.2
16.1.3
16.1.7
16.1.9
16.2.7
16.2.10
16.2.11
16.2.15AC-2
AC-3.2Best Practice
4.6.5bHardware and Software MaintenanceMA-18.1.110
MA-2
MA-2 (1)
MA-2 (2)7.2.410.1.1
10.1.3
10.2.1SS-3.1Best Practice
4.6.5cHardware and Software MaintenanceMA-2
MA-2 (1)7.2.410.1.1
10.1.3
10.2.1SS-3.1Best Practice
4.6.5dHardware and Software MaintenanceMA-310.1.3
11.2.4
4.6.5eHardware and Software MaintenanceCM-1
4.6.5fHardware and Software MaintenanceMA-4
MA-4 (1)9.4.510.1.1SS-3.1
4.6.5gHardware and Software MaintenanceMA-57.2.410.1.1
10.1.3SS-3.1
4.6.5hHardware and Software MaintenanceMA-69.1.2SC-1.2
4.6.5iHardware and Software MaintenanceCM-1
4.6.5jHardware and Software MaintenanceMA-4
MA-4 (2)9.4.510.1.1SS-3.1
4.6.5kHardware and Software MaintenanceMA-4
MA-4(2)9.4.510.1.1SS-3.1
4.6.6aPersonal Use of Government Office Equipment and HUD
Information Systems/ComputersBest Practice
4.6.6bPersonal Use of Government Office Equipment and HUD
Information Systems/ComputersBest Practice
4.7.1aSecurity Incident and Violation HandlingIR-143.1.114
IR-4
IR-4 (1)8.1.314.1.1
14.1.2
14.1.6SP-3.4FISMA-2004
E.1.a
IR-7

IR-7 (1)8.1.1
14.1.1SP-3.4
4.7.1bSecurity Incident and Violation HandlingSI-4
SI-4 (1)
SI-4 (2)9.7.211.2.5
11.2.6
SI-514.1.1
14.1.2
14.1.5SP-3.4
4.7.1cSecurity Incident and Violation HandlingSI-111.
SI-6(1)11.2.1
11.2.2SS-2.2
SI-2
SI-2 (1)
SI-2 (2)10.4.110.3.2
11.1.1
11.1.2
11.2.2
11.2.7SS-2.2
4.7.1dSecurity Incident and Violation HandlingIR-5
IR-5 (1)8.1.314.1.3FISMA-2004
F.1.a, b, c
F.2.c
4.7.1eSecurity Incident and Violation HandlingIR-2
IR-2 (1)
IR-2 (2)6.3.114.1.4SP-3.4
4.7.1fSecurity Incident and Violation HandlingIR-3
IR-3 (1)
4.7.1gSecurity Incident and Violation HandlingIR-6
IR-6 (1)8.1.314.1.1
14.1.2
14.1.3
14.2.1
14.2.3
4.7.1hSecurity Incident and Violation HandlingIR-6
IR-6 (1)8.1.314.1.1
14.1.2
14.1.3
14.2.1
14.2.3FISMA 2004
E.1.b, c
F.1.b, c
4.7.1iSecurity Incident and Violation HandlingIR-6
IR-6 (1)8.1.314.1.1
14.1.2
14.1.3
14.2.1
14.2.3
4.7.1jSecurity Incident and Violation HandlingIR-7
IR-7 (1)8.1.1
14.1.1SP-3.4
4.7.2aDocumentation (Manuals and Network Diagrams)SA-5
SA-5 (1)
SA-5 (2)8.6.43.2.2
3.2.3
3.2.4
3.2.8

12.1.6CC-2.1
4.7.3aInformation and Data BackupCP-9 (1)
CP-9 (2)
CP-9 (3)8.4.19.2.6
9.2.9
12.1.9SC-2.1
4.7.3bInformation and Data BackupCP-9 (1)
CP-9 (2)
CP-9 (3)8.4.19.2.6
9.2.9
12.1.9SC-2.1
4.7.3cInformation and Data BackupCP-9 (1)
CP-9 (2)
CP-9 (3)8.4.19.2.6
9.2.9
12.1.9SC-2.1
4.7.3dInformation and Data BackupCP-9 (1)
CP-9 (2)
CP-9 (3)8.4.19.2.6
9.2.9
12.1.9SC-2.1
4.7.3eInformation and Data BackupCP-9 (1)
CP-9 (2)
CP-9 (3)8.4.19.2.6
9.2.9
12.1.9SC-2.1
4.7.3fInformation and Data BackupCP-9 (1)
CP-9 (2)
CP-9 (3)8.4.19.2.6
9.2.9
12.1.9SC-2.1
4.7.4aInput/Output ControlsSI-10
SI-10 (1)
4.7.4bInput/Output ControlsSI-11
Technical Policies
5.1aIdentification and AuthenticationIA-49.5.315.1.1
15.2.2
16.1.5
15.1.8AC-2.1
AC-3.2
SP-4.1
IA-2
IA-2 (1)9.5.315.1
IA-111.2.3
5.1bIdentification and AuthenticationIA-49.5.315.1.1
15.2.2
16.1.5
15.1.8AC-2.1
AC-3.2
SP-4.1
IA-515.1.7
15.1.10
15.1.11
15.1.12
15.1.13AC-3.2
5.1cIdentification and AuthenticationBest Practice
5.1dIdentification and AuthenticationAC-2 (1)

AC-2 (3)
AC-2 (4)9.2.1
9.2.26.1.8
15.1.1
15.1.4
15.1.8
15.2.2
16.1.3
16.1.5
16.2.12AC-2.1
AC-2.2
AC-3.2
SP-4.1
5.1eIdentification and AuthenticationAC-2 (1)
AC-2 (3)
AC-2 (4)9.2.1
9.2.26.1.8
15.1.1
15.1.4
15.1.8
15.2.2
16.1.3
16.1.5
16.2.12AC-2.1
AC-2.2
AC-3.2
SP-4.1
5.1.1aE-AuthenticationIA-29.5.315.1OMB-04-04
IA-716.1.7
5.1.1bE-AuthenticationIA-5OMB-04-04
5.1.2aDevice and Application AuthenticationIA-39.4.4
9.5.1
9.8.116.2.7
5.1.3aPasswordsIA-515.1.7
15.1.10
15.1.11
15.1.12
15.1.13AC-3.2
5.1.3bPasswordsIA-515.1.7
15.1.10
15.1.11
15.1.12
15.1.13AC-3.2
5.1.3cPasswordsIA-515.1.7
15.1.10
15.1.11
15.1.12
15.1.13AC-3.2
5.1.3dPasswordsIA-515.1.7
15.1.10
15.1.11
15.1.12
15.1.13AC-3.2
5.1.3ePasswordsIA-515.1.7
15.1.10
15.1.11
15.1.12

15.1.13AC-3.2Best Practice
5.1.3fPasswordsIA-515.1.7
15.1.10
15.1.11
15.1.12
15.1.13AC-3.2
5.1.3gPasswordsIA-515.1.7
15.1.10
15.1.11
15.1.12
15.1.13AC-3.2
IA-6
5.1.3hPasswordsIA-515.1.7
15.1.10
15.1.11
15.1.12
15.1.13AC-3.2
SC-1116.2.7
5.1.3iPasswordsIA-515.1.7
15.1.10
15.1.11
15.1.12
15.1.13AC-3.2
5.1.3jPasswordsIA-515.1.7
15.1.10
15.1.11
15.1.12
15.1.13AC-3.2
5.2aAccess ControlAC-19.1.1
9.4.115
16
AC-2 (1)
AC-2 (3)
AC-2 (4)9.2.1
9.2.26.1.8
15.1.1
15.1.4
15.1.8
15.2.2
16.1.3
16.1.5
16.2.12AC-2.1
AC-2.2
AC-3.2
SP-4.1
5.2bAccess ControlAC-2 (1)
AC-2 (3)
AC-2 (4)9.2.1
9.2.26.1.8
15.1.1
15.1.4
15.1.8
15.2.2
16.1.3
16.1.5
16.2.12AC-2.1
AC-2.2

AC-3.2
SP-4.1
5.2cAccess ControlAC-58.1.46.1.1
6.1.2
6.1.3
15.2.1
16.1.2
17.1.5SD-1.2
AC-69.2.216.1.2
16.1.3
17.1.5AC-3.2
5.2dAccess ControlAC-2
AC-2 (2)
5.2eAccess ControlAC-2 (1)
AC-2 (3)
AC-2 (4)9.2.1
9.2.26.1.8
15.1.1
15.1.4
15.1.8
15.2.2
16.1.3
16.1.5
16.2.12AC-2.1
AC-2.2
AC-3.2
SP-4.1
5.2fAccess ControlAC-1416.2.12
5.2.1aAutomatic Account LockoutAC-79.5.215.1.14AC-3.2
5.2.1bAutomatic Account LockoutAC-79.5.215.1.14AC-3.2
5.2.2aLogon and Session SecurityAC-129.5.716.1.4
16.2.6AC-3.2
SC-1016.2.6AC-3.2
5.2.2bLogon and Session SecurityAC-10
SC-1710.3.5
5.2.3aWarning BannerAC-89.5.216.2.13
17.1.9AC-3.2
5.2.3bWarning BannerAC-89.5.216.2.13
17.1.9AC-3.2
5.2.3cWarning BannerAC-89.5.216.2.13
17.1.9AC-3.2
Audit and Accountability
5.3aAudit and AccountabilityAU-117
AU-2
AU-2 (1)11.1.217.1.1
17.1.2
17.1.4
AU-3
AU-3 (1)
AU-3 (2)9.7.217.1.1
5.3bAudit and AccountabilityAU-912.3.217.1.3
17.1.4
5.3cAudit and AccountabilityAU-1110.7.1
12.1.317.1.4
5.3dAudit and AccountabilityAC-13
AC-13 (1)9.2.47.1.10
11.2.2

16.1.10
17.1.6
17.1.7AC-4
AC-4.3
SS-2.2
AU-6
AU-6 (1)9.7.217.1.1
5.3eAudit and AccountabilityAU-49.7.2
5.3fAudit and AccountabilityAU-5
AU-5 (1)9.7.2
5.3gAudit and AccountabilityAU-59.7.2
5.3hAudit and AccountabilityAU-7
AU-7 (1)17.1.2
17.1.7
5.3iAudit and AccountabilityAU-2
AU-2 (1)11.1.217.1.1
17.1.2
17.1.4
AU-3
AU-3 (1)
AU-3 (2)9.7.217.1.1
5.3jAudit and AccountabilityAU-89.7.3
5.4.1aRemote Access and Dial-InAC-17
AC-17 (1)
AC-17 (2)
AC-17 (3)9.4.3
9.4.416.2.12
16.2.4
16.2.8AC-3.2
5.4.1bRemote Access and Dial-InAC-17
AC-17 (1)
AC-17 (2)
AC-17 (3)9.4.3
9.4.416.2.12
16.2.4
16.2.8AC-3.2
5.4.1cRemote Access and Dial-InAC-17
AC-17 (1)
AC-17 (2)
AC-17 (3)9.4.3
9.4.416.2.12
16.2.4
16.2.8AC-3.2
5.4.1dRemote Access and Dial-InAC-17
AC-17 (1)
AC-17 (2)
AC-17 (3)9.4.3
9.4.416.2.12
16.2.4
16.2.8AC-3.2
5.4.2aNetwork Security MonitoringSI-4
SI-4 (1)
SI-4 (2)9.7.211.2.5
11.2.6
5.4.2bNetwork Security MonitoringSI-4
SI-4 (1)
SI-4 (2)9.7.211.2.5

11.2.6
5.4.2cNetwork Security MonitoringRA-510.3.2
14.2.1FISMA-2004
E.2.a
5.4.2.dNetwork Security MonitoringNIST SP 800-42
5.4.3aNetwork ConnectivityAC-3
AC-3 (1)9.2.4
9.4.6
9.4.815.1.1
16.1.1
16.1.2
16.1.3
16.1.7
16.1.9
16.2.7
16.2.10
16.2.11
16.2.15AC-2
AC-3.2
AC-19.1.1
9.4.115
16
5.4.3bNetwork ConnectivitySC-7
SC-7 (1)9.4.616.2.2
16.2.7
16.2.8
16.2.9
16.2.10
16.2.11
16.2.14AC-3.2
AC-49.4.6
9.4.8
5.4.3cNetwork ConnectivityCM-7
CM-7 (1)9.4.210.3.1
5.4.3dNetwork ConnectivitySC-7
SC-7 (1)9.4.616.2.2
16.2.7
16.2.8
16.2.9
16.2.10
16.2.11
16.2.14AC-3.2
5.4.3eNetwork ConnectivitySC-7
SC-7 (1)9.4.616.2.2
16.2.7
16.2.8
16.2.9
16.2.10
16.2.11
16.2.14AC-3.2
5.4.3fNetwork ConnectivitySC-7
SC-7 (1)9.4.616.2.2
16.2.7
16.2.8
16.2.9
16.2.10
16.2.11

16.2.14AC-3.2
5.4.3gNetwork ConnectivityAC-199.5.1
9.8.17.3.1
7.3.2
5.4.3hNetwork ConnectivityAC-199.5.1
9.8.17.3.1
7.3.2
5.4.4aInternet SecuritySC-18
SC-7
SC-7 (1)9.4.616.2.2
16.2.7
16.2.8
16.2.9
16.2.10
16.2.11
16.2.14AC-3.2
5.4.4bInternet SecuritySC-7
SC-7 (1)9.4.616.2.2
16.2.7
16.2.8
16.2.9
16.2.10
16.2.11
16.2.14AC-3.2
5.4.4cInternet SecuritySC-18
5.4.4dInternet SecuritySC-58.1.3
5.4.4eInternet SecuritySC-148.7.616.3.1
5.4.5aPersonal Email AccountsBest Practice
5.4.5bPersonal Email AccountsHUD Policy
5.5.1aEncryptionSC-1316.1.7
16.1.8FIPS 46-3
FIPS 140-2
FIPS 197
5.5.1bEncryptionSC-1210.3.516.1.7
16.1.8
5.5.1cEncryptionAC-17
AC-17 (1)
AC-17 (2)
AC-17 (3)9.4.3
9.4.416.2.12
16.2.4
16.2.8AC-3.2
SC-9
SC-9 (1)
SC-8
SC-8 (1)8.7.311.2.1
11.2.4
11.2.9
16.2.14AC-3.2
IA-716.1.7
AC-18
AC-18 (1)
5.5.1dEncryptionAC-19 (1)9.5.1
9.8.17.3.1
7.3.2
5.5.2aPublic Key InfrastructureBest Practice
5.5.2bPublic Key InfrastructureSC-17

5.5.2cPublic Key InfrastructureSC-17
5.5.2dPublic Key InfrastructureBest Practice
5.5.2ePublic Key InfrastructureBest Practice
5.5.2fPublic Key InfrastructureIA-716.1.7OMB
GPEA
5.5.2gPublic Key InfrastructureIA-716.1.7Homeland
Security PDD-12
5.5.3aPublic Key/Private KeyBest Practice
5.5.3bPublic Key/Private KeyFIPS 186-2
5.5.3cPublic Key/Private KeyFIPS 186-2
5.6aMalicious Code ProtectionSI-111
SI-3
SI-3 (1)
SI-3 (2)8.3.111.1.1
11.1.2
SI-4
SI-4 (1)
SI-4 (2)9.7.211.2.5
11.2.6
SI-514.1.1
14.1.2
14.1.5SP-3.4
5.6bMalicious Code ProtectionSI-111
5.6cMalicious Code ProtectionSI-8
SI-8 (1)
SI-8 (2)
5.7aMiscellaneousSC-15Best Practice
5.7bMiscellaneousSC-19Best Practice

Appendix B. Acronyms

3DESTriple Data Encryption Standard
AESAdvanced Encryption Standard
AISAutomated Information System
AOAuthorizing Official
APAccess Point
BIABusiness Impact Analysis
C&ACertification and Accreditation
CACertification Authority
CBACost-Benefit Analysis
CDCompact Disk
CFRCode of Federal Regulations
CIOChief Information Officer
CIPCritical Infrastructure Protection
CISOChief Information Security Officer
CMConfiguration Management
COContracting Officer
COOPContinuity of Operations
COTSCommercial off-the Shelf
CPICCapital Planning & Investment Control
CSAComputer Security Act
CSIRCComputer Security Incident Response Center
CSOChief Security Officer
DHCPDynamic Host Configuration Protocol
DoSDenial of Service
DVDDigital Versatile Disk
EAEnterprise Architecture
EAPExtensible Authentication Protocol
EOExecutive Order
FARFederal Acquisition Regulation
FIPSFederal Information Processing Standard
FISCAMFederal Information System Controls Audit Manual
FISMAFederal Information Security Management Act
GAOGeneral Accountability Office
GISRAGovernment Information Security Reform Act
GSAGeneral Service s Administration
GTMGovernment Technical Monitor
GTRGovernment Technical Representative
HIPAAHealth Insurance Portability and Accountability Act
HSPDHomeland Security Presidential Directive
HUDDepartment of Housing and Urban Development
HUDARHUD Acquisition Regulation
IATOInterim Authority to Operate
IDIdentification
IDSIntrusion Detection System
IECInternational Electrotechnical Commission
IEEEInstitute of Electrical and Electronic Engineers
IGInspector General
ISOInternational Standards Organization
ISSBInformation Systems Security Branch

ISSOInformation System Security Officer
ITInformation Technology
ITMRAInformation Technology Management Reform Act
LANLocal Area Network
MACMedia Access Control
MBIMinimum Background Investigation
MOAMemorandum of Agreement
NISTNational Institute of Standards and Technology
NIST SPNational Institute of Standards and Technology Special Publication
NSANational Security Agency
O&MOperations & Maintenance
OAMSOffice of Administration and Management Services
OIGOffice of Inspector General
OMBOffice of Management and Budget
OPCOffice of Procurement and Contracts
OPMOffice of Personnel Management
PDAPersonal Digital Assistant
PDDPresidential Decision Directive
PIVPersonal Identity Verification
PKIPublic Key Infrastructure
POA&MPlans of Action and Milestones
POCPoint of Contact
QAQuality Assurance
SDLCSystem Development Life Cycle
SOWStatement of Work
SPSpecial Publication
SSLSecure Sockets Layer
TBDTo Be Determined
TCP/IPTransmission Control Protocol/Internet Protocol
TLSTransport Layer Security
TSPTelecommunications Service Priority
U.S.C.United States Code
USBUniversal Serial Bus
USCERTUnited States Computer Emergency Readiness Team
USERIDUser ID
VoIPVoice over Internet Protocol
VPNVirtual Private Network
WANWide Area Network
WAPWiFi Access Protection
WGWorking Group
WLANWireless Local Area Network

1.0 INTRODUCTION

The Department of Housing and Urban Development (HUD) relies extensively on information technology (IT) to execute its mission and provide services to the American public and HUD's business partners. Given the prevalence of cyber threats today, HUD must manage its IT assets with due diligence and take the necessary steps to safeguard them while complying with federal mandates and the dictates of good stewardship.

Information security policies are an essential prerequisite to sound IT security. They are designed to preserve the confidentiality, integrity, availability, and value of assets, as well as ensure the continued delivery of services. They also establish the appropriate focus and standards for acceptable security practices across an organization. This policy is based on federal regulations and highlights HUD's goals and requirements for protecting its IT assets.

All HUD components must comply with the basic requirements of this policy and its associated operational standards and technical documentation. Each component must also determine any need for additional safeguards above this baseline level and implement them appropriately. Additional safeguards should be based on an assessment of risk and local conditions.

1.1 Purpose

This document establishes the information security policy for HUD. The policy prescribes responsibilities, practices, and conditions that directly or indirectly promote security in the development, operation, maintenance, and support of all HUD IT resources.

The policy identifies security practices that are appropriate to HUD's mission, provide cost-effective protection of HUD's IT, respond to security issues associated with contemporary technologies and risks, and are consistent with current applicable federal security laws, policies, and regulations.

1.2 Scope

This policy provides a comprehensive view of IT security considerations. It addresses technical security services, as well as the management and operational requirements for IT security, and it identifies all relevant security roles and responsibilities and affected organizations. In addition, the policy addresses security-relevant boundaries (e.g., interfaces with external systems and networks and any use of personal computing in the conduct of HUD's business). It also reflects the increasing requirements for internal and external security oversight from the HUD Office of Inspector General (OIG) and in response to the Federal Information Security Management Act (FISMA).

Since this policy is intended to provide a set of basic protection goals and standards, the procedural details normally found in operational and technical documentation are not within the scope of this document.

Information security policies conventionally require systems to provide various technical security services (e.g., authentication, access control, and intrusion detection); however, a comprehensive policy also identifies managerial and operational requirements, which recent regulations have emphasized. For example, federal departments are required to integrate security planning into their Capital Planning and Investment Control (CPIC) process. Also, the Office of Management and Budget (OMB) requires periodic reports on the state of information security activities at all federal departments, and these reports have implications for acquiring and maintaining such information.

As a result, this policy has implications for more than security specialists and will affect System Owners and developers, practitioners of non-IT security disciplines, support operations personnel (e.g., security training and awareness personnel, contract managers), and personnel interacting with the HUD privacy advocate, OIG, external auditors, HUD Enterprise Architecture (EA) developers, and other agencies.

In addition, this information security policy applies to HUD Program Offices that have security-specific or security-relevant roles and responsibilities, such as system security planning, certification and accreditation (C&A), security audit, configuration management (CM), continuity of operations (COOP) activities, and security incident response. The policy also applies to all HUD employees, contractors, and service providers who must comply with day-to-day provisions of HUD policy (e.g., proper password choice and management, maintaining security awareness, incident reporting, and prompt system upgrades).

1.3 Authority for Policy

The authority for the issuance of this policy rests with the Office of Chief Information Officer. The Program Office that will subsequently issue and maintain this policy includes those responsible for the following:

- Information security policy development
- IT security review and evaluation
- Information security policy enforcement
- Conformance monitoring and evaluation, including the identification and monitoring of metrics where possible
- Interactions with associated policy elements, HUD business functions, system acquisition authorities, and external agencies
- Policy revisions, including interim updates and annual re-issuances, when required

1. Policy waiver evaluations

Section **Error! Reference source not found.** provides the detailed allocation of information security roles and responsibilities among HUD personnel.

1.4 Policy Basis

This policy is primarily based on recent federal laws, regulations, and guidance on information security (e.g., the rapidly growing series of National Institute of Standards and Technology [NIST] Special Publications [SP] on information security). In areas where federal guidelines are lacking or still evolving, the policy reflects established best security practices within the security community. The policy also incorporates previously published HUD information security policy and guidelines.

1.5 Relationship to Other Documents and Processes

As the primary information source for fundamental requirements for maintaining the confidentiality, integrity, and availability of IT resources, the policy identifies and characterizes a comprehensive set of basic protection goals without stipulating how the goals should be met (i.e., the specific technologies, mechanisms, or procedures involved). Procedural details, particularly technical details that are either changeable or applicable to one type of system (e.g., configuration for a particular operating system) are documented separately.

The information security policy may change from time to time. For example, the potential use of some newer technologies (e.g., wireless communications) can give rise to additional policy requirements. In such cases, the policy will outline the basic relevant security policy requirements; however, in general, the policy is free from low-level procedural and technical detail.

The requirements of this policy complement other agency measures for effective management of assets and regulatory compliance (e.g., with the federal privacy laws). References are made to those sources throughout this document.

Guidance on HUD information security standards, methodologies, procedures, and adaptations to ongoing legislation and federal regulations and standards will be expanded in a separate *Information Technology Security Handbook*. The handbook provides additional guidance on information security policy elements, examples of which might include password enforcement mechanisms, C&A procedures, and incident-response procedures.

Where necessary, the most detailed, procedure-intensive, or volatile IT security guidance will be issued in topic-specific guidelines. Generally, technical specialists are the principal users of such guidelines (e.g., specifications of product version-specific configuration settings that are consistent with security requirements or instructions for recovering from a virus attack).[1]

The information security policy, handbook, and set of detailed guidelines form an information security policy compendium as shown in Figure 1. This document compendium becomes the foundation for secure HUD information system design, operation, and maintenance. The figure also depicts mutual influences between

---

[1] Examples of topic areas being addressed in separate guidelines include security configuration guides for IT products, media sanitization techniques, and certification practice statements.

information security policy and a variety of affiliated processes that information security relies upon or affects to some extent, including Quality Assurance (QA), COOP procedures, Critical Infrastructure Protection (CIP), and EA development.

Information security policy makes certain assumptions about protection measures that respond to other HUD security policies and practices (e.g., physical security and personnel security). For example, this policy presupposes reliable processes for confirming the credentials of prospective system users. Information security policy also presupposes the enforcement of suitable physical protection of the means of access to facilities housing HUD IT resources. However, since physical and personnel security policies are not exclusively or primarily concerned with IT resource protection, documents in the information security policy compendium refer to such separate policies or make assumptions about their provisions, as appropriate.

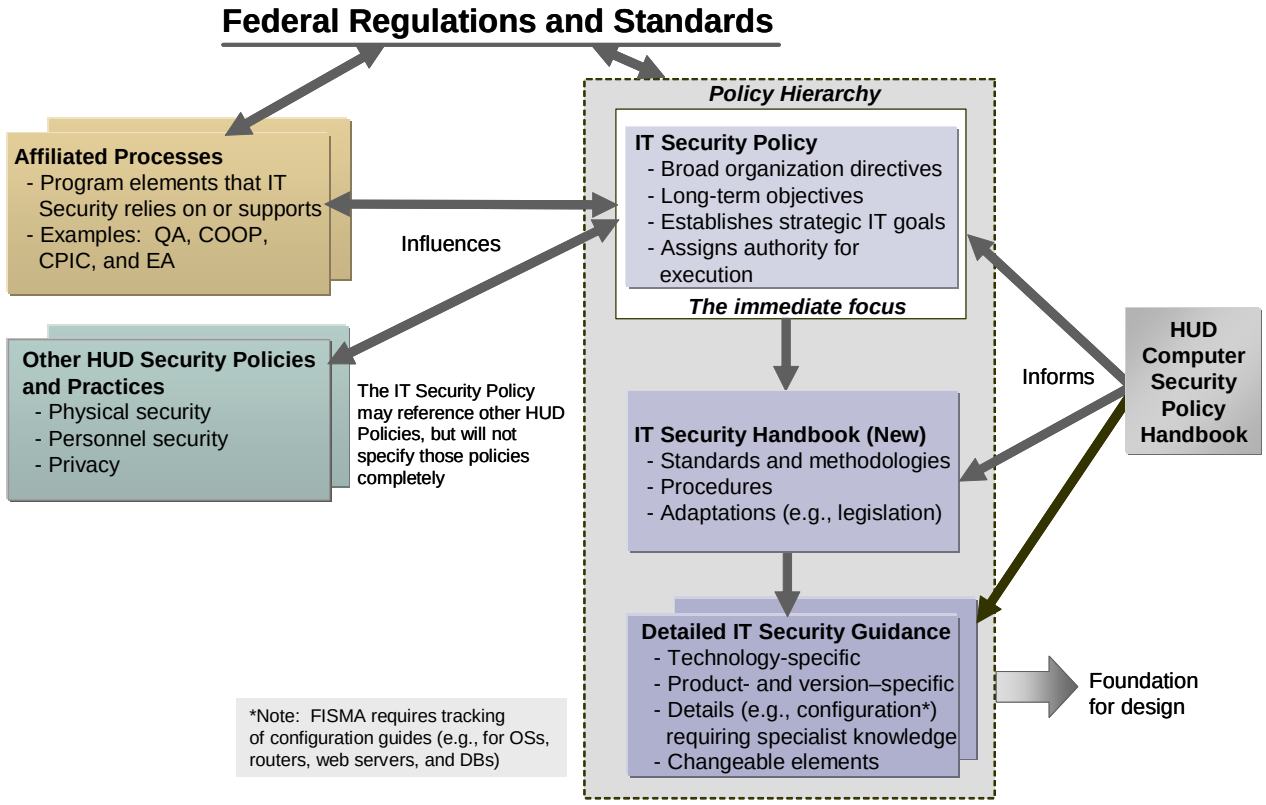

Figure 1. Security Policy Relationships

1.6 Document Organization

Section 2 describes the information security roles and responsibilities assigned to HUD personnel. The policies in Sections 3, 4, and 5 describe in more detail the management, operational, and technical areas of controls necessary to evaluate or assess compliance:

- **Management Controls**—focus on IT security system management and system risk management that consist of risk mitigation techniques and concerns normally addressed by management.
- **Operational Controls**—address security methods that focus primarily on the mechanisms implemented and executed by people. These controls are designed to improve the security of a particular system or group of systems. These controls frequently require technical or specialized expertise and often rely on management and technical controls.

2. **Technical Controls**—focus on security controls that a computer system executes. These controls can provide automated protection for unauthorized access or misuse, facilitate detection of security violations, and support security requirements for applications and data.

Within individual policy requirements, this document includes, where applicable, references to federal standards and regulations that are sources of the policy requirements. These are summarized in Appendix A. The inclusion of the references is intended to provide the policy user with additional information and to serve as a means of confirming the comprehensiveness of HUD's response to the standards and regulations.

1.7 Laws and Regulations

HUD has established a department-wide IT security policy based on the following Executive Orders (EO), public laws, and national policies:

- Electronic Government Act (P.L. 107–347), December 2002.
- Executive Order 13231, *Critical Infrastructure Protection in the Information Age*, October 16, 2001.
- Federal Information Security Management Act (FISMA) of 2002, November 25, 2002.
- FIPS Pub 140–1, *Security Requirements for Cryptographic Modules,* January 1994.
- FIPS Pub 140–2, *Security Requirements for Cryptographic Modules,* May 2001.
- FIPS Pub 199, *Standards for Security Categorization of Federal Information and Information Systems*, December 2003.
- FIPS Pub 200, *Minimum Security Requirements Controls for Federal Information and Information Systems* (projected for publication December 2005).
- FIPS Pub 201, *Personal Identity Verification for Federal Employees and Contractors*, February 2005.
- Homeland Security Presidential Directive (HSPD) 7, *Critical Infrastructure Identification, Prioritization, and Protection*, December 17, 2003.
- Office of Management and Budget Memorandum 03–19, *Reporting Instructions for the Federal Information Security Management Act and Updated Guidance on Quarterly IT Security Reporting*, August 2003.

- Office of Management and Budget Memorandum 03–22, *OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002*, September 2003.
- Office of Management and Budget Memorandum 04–04, *E-Authentication Guidance for Federal Agencies*, December 2003.
- Office of Management and Budget, Circular A-130, Appendix III, Transmittal Memorandum #4, *Management of Federal Information Resources*, November 2000.
- Paperwork Reduction Act of 1995 (P.L. 104-13), May 1995.
- Privacy Act of 1974, As Amended, 5 United States Code (U.S.C.) 552a, Public Law 93-579, Washington, D.C., July 14, 1987.
- Public Law 104–106, Clinger-Cohen Act of 1996 (formerly, Information Technology Management Reform Act [ITMRA]), February 10, 1996.
- Public Law 104–191 (H.R. 3103), Health Insurance Portability and Accountability Act of 1996.
- Public Law 107–296, Homeland Security Act of 2002.

3. Various NIST Special Publications (SP).

1.8 Definitions

Following is a series of the key definitions applicable to the policies and procedures outlined in this document.

1.8.1 Sensitive Information

"Sensitive information" (defined by the Computer Security Act of 1987) is information to which access must be controlled and restricted in order to protect the national interest, the conduct of federal programs, and the privacy to which individuals are entitled under the Privacy Act (Section 552a of Title 5, U.S.C.), but is not specified by Executive Order or an act of Congress to be kept secret (i.e., classified as Top Secret, Secret, or Confidential) in the interest of national security or foreign policy. Examples of sensitive information include personal data (e.g., Social Security Number), trade secrets, system vulnerability information, pre-solicitation procurement documents (e.g., Statement of Work [SOW]), and law enforcement investigative methods. Sensitive information must be protected from loss, misuse, modification, and unauthorized access.

FIPS Pub 199, *Standards for Security Categorization of Federal Information and Information Systems*, was published in December 2003. It is now the mandatory standard for categorizing the sensitivity associated with federal information and information systems (except national security systems).

FIPS Pub 199 provides federal departments with a more detailed categorization of their information assets than the Computer Security Act of 1987 recognized. FIPS Pub 199 distinguishes among *low*, *moderate*, and *high* sensitivity categories and deals explicitly with integrity, availability, and confidentiality as security goals. Categories correspond

to the different degrees of potential impact a security incident may have on a department's mission, assets, legal responsibilities, functions, or individuals.

1.8.2 Public Information

This type of information can be disclosed to the public without restriction, but requires protection against erroneous manipulation or alteration (e.g., a public website).

1.8.3 Information Technology

The Clinger-Cohen Act defines information technology as any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by an executive agency. For purposes of the preceding definition, "equipment" refers to that used by HUD or by a contractor under contract with HUD if that contractor (1) requires the use of such equipment or (2) requires the use, to a significant extent, of such equipment in the performance of a service or the furnishing of a product. The term "information technology" includes computers, ancillary equipment, software, firmware, and similar procedures, services (including support services), and related resources.

1.8.4 HUD Information Technology System

A HUD system is information technology that is (1) owned, leased, or operated by a Program Office, (2) operated by a contractor on behalf of HUD, or (3) operated by another federal, state, or local government agency on behalf of HUD. HUD systems include both general support systems and major applications.

1.8.4.1 *General Support System*

An interconnected set of information resources under the same direct management control that shares common functionality. It normally includes hardware, software, information, data, applications, communications, and people. A general support system can be, for example, a local area network (LAN) including smart terminals that support a branch office, an agency-wide backbone, a communications network, a departmental data processing center and its operating system and utilities, a tactical radio network, or a shared information-processing service organization. The Office of the Chief Information Officer is the Program Office responsible for most of these systems at HUD and the Deputy CIO for IT Operations is the System Owner for such systems.

1.8.4.2 *Major Application*

A major application is an information system that requires special attention to security due to the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of the information in the application. A major application may actually be made up of hardware, software, and firmware, but it is distinguishable from a general support system by the fact that it is a discreet application; whereas, general support systems may support multiple applications.

1.9 Exceptions

When a Program Office is unable to comply with policy, it may request an exception. Exceptions are generally limited to mission-specific systems that are not part of the HUD Enterprise Infrastructure. This request is made to the Chief Information Security Officer (CISO) through the Authorizing Official (AO) and must include the operational justification, risk acceptance, and risk mitigation measures.

2.0 ROLES AND RESPONSIBILITIES

Responsibility for protecting the confidentiality and integrity of HUD's information and technological resources is shared jointly by its employees, business partners, and contractors. However, in an effort to enable effective and complete implementation of this policy, specific duties have been assigned to individuals who will be fully accountable for fulfilling the associated requirements. This section describes the specific information security roles and responsibilities.

2.1 Secretary of the Department of Housing and Urban Development

The Secretary of HUD is responsible for ensuring that HUD IT systems and their data are protected in accordance with congressional and presidential directives. To that end, the Secretary will:

* Ensure the integrity, confidentiality, and availability of information and information systems.
* Ensure that HUD adheres to the requirements of its Information Security Program throughout the life cycle of each HUD system.
* Submit the results of independent evaluations performed by the HUD Inspector General (IG) to the Director of the OMB annually. These evaluations are to accompany HUD annual budget submissions.

2.2 Chief Information Officer

The HUD Chief Information Officer (CIO) will establish and oversee the department-wide Information Security Program and provide consulting assistance to all HUD offices for their individual programs. In addition, the CIO has the following information security responsibilities:

* Appoint, in writing, a federal employee to serve as the CISO.
* Participate in developing HUD performance plans, including descriptions of timeframes and budget, staffing, and training resources required to implement the departmentwide Information Security Program.
* Establish policy and oversight procedures to ensure that all information systems acquisition documents, including existing contracts, incorporate appropriate IT security requirements and comply with HUD IT security policies.
* Ensure that HUD's Information Security Program integrates fully into the HUD EA and CPIC processes.
* Ensure that Program Officials and/or System Owners understand and appropriately address risks, especially interconnectivity with other programs and systems outside their control.
* Review and evaluate the Information Security Program at least annually.
* Ensure that an IT Security Performance Metrics Program is developed, implemented, and funded.
* Report to the Secretary on matters relating to the security of HUD

IT systems.
* Continuously strengthen the Information Security Program.
* Ensure that adequate resources are provided for the Information Security Program.
* Direct that all IT security requirements be followed.
* Accept responsibility for the Information Security Program successfully meeting all federal regulations.
* Ensure overall program success.

2.3 Chief Information Security Officer

The Chief Information Security Officer (CISO) reports directly to the CIO on matters pertaining to IT security within HUD. The CISO will perform the following duties:

* Serve as the departmentwide principal advisor on IT security matters.
* Issue department-wide IT security policy, guidance, and architecture requirements for all HUD IT systems and networks and provide oversight to ensure these policies are implemented.
* Serve as the principal departmental liaison with organizations outside HUD for matters relating to IT security.
* Review and approve the processes, techniques, and methodologies planned for use in certifying and accrediting HUD IT systems. These include security test and evaluation plans, contingency plans, and risk assessments.
* Carry out CISO responsibilities under FISMA.
* Possess the professional qualifications, including training and experience, required to administer the functions described.
* Head an office with the mission and resources required to assist in ensuring HUD compliance.
* Develop and maintain a HUD Information Security Program.
* Direct HUD's day-to-day management of the Information Security Program.
* Coordinate all security-related interactions among Program Offices involved in the Information Security Program, as well as those external to HUD.
* Support Information System Security Officers (ISSO) and participate in the selection of qualified staff from the Program Offices.
* Serve as a member in the Technology Investment Board Working Group.

2.4 Information System Security Officer

An ISSO shall be appointed in writing by the appropriate Program Official for each general support system and major application. The ISSO can be either a government employee or an appropriately cleared support contractor. The ISSO is responsible for ensuring that management, operational, and technical controls for securing IT systems belonging to the Program Office are in place and followed. The ISSO will perform the following functions for the Program Office:

* Serve as the principal Point of Contact (POC) for all matters pertaining to the security of the IT systems for which the ISSO is responsible.
* Oversee the preparation of security plans, such as those required for C&A in coordination with the System Owner.
* Periodically review computer systems and networks to ascertain if changes have occurred that could adversely affect security.
* Ensure that system users receive initial computer security indoctrination and annual follow-on training, as required by applicable directives.
* Enforce an access control policy by which only authorized persons

can gain access to HUD IT systems and networks.
* Immediately report any security violation, attempt to gain unauthorized access to sensitive data, virus infection, or other event affecting the security of HUD systems and networks to the appropriate Computer Security Incident Response Center (CSIRC).
* Enforce the capability to track user activity on a system and report any discrepancies or misuse of automated resources.
* Manage the IT Security Metrics Program for the IT system. Collect and analyze data and coordinate with the CISO, as appropriate.
* Implement IT security policies as directed by, and in coordination with, higher authority.
* Attend required role-based security training.

An ISSO can be assigned to more than one general support system or major application.

2.5 Contracting Officer, Government Technical Monitor, and Government Technical Representative

Contracting Officers, Government Technical Monitors (GTM), and Government Technical Representatives (GTR) are responsible for ensuring that security is properly and adequately addressed as part of system acquisition and other contracting activities.

Specifically, these individuals will ensure that:
* New contracts include appropriate language and clauses to enforce HUD IT security policy and that existing contracts include appropriate language when modified.
* Any security clauses are developed and used in accordance with Departmental procurement policy, the HUD Acquisition Regulation (HUDAR) and Federal Acquisition Regulation (FAR).
* All new or modified HUD contracts include a clause requiring IT security awareness training and, where appropriate, role-based training for specific job categories with security responsibilities.
* All new or modified HUD contracts include a clause requiring contractor compliance with HUD computer security incident identification and reporting policy and procedures.
* IT security functional and assurance requirements are incorporated in information system procurement documents in accordance with HUD IT security policy.
* Contractors and subcontractors provide copies of their internal IT security plans and procedures to the CISO upon request.
* Existing and future contracts include requirements to have qualified security representatives (e.g., CISO, ISSO, or other designated HUD Program Office personnel) conduct site surveys at non-HUD facilities.

2.6 Help Desk

The help desk staff will:
* Assist HUD employees in technical security matters.
* Recognize and report security incidents to HUD CSIRC, engage resources for corrective action, and assist users in recovery.

2.7 Physical Security/Facilities Group/Security Officer

This generic title is used to identify the person or persons responsible for the physical security of the facility and the person or persons responsible for issuing badges and conducting required background checks for employees and contractors. In addition, the title is generic to cover outsourced computer services and operations.

The physical security staff and security officer will:
* Develop and enforce appropriate physical security controls.
* Identify and address the physical security needs of computer

installations, office environments, and backup installations.
* Process and maintain personal background checks and security clearance records.
* Issue HUD Identification (ID) badges to employees and contractors in accordance with HSPD-12.

2.8 Deputy Chief Information Officer for Information Technology Operations

The Deputy CIO for IT Operations will:
* Monitor security technology developments and evaluate their usefulness for, or impact upon, HUD mission, architecture, and operations.
* Direct IT contingency planning.
* Work with the Program Offices, functional managers, and System Owners on technology and contingency planning issues.
* Own and secure the IT infrastructure (e.g., general support systems) that provides shared services across Program Offices.

2.9 Program Offices/System Owners

Program Offices, or System Owners, use IT to help fulfill the business requirements necessary to achieve the mission needs within their program area of responsibility. As such, they are responsible for the successful operation of IT systems within their program area and are ultimately accountable for the security of the IT systems and programs under their control. The Office of the Chief Information Officer is the Program Office responsible for most General Support Systems at HUD; the Deputy CIO for IT Operations is the System Owner for such systems. The Program Offices/System Owners will:
* Work closely with the CIO and other program and IT managers to ensure a complete understanding of risks, especially the increased risks resulting from interconnectivity with other programs and systems over which the Program Offices have little or no control.
* Prepare information system security plans and risk assessments for information systems under their purview.
* Ensure information systems under their purview are certified and accredited.
* Review, in consultation with the CISO, the IT system security within their program area at least annually.
* Manage the procurement and operation of their Program Office information systems.
* Assure adherence to information security policy in the design and operation of application systems.
* Coordinate with the Deputy CIO for IT Operations and the CISO on security matters involving HUD information architecture, as a whole.

2.10 HUD Managers, Supervisors, and Employees

All HUD personnel and support contractors who have been authorized access to sensitive data are responsible for protecting that data. These responsibilities include the following:
* Comply with IT security policy and apply its principles to daily work activities.
* Enforce IT security policy and ensure that employees and contractors comply with IT policies and procedures.
* Assume accountability for protecting sensitive information under their control in accordance with this policy.
* Attend annual IT Security Awareness training.
* Attend required role-based security training-pertains to those having a security-related role (e.g., system and network administrators).
* Report IT security incidents (e.g., virus and malicious code

attacks) to the appropriate CSIRC according to established procedures.
* Cooperate with CSIRC Team members.
* Cooperate with Information Security Program representatives or other designated HUD Program Office personnel during security compliance reviews at HUD Program Office facilities and site surveys at non-HUD facilities.
* Ensure that IT security metrics data are collected in accordance with direction from the CISO and ISSO-Managers/Supervisors.
* Understand and comply with HUD policies, standards, and procedures regarding the protection of sensitive HUD information assets.

2.11 Authorizing Official

The Authorizing Official (AO) is a senior government management official with the authority to formally assume responsibility for operating an IT system at an acceptable level of risk. AOs control personnel, operations, maintenance, and budgets for their systems or field sites; therefore, AOs shall control the resources necessary to mitigate risks. An AO shall be assigned to each general support system and major application. The AO shall be a Senior Official who is the Program Assistant Secretary, Deputy Assistant Secretary, or equivalent Program Head.

The AO may assign a designated representative to act on the AO's behalf and be empowered to make certain decisions with regard to the planning and resourcing of security C&A activities, the acceptance of system security plans, and the determination of risk to agency operations, agency assets, and individuals. The only activity the AO cannot delegate is the security accreditation decision and signing the associated accreditation decision letter (i.e., the acceptability of risk to the agency).

AOs are responsible for the following:
* Reviewing and approving the corrective actions necessary to mitigate residual risks.
* Approving/disapproving system accreditation.
* Terminating system operations if security conditions warrant such action.

An AO can be responsible for more than one general support system or major application.

2.12 Certification Agent

A Certification Agent is assigned to each HUD IT system by an appropriate department-level official. Normally, the CISO is designated as the Certification Agent for all IT systems under the department's control.

To preserve the impartial and unbiased nature of security certification, the Certification Agent should be in a position that is independent from individuals directly responsible for information system development and day-to-day system operations. The Certification Agent should also be independent of those individuals responsible for correcting security deficiencies that are identified during security certification.

Certification Agents must be government employees and must be designated in writing at the department level. Designation letters shall be signed by the appropriate Under Secretary or Program Office Head. For each IT system, the Certification Agent shall:
* Ensure that a risk analysis is performed, that required C&A activities are completed, and that the results are documented.
* Prepare a Security Evaluation Report that clearly documents residual risks on the status of the certification for the AO.

A Certification Agent can be responsible for more than one general support system or major application.

3.0 MANAGEMENT POLICIES

3.1 Basic Requirements

In order to ensure the security of HUD information resources, basic security management principles must be followed. These principles are applicable throughout the department and form the cornerstone of the Information Security Program.

HUD Policya. Every HUD computing resource (e.g., desktops, laptops, servers, portable electronic devices, Commercial off-the-Shelf [COTS] software packages, and applications) shall be individually accounted for as part of a recognized information system inventory. The Office of Administration and Management Services (OAMS) shall maintain inventory accountability for all systems hardware and microcomputers with an acquisition cost of $500 or more. The Deputy CIO for IT Operations, in coordination with the Inspector General (IG), shall maintain a current system inventory for all commercial software and application systems used by HUD to process, store, and/or transmit information. This inventory shall be updated once a year.b. Program Offices/System Owners shall prepare and maintain an active and effective Information Security Plan for each HUD information system under their purview. The Information System Security Plan is required prior to the start of certification and accreditation and it shall be reviewed and updated, if needed, once a year.c. Program Offices shall designate an ISSO for every HUD information system under their purview.d. Program Offices/System Owners shall conduct a privacy impact assessment on all systems under their purview that process personally identifiable information in accordance with OMB Memorandum 03-22 and the E-Government Act.e. Program Offices/System Owners shall apply all mandated Health Insurance Portability and Accountability Act (HIPAA) Privacy and Security regulations to all systems under their purview that process personal health information.

3.1.1 Information and Information System Categorization

The FIPS Pub 199, Standards for Security Categorization of Federal Information and Information Systems, was published in February 2004. This publication is the mandatory standard for categorizing the sensitivity associated with all federal systems except those that deal with national security systems.
FIPS Pub 199 provides federal departments with a more detailed categorization of their information assets than was recognized under the Computer Security Act of 1987. This publication distinguishes among low, moderate, and high sensitivity categories, and deals explicitly with integrity, availability, and confidentiality as security goals. These categories correspond to different degrees of potential impact that a security incident may have on a department's mission, assets, legal responsibilities, functions, or individuals.
The NIST SP 800-60, Guide for Mapping Types of Information and Information Systems to Security Categories, provides guidance on assigning sensitivity categories to information systems.
..TD:

HUD Policya. Program Officials shall include IT security requirements in their capital planning and investment business cases in accordance with NIST SP 800-65, Integrating IT Security into the Capital Planning and Investment Control Process.b. Program Officials shall ensure that IT security requirements are adequately funded and documented in accordance with current OMB budgetary guidance and NIST SP 800-65.c. The CISO shall certify in writing that adequate security funding is included for all IT infrastructure projects, as appropriate, for the projects' System Development Life Cycle (SDLC) phase.d. The Technology Investment Board Executive Committee shall not approve any capital investment in which the IT security requirements are not adequately defined and funded.

3.3 Contractors and Outsourced Operations

Computer security requirements must be incorporated in contractual documents that involve the acquisition, development, and/or operation and maintenance (O&M) of computer resources. These requirements must be applied at the beginning of a project or acquisition and in all follow-on contracts or purchasing agreements involving the acquisition of computer resources. Computer resources include hardware, software, maintenance, and other associated IT products and services.

The use of contractors is essential to the success of HUD. Contractors fill a vital role in the daily operations of the department and they too have a responsibility to protect the information they process. To ensure the security of the information in their charge, contractors must adhere to the same rules and regulations as government employees.

HUD Policy

a. The Office of Procurement and Contracts (OPC) and Contracting Officers (CO) shall ensure that all solicitation documents, SOWs, and applicable contract vehicles identify and document the specific security requirements for IT services and operations that are required of the contractor.

The security requirements shall include how sensitive information is to be handled and protected at the contractor's site. The requirements shall apply to any information stored, processed, or transmitted using the contractor's computer systems, as well as background investigations, clearances, and/or required facility security.

The SOWs and contracts shall require that at the end of the contract, the contractor must return all information and IT resources provided during the life of the contract and must certify that all HUD information has been purged from any contractor-owned system used to process HUD information.

b. OPC and COs shall ensure that all solicitation documents, SOWs, and applicable contract vehicles contain a statement requiring contractors to adhere to HUD IT security policies.

c. The CISO and Program Offices that outsource IT security services shall do so in accordance with NIST SP 800-35, Guide to Information Technology Security Services.

d. Program Offices/System Owners shall conduct reviews in accordance with NIST SP 800-26, Security Self-Assessment Guide for Information Technology Systems, and NIST SP 800-53, Recommended Security Controls for Federal Information Systems, once a year to ensure that contract IT security requirements are implemented and enforced for systems under their purview.

3.4 Performance Measures and Metrics

Security metrics are collected measures of the adequacy of in-place

HUD security policies, procedures, and controls. At several organizational levels, the routine collection and review of security metrics help identify new security goals and justify investment in them. NIST SP 800-55, Security Metrics for Information Technology Systems, July 2003, provides guidance in the identification and use of security metrics. NIST prescribes the use of readily obtainable quantifiable measures that are capable of repeatable collection to measure progress toward defined security goals. NIST 800-55 defines security metrics of three types:

1. Implementation metrics-used to evaluate compliance with security policy
2. Effectiveness metrics-used to evaluate the effectiveness of security services
3. Impact metrics-used to measure the effect of security events on business or mission

HUD Policy

a. The CIO shall ensure that development, adequate resource assignment, and effective operations of the HUD Security Metrics Program are in accordance with NIST SP 800-55, Security Metrics for Information Technology Systems.

b. The CIO, in conjunction with the CISO, shall work with Program Offices, System Owners, and other personnel with information security responsibilities to assure understanding of and compliance with the Metrics Program and to define and track suitable performance measures.

c. Program Offices shall provide the CISO with semiannual data on their progress in implementing IT security performance measures.

3.5 Critical Infrastructure Protection

Critical Infrastructure Protection (CIP) is concerned with providing and maintaining adequate levels of security and redundancy to assure the performance of a minimal set of government and human-related services vital to the protection of people, the stability of the national economy, and the security of the nation. Homeland Security Presidential Directive (HSPD) 7, Critical Infrastructure Identification, Prioritization, and Protection, dated December 17, 2003, stipulates that the national goal is to assure that any interruption or manipulation of these critical national infrastructures is brief, infrequent, manageable, geographically isolated, and minimally detrimental to the welfare of the United States. EO 13231 and its amendments (i.e., EO 13284, EO 13286, and EO 13316), Critical Infrastructure Protection in the Information Age, reaffirms the need to take continual actions to secure information systems, emergency preparedness communications, and physical assets. It is HUD's policy to have in place a comprehensive and effective program and methodology to identify and protect HUD's national critical assets.

HUD Policy

a. The CIO, in coordination with the Program Offices, shall identify all critical assets in accordance with HSPD 7, Critical Infrastructure Identification, Prioritization, and Protection, to determine the interdependencies of these critical assets and develop and implement a CIP Risk Management Plan to ensure that these assets are adequately protected.

b. The CISO shall conduct yearly vulnerability assessments of IT resources that have been identified as part of HUD's critical infrastructure.

c. In the event that the primary and/or alternate telecommunications services are provided by a wireline carrier, the Deputy CIO for IT Operations shall request Telecommunications Service Priority (TSP) for all telecommunications services used for national security emergency preparedness.

3.6 Information Technology Contingency Planning

Information technology contingency planning refers to the interim measures needed to recover IT services following an emergency or system disruption. Interim measures may include the relocation of IT systems and operations to an alternate site, the recovery of IT functions using alternate equipment, or the performance of IT functions using manual methods.

The IT contingency planning is an integral part of CIP and COOP planning; therefore, this policy supports CIP and COOP. The planning is also closely related to the Business Impact Analysis (BIA) portion of COOP. The BIA identifies, among other things, the impact on business-function missions, if the system is unavailable for a specific amount of time. The IT Contingency Plan will consider the CIP, COOP Plans, and BIAs in establishing processing priorities.

HUD Policy

a. The CISO shall develop, document, and maintain a standard HUD-wide process for IT contingency planning in accordance with NIST SP 800-34, Contingency Planning Guide for Information Technology Systems.

b. Program Offices/System Owners shall develop contingency plans for information systems under their purview in accordance with NIST SP 800-34. For systems rated moderate or high, Program Offices/System Owners shall coordinate with the Program Office responsible for CIP and COOP.

c. Program Offices/System Owners shall review contingency plans once a year, update them, and communicate any changes to the Program Office responsible for COOP and CIP, if applicable.

d. Program Offices/System Owners shall ensure that all personnel involved in IT contingency planning efforts are identified and trained in the procedures and logistics of IT contingency planning and implementation for systems under purview rated moderate or high. Refresher training shall be provided annually. For systems rated high, the training shall include simulated events.

e. Program Offices/System Owners shall ensure that plans for systems rated moderate or high are tested/exercised at least annually. Testing should be coordinated with elements responsible for COOP, CIP, and incident response. For systems rated high, the Program Offices/System Owners shall ensure testing at the alternate processing site.

f. The Deputy CIO for IT Operations shall provide an alternate site for storing system backup information. The alternate site must be geographically separated from the primary storage site for backup information of systems rated moderate or high. For systems rated high, the storage site shall:

Be configured to facilitate timely and effective recovery operations

Identify potential accessibility problems in the event of an area-wide disruption or disaster and outline explicit mitigation actions

g. The Deputy CIO for IT Operations shall provide an alternate processing site for systems rated moderate or high and ensure that the equipment and supplies required to resume operations are either

available at the alternate site or contracts are in place to support delivery to the site. The alternate site shall:

Be geographically separated from the primary processing site

Be reviewed to identify potential accessibility problems in the event of an area-wide disruption or disaster and outline explicit mitigation actions

Have priority-of-service provisions in accordance with HUD's availability requirements

For systems rated high, the site shall be fully configured to support a minimum required operational capability and ready to use as the operational site.

h. The Deputy CIO for IT Operations shall provide for primary and alternate telecommunications services to support systems rated moderate and high. The Deputy CIO for IT Operations shall also initiate the necessary agreement to permit the resumption of system operations for critical business within 24 hours when primary telecommunications are unavailable. The Deputy CIO for IT Operations shall ensure that:

Agreements contain priority-of-service provisions in accordance with HUD's availability requirements

Alternate service does not share a single point of failure with the primary service

For systems rated high, the Deputy CIO for IT Operations shall ensure that:

Providers of alternate sites are sufficiently separated from primary service providers so they are not susceptible to the same hazards

Providers of primary and alternate services have adequate contingency plans

i. The Deputy CIO for IT Operations shall ensure that HUD has mechanisms with supporting procedures to allow the information system to be recovered and reconstituted to the systems original state after a disruption or failure. For systems rated high, the Deputy CIO for IT Operations shall ensure that the systems are fully recovered and reconstituted as part of the contingency plan test.

3.7 System Development Life Cycle

All federal information systems, including operational systems, systems under development, and systems undergoing modification or upgrade, are in some phase of what is commonly referred to as the SDLC. Many activities during a system's life cycle have cost, schedule, and performance implications. In addition to the functional requirements levied on an information system, security requirements must also be considered. When fully implemented, the information system must be able to meet its functional requirements and do so in a manner that is secure enough to protect agency operations, assets, and individuals.

In accordance with the provisions of FISMA, agencies are required to have an agency-wide Information Security Program and that program must be effectively integrated into the SDLC.

HUD Policy

a. Program Offices/System Owners shall ensure that security is integrated into the SDLC from IT system inception to system disposal through adequate and effective management, personnel, operations, and technical control mechanisms in accordance with NIST SP 800-64, Security Considerations in the Information System Development Life Cycle.

b. Program Offices/System Owners shall ensure information systems

that have been rated moderate or high are designed and implemented using security engineering principles in accordance with NIST SP 800-27 Rev A, Engineering Principles for Information Technology Security (A Baseline for Achieving Security).

c. Program Offices/System Owners shall ensure information systems that have been rated moderate or high physically or logically separate user interface services (e.g., public web pages) from information storage and management services (e.g., database management). Separation may be accomplished using different computers, different central processing units, different instances of the operating system, different network addresses, combinations of these methods, or other methods as appropriate.

3.8 Configuration Management

Configuration Management's (CM) primary concern is managing the configuration of all hardware and software elements of IT systems and networks and the security implications when changes occur. The initial configuration of the system or network must be documented in detail and all subsequent changes to any components must be controlled through a complete and robust CM process. Configuration Management has security implications in three areas to ensure:

* The configuration in which the system or network is actually installed and operated is consistent with the one under which its security C&A was performed.
* Any subsequent changes have been approved, including an analysis of any potential security implications.
* All recommended and approved security patches are properly installed.

HUD Policy

a. Program Offices/System Owners shall prepare Configuration Management Plans for all IT systems and networks under their purview. The plan must include a baseline configuration. For moderate to high-impact systems, the system shall use automated mechanisms to maintain an up-to-date, complete, accurate, and readily available baseline configuration. The baseline is updated during installations.

b. Program Offices/System Owners shall establish, implement, and enforce change management and CM controls on all IT systems and networks under their purview. Changes to the information system must be documented and they must include emergency change procedures. For high-impact systems, the system shall use automated mechanisms to:

  Document proposed changes
  Notify appropriate approval authorities
  Highlight approvals that have not been received in a timely manner
  Inhibit changes until necessary approvals are received
  Document completed changes

c. IT security patches shall be installed in accordance with Configuration Management Plans or from direction of higher authorities.

d. Program Offices/System Owners shall monitor and audit changes to information systems under their purview and conduct security impact analysis as required by NIST SP 800-37 and check the security features of the system to ensure the features are still functioning properly.

e. Program Offices/System Owners shall ensure that changes to the information system are restricted to a limited number of personnel who require access for their job responsibilities. For high-impact systems, the system shall use an automated mechanism to enforce the

restrictions and provide audit information.
f. Program Offices/System Owners shall ensure that security settings have been set to their most restrictive values consistent with operational requirements. For COTS packages, Program Offices/System Owners shall consult NIST SP 800-70, Security Configuration Checklists Program for IT Products for the Configuration Checklist and configure the system accordingly. For high-impact systems, the system shall use automated mechanisms to centrally apply and verify configuration settings.
g. Program Offices/System Owners of systems that have been rated high shall ensure that their software and information are protected against unauthorized changes. The Program Offices/System Owners shall use automated tools to monitor the integrity of such information and software. Acceptable methods for COTS packages include, but are not limited to, parity checks, cyclical redundancy checks, and cryptographic hashes.
h. Program Offices/System Owners of systems under development that have been rated high shall ensure that the system developer creates and implements a configuration management plan that controls changes to the system during development, tracks security flaws, requires authorization of changes, and provides documentation of the plan and its implementation.
i. Program Offices/System Owners of systems under development that have been rated moderate or high shall ensure that the system developer creates a security test and evaluation plan, implements the plan, and documents the results. Developmental security test results should only be used when no security relevant modifications of the information system have been made subsequent to developer testing and after selective verification of developer test results.

3.9 Risk Management and Risk Assessment

Risk assessment is a process of identifying system security risks and determining the probability of occurrence, resulting impact, and additional safeguards that would mitigate this impact. Risk management is a process that allows Program Officials to balance the operational and economic costs of protective measures to achieve gains in mission capability by protecting the IT systems and data that support their organization's missions. It is the total process of managing risks to agency operations, agency assets, or individuals resulting from the operation of an information system. It includes risk assessment and Cost-Benefit Analysis (CBA); as well as the selection, implementation, testing, and security evaluation of safeguards. This overall system security review considers both effectiveness and efficiency, including the impact on the mission and constraints due to policy, regulations, and laws.

As a preliminary risk assessment, Program Offices/System Owners shall ensure that all systems and data under their purview have been categorized in accordance with FIPS 199, Standards for the Security Categorization of Federal Information and Information Systems.

HUD Policy

a. Program Offices/System Owners shall ensure that all systems under their purview have been subjected to a current risk assessment in accordance with the NIST SP 800-30, Risk Management Guide for Information Technology Systems. Risk assessments are required prior to the start of C&A.
b. Program Offices/System Owners shall conduct a risk assessment every three years and when a significant change is planned for any system under their purview.

c. Program Offices/System Owners shall conduct an "e-authentication risk assessment" of the transactional systems under their purview that provide government services using the Internet. The risk assessment shall be conducted in accordance with OMB guidance under OMB-04-04,
E-Authentication Guidance for Federal Agencies.

3.10 Certification and Accreditation

Security accreditation is the official management decision given by a senior agency official to authorize the operation of an information system and to explicitly accept the risk to agency operations, agency assets, or individuals based on the implementation of an agreed-upon set of security controls. By accrediting an information system, the Authorizing Official accepts responsibility for the security of the system and is fully accountable for any adverse impacts to the agency if a breach of security occurs.

Security certification is a comprehensive assessment of the suitability and effectiveness of management, operational and technical security controls in an information system. This assessment is made in support of security accreditation to determine the extent to which the controls are being implemented correctly, operating as intended, and producing the desired outcome with respect to meeting system security requirements. The results of the security certification are used to reassess the risks and update the system security plan, thus providing the factual basis for an AO to render a security accreditation decision.

Completing a security accreditation ensures that an information system will be operated with appropriate management review, that there exists ongoing monitoring of security controls, and that reaccreditations occurs periodically in accordance with federal or HUD policy, including when there is a significant change to the system or its operational environment.

HUD Policy

a. Program Offices/System Owners shall follow the guidelines contained in NIST SP 800-37, Guidelines for the Security Certification and Accreditation of Federal Information Technology Systems, in certifying and accrediting their information systems.

b. Program Offices/System Owners shall ensure that whenever changes are made to IT systems, networks, or to their physical environment, interfaces, or user-community makeup, the impact on the security of the information processed is reviewed via a documented security-impact analysis as required by NIST SP 800-37.

c. Program Offices/System Owners shall ensure that systems are certified and accredited at their initial operating capability every three years thereafter and whenever a significant change occurs in accordance with NIST 800-37.

d. Existing accreditations completed before the issuance of this policy shall remain in effect if the accreditation complied fully with the policy in effect at the time of accreditation, no significant deficiencies have been identified, and the system configuration has not changed since accreditation.

e. Program Offices shall update their POA&Ms on a quarterly basis for systems under their purview as required by OMB.

f. Program Offices/System Owners shall conduct an annual security review of systems under their purview in accordance with NIST SP 800-26, Security Self-Assessment Guide for Information Technology Systems, and NIST SP 800-53, Recommended Security Controls for Federal Information Systems. The results of such reviews shall be

included in the annual FISMA report to OMB.
g. Program Offices/System Owners shall conduct vulnerability assessments and/or security testing to identify vulnerabilities in IT systems under their purview. These assessments shall be conducted yearly and when significant changes are made to the IT systems.
h. Program Offices/System Owners shall authorize and monitor all connections between systems under their purview and other systems outside the accreditation boundary. The connection(s) shall be documented in an Interconnection Security Agreement in accordance with NIST SP 800-47, Security Guide for Interconnecting Information Technology Systems.
i. The CISO shall implement a standard C&A methodology for all HUD systems.
j. Program Offices/System Owners shall use this methodology for all C&As.

3.11 Incidents, Violations, and Disciplinary Action

Individual accountability is a cornerstone of an effective security policy. If individuals are not held accountable for their actions, there is little incentive for compliance. Program Office heads are responsible for holding personnel accountable for intentional transgressions and for taking corrective actions when security incidents and violations occur. Corrective action does not necessarily mean disciplinary action. Sometimes remedial training is more appropriate. Each Program Office must determine how best to address each individual case.

An incident is a violation or imminent threat of violation of information security policies, acceptable use policies, or standard computer security practices. Incidents may result from intentional or unintentional actions. Inappropriate uses of HUD computer resources are also considered security incidents.

HUD Policy

a. HUD employees may be subject to disciplinary action for failure to comply with HUD security policies, whether or not the failure results in criminal prosecution. IT security-related violations are addressed in U.S. Department of Housing and Urban Development Ethics Letters 92-1, Standards of Conduct and Principles of Ethical Service for Federal Employees.
b. HUD contractors and external users who fail to comply with department security policies shall be subject to having their access to HUD IT systems and facilities terminated, whether or not the failure results in criminal prosecution.
c. Any person who improperly discloses sensitive information shall be subject to criminal and civil penalties and sanctions under a variety of laws (e.g., the Privacy Act).

4.0 OPERATIONAL POLICIES

4.1 Personnel

HUD systems face threats from many sources, including the actions of HUD employees, external users, and contractor personnel. The intentional and unintentional actions of these individuals can potentially harm or disrupt HUD systems and their facilities. These actions can result in the destruction or modification of the data being processed, denial of service (DoS) to the end users, and unauthorized disclosure of data, potentially jeopardizing HUD's mission. Therefore, it is highly important that stringent safeguards be taken to reduce the risk associated with these types of threats.

HUD Policy

a. Program Offices shall designate the position sensitivity level for all government positions that use, develop, operate, or maintain IT systems under their purview and shall determine risk levels for each contractor position in accordance with the Office of Personnel Management (OPM) policy and guidance. Position sensitivity levels and risk levels shall be reviewed periodically in accordance with OPM guidance.

b. Program Offices shall ensure that the incumbents of these positions have favorably adjudicated background investigations commensurate with the defined position's sensitivity levels. Screening shall be consistent with: (i) 5 Code of Federal Regulations (CFR) 731.106(a); (ii) OPM policy, regulations, and guidance; (iii) organizational policy, regulations, and guidance; (iv) FIPS 201 and its attendant SP 800-73 and 800-76; and (v) the criteria established for the risk designation of the assigned position.

c. Program Offices/System Owners shall ensure that no employee is granted access to HUD systems without having a favorably adjudicated Minimum Background Investigation (MBI), as defined in HUD's Personnel Security Program for systems under their purview.

d. Program Offices/System Owners shall ensure that no contractor employee is granted access to HUD systems under their purview without having a favorably adjudicated background Investigation, as defined in HUD's Handbook 732.3, Personnel Security/Suitability. Exceptions may be granted by the CISO.

e. Program Offices/System Owners shall ensure that no government employee is granted access to HUD systems processing sensitive information under their purview who is not a citizen of the United States. Exceptions may be granted at the Program Office level and must be reported to the CISO and the security officer.

f. Program Offices/System Owners shall ensure that no contractor employee is granted access to HUD systems processing sensitive information under their purview who is not a citizen of the United States, a national of the United States (see 8 U.S.C. 1408), or an alien lawfully admitted to the United States for permanent residence. Exceptions may be granted at the Program Office level and reported to the CISO and the security officer.

4.1.1 Rules of Behavior

Rules of behavior are part of a comprehensive program to provide complete information security guidelines. The rules of behavior establish standards of behavior in recognition of the fact that knowledgeable users are the foundation of a successful Information Security Program. These guidelines are established to hold users accountable for their actions and responsible for IT security.

HUD Policy

a. The CISO shall define generic rules of behavior for all IT systems.

b. Program Offices/System Owners shall define additional rules of behavior for all IT systems under their purview, when necessary.

c. ISSOs shall ensure that users of systems sign the rules of behavior and are given training regarding the rules of behavior and the disciplinary actions that may result if the rules are violated.

4.1.2 Access to Sensitive Information

To protect sensitive information and limit the damage that can result from accident, error, or unauthorized use, the principle of least privilege must be applied. The principle of least privilege requires that users be granted the most restrictive set of privileges (or lowest clearance) needed to perform authorized tasks (i.e., users should be able to access only the system resources needed to fulfill their job responsibilities).

The application of this principle ensures that access to sensitive information is granted only to those users with a valid need to know.

HUD Policy

a. Program Offices/System Owners shall ensure that users of IT systems supporting their programs have a validated requirement to access these systems.

b. Program Offices/System Owners shall ensure that users of IT systems under their purview have approved access requests prior to granting access to the systems.

4.1.3 Separation of Duties Policy

Separation of duties is designed to prevent a single individual from being able to disrupt or corrupt a critical security process. This separation is necessary for adequate internal control of sensitive IT systems.

HUD Policy

a. Program Offices/System Owners shall divide and separate duties and responsibilities of critical IT system functions among different individuals to minimize the possibility that any one individual would have the necessary authority or systems access to be able to engage in fraudulent or criminal activity.

4.1.4 Training and Awareness

A key objective of an effective Information Security Program is to ensure that all employees and contractors understand their roles and responsibilities and are adequately trained to perform them. HUD cannot protect the confidentiality, integrity, and availability of its IT systems and the information they contain without the knowledge and active participation of its employees and contractors in the implementation of sound security principles.

HUD Policy

a. The CISO shall establish an IT security awareness and training

program in accordance with NIST 800 SP 800-50, Building an Information Technology Security Awareness and Training Program. The program shall be consistent with CFR 930.301.
b. Program Offices/System Owners shall establish additional system-specific security training for sensitive systems under their purview, when necessary.
c. Program Offices/System Owners shall ensure that HUD personnel and contractors accessing HUD IT systems receive initial training in security awareness and accepted security practices as part of their orientation. They shall sign the rules of behavior and receive refresher training by May 31 of each year.
d. Program Offices/System Owners shall ensure that HUD personnel and contractors with significant security responsibilities (e.g., ISSOs and system administrators) receive annual specialized training specific to their security responsibilities. The level of training shall be commensurate with the individual's duties and responsibilities and promote a consistent understanding of the principles and concepts of IT system security.
e. Program Offices shall maintain training records that include the individual names and positions, types of training received, and cost of training.
f. Unless a waiver is granted by the CISO, user accounts and access privileges, including access to email, will be disabled for those HUD employees who have not received annual refresher training.
g. Program Offices shall prepare and submit an IT Security Professional Training Plan to the CISO by September 1 of each year.
h. Program Offices shall prepare and submit awareness and training statistics semiannually to the CISO. These statistics shall include the (1) total number of personnel and the total number of personnel who received awareness training and (2) total number of IT security personnel and the total number who were trained.

4.1.5 Separation from Duty

This section addresses HUD's policy for an employee or contractor who terminates employment or transfers to another organization.

HUD Policy

a. Program Offices/System Owners shall implement procedures to ensure that system accesses are revoked or reassigned when HUD or contractor employees either change their employer or are reassigned to other duties. The procedures shall include:

Exit interviews

Process for returning all organizational information and system-related property (e.g., keys and ID cards)

Access by appropriate personnel to official records created by the terminated/transferred employee/contractor that are stored on organizational information systems

Formal notification to the facilities group or security officer

4.2 IT Physical Security

HUD security personnel and users must address physical security as an integral element in the effective implementation of an Information Security Program. Physical security represents the first line of defense against intruders and adversaries attempting to gain access to HUD facilities and or information systems.

4.2.1 General Physical Access

General physical access controls restrict the entry and exit of personnel from a protected area, such as an office building, data center, or room containing IT equipment. They include the protection of sensitive data and systems while in rest, as well as while away

from the protection of HUD facilities. These controls protect against threats associated with the physical environment. It is important to review the effectiveness of general physical access controls in each area during business hours and at other times. Effectiveness depends not only on the characteristics of the controls used but also on their implementation and operation.

Homeland Security Presidential Directive 12 mandates government-wide standard for secure and reliable forms of identification issued by the federal government to its employees and contractors (including contractor employees). Program Offices responsible for issuing ID badges at HUD shall consult FIPS 201 and its attendant SP 800-73 and SP 800-76 for specific guidance.

HUD Policy

a. The facilities group or security officer shall ensure that access to HUD buildings, rooms, work areas, and spaces is limited to authorized personnel. Controls shall be in place for deterring, detecting, monitoring, restricting, and regulating access to specific areas at all times.

b. The facilities group or security officer shall ensure that all visitors sign in and out when entering and leaving the facility. Visitor logs shall be reviewed at closeout, maintained on file, and available for further review for one year. Contractors' access shall be limited to those work areas requiring their presence. Records of their ingress and egress shall also be maintained for one year. For systems rated moderate or high, the maintenance and review of access logs shall use automated mechanisms.

c. For systems rated moderate or high, the facilities group or security officer shall ensure that all visitors are escorted.

d. For systems rated moderate or high, individuals within HUD shall employ appropriate security controls at alternate work sites in accordance with NIST SP 800-46, Security for Telecommuting and Broadband Communications. These individuals shall report security problems to HUD's Computer Security Incident Response Center (CSIRC).

e. Program Offices and users shall ensure that unattended laptops in offices are secured via a locking cable, locked office, or a locked cabinet or desk.

4.2.2 Facilities Housing Information Technology Assets

Facilities supporting large-scale IT operations (e.g., enterprise servers and telecommunication facilities) require additional environmental and physical controls as determined by a risk analysis. Section 4.2.1 provides policies for both general physical access and sensitive facilities. For facilities supporting large-scale IT operations, all of the following physical security controls also must be addressed. The risk assessment shall specifically document the rationale for not incorporating any such physical security controls.

HUD Policy

a. The Deputy CIO for IT Operations shall ensure that facilities processing, transmitting, or storing sensitive information incorporate physical protection measures. These facilities include data centers, wiring closets, server rooms at non-HUD facilities, contractor facilities housing HUD IT systems, and in some cases, areas designated as publicly accessible inside HUD facilities.

b. The facilities group or security officer shall ensure that lists of personnel authorized to access these facilities are current and shall issue appropriate credentials. Access shall be promptly removed for personnel no longer needing it.

c. The Official responsible for approving initial access to these

facilities shall review and approve access lists and authorization credentials once a year.
d. The facilities group or security officer shall control all access points with physical access devices and/or guards. Keys, combinations, and other access devices shall be secured and inventoried every six months and changed any time the keys are lost, combinations are compromised, or individuals are terminated or transferred.
e. The facilities group or security officer shall develop and implement procedures to ensure that only authorized individuals can reenter the facility after emergency-related events.
f. For systems rated moderate or high, the Program Offices/System Owners shall ensure that physical access to devices displaying information is controlled to prevent unauthorized disclosure.
g. The facilities group or security officer shall monitor physical access to detect and respond to incidents. Logs shall be reviewed daily for apparent security violations or suspicious activities and responded to accordingly. For systems rated moderate or high, the monitoring shall be in real-time for intrusion alarms and surveillance equipment. For systems rated high, the monitoring shall use automated mechanisms to recognize intrusions and to take appropriate action.
h. For systems rated moderate or high, the facilities group or security officer shall ensure that power equipment and cabling are protected from damage and destruction.
i. For specific locations within a facility containing concentrations of information system resources (e.g., data centers and server rooms), the facilities group or security officer shall provide for the capability of shutting off power to any IT component that may be malfunctioning (e.g., due to an electrical fire) or threatened (e.g., due to a water leak) without endangering personnel by requiring them to approach the equipment.
j. For specific locations within a facility containing concentrations of information system resources (e.g., data centers and server rooms), the facilities group or security officer shall maintain a redundant air-cooling system.
k. The facilities group or security officer shall provide short-term UPS to facilitate an orderly shutdown in the event of a primary power source loss.
l. The facilities group or security officer shall provide a long-term alternate power supply to maintain minimal operational capability for systems rated moderate or high in the event of an extended loss of the primary power source.
m. The facilities group or security officer shall provide automatic emergency lighting systems that activate in the event of a power outage or disruption and cover emergency exits and evacuation routes.
n. The facilities group or security officer shall provide fire suppression and detection devices/systems that can be activated in the event of fire. The devices/systems shall include, but are not limited to:
  Sprinkler systems
  Handheld fire extinguishers
  Fixed fire hoses
  Smoke detectors
o. For systems rated moderate or high, the facilities group or security officer shall provide fire suppression devices/systems that activate automatically in the event of fire.

p. For systems rated high, the facilities group or security officer shall provide fire suppression devices/systems that automatically notify any activation to the organization and emergency responders in the event of fire.
q. The facilities group or security officer shall ensure that facilities containing information systems monitor and maintain acceptable levels of temperature and humidity.
r. The facilities group or security officer shall ensure that the information systems contained in the facility are protected from water damage resulting from broken plumbing lines or other sources of water leakage by ensuring that master shutoff valves are accessible, working properly, and known to key personnel. For systems rated high, the shutoff shall use automatic mechanisms in the event of a significant water leak.
s. The facilities group or security officer shall ensure that the facility has procedures to control the entering and exiting of information system-related items and maintains appropriate records. Delivery and removal of these items shall be authorized by an appropriate HUD official. If possible, the delivery area shall be separate from the system and media library area.

4.3 Media Controls

Information resides in many forms and can be stored in many different ways. Media controls are protective measures specifically designed to safeguard electronic data and hardcopy information. This policy addresses the protection, marking, sanitization, production input/output, and disposal of media containing sensitive information. Media destruction and disposal should be accomplished in an environmentally approved manner. The National Security Agency (NSA) provides media destruction guidance at http://www.nsa.gov/ia/government/mdg.cfm.

Proper storage of hardcopy and magnetic media enhances protection against unauthorized disclosure. There are additional security risks associated with the portability of removable storage media. Loss, theft, or physical damage to disks and other removable media can compromise the confidentiality, integrity, or availability of the data contained in these devices.

HUD Policy

a. Program Offices/System Owners shall establish procedures to ensure that sensitive information in printed form or digital media cannot be accessed, removed, or stolen by unauthorized individuals.
b. Program Offices/System Owners and users shall ensure that all media containing sensitive information rated moderate or high is appropriately marked with the sensitivity of the information stored on the media. At a minimum, printed output that is not otherwise appropriately marked shall have a cover sheet and digital media shall be labeled with the distribution limitations, handling caveats, and applicable security markings, if any, of the information. Systems rated high shall use an automated marking mechanism.
c. Program Offices/System Owners and users shall control access to and securely store all information system media (i.e., both paper and digital) containing sensitive information rated moderate or high, including backup and removable media, in a secure location when not in use.

The following policy statements apply only to media that contain information that has been rated moderate or high.

d. Program Offices/System Owners shall ensure that any sensitive information stored on media that will be surplused or returned to the

manufacturer shall be purged from the media before disposal.
e. Disposal shall be performed using approved sanitization methods in accordance with NIST SP 800-36, Guide to Selecting Information Security Products.
f. Program Offices/System Owners shall maintain records certifying that such sanitization was performed.
g. Program Offices/System Owners shall establish procedures to ensure that sensitive information stored on any media is transferred to an authorized individual upon the termination or reassignment of an employee or contractor.
h. Program Offices/System Owners shall ensure that sensitive information is purged from the hard drives of any workstation or server returned to the equipment surplus pool or transferred to another individual.
i. Program Offices/System Owners shall ensure that media (e.g., paper, diskettes, and removable disk drives) containing sensitive information is destroyed in such a manner that all sensitive information on that media cannot be recovered by ordinary means. Examples of appropriate methods are crosscut shredders, degaussing, and approved disk-wiping software.
j. Program Offices/System Owners shall maintain records certifying that such destruction was performed.
k. Program Offices/System Owners shall establish procedures to ensure that sensitive information in printed form or digital media can only be picked up, received, transferred, or delivered to authorized individuals.
The following policy statements apply only to media that contain information that has been rated high.
l. Program Offices/System Owners shall ensure that access to media storage areas is controlled through guard stations or automated mechanisms that ensure only authorized access. All access and access attempts shall be audited.

4.4 Data Communications

4.4.1 Telecommunications Protection Techniques

Extreme caution should be exercised when telecommunications protection techniques (e.g., protective distribution systems) are being considered as alternatives to the use of encryption. While such technologies may represent a lower-cost approach, they may not provide an adequate level of protection.
The FIPS 199 security category (for integrity) of the information being transmitted should guide the decision on the use of cryptographic mechanisms. NSTISSI No. 7003 contains guidance on the use of Protective Distribution Systems.
HUD Policy
a. Program Offices/System Owners shall ensure that the integrity of the information in systems under their purview is protected during transmission. For systems rated high, the system shall employ cryptographic mechanisms to ensure recognition of changes to information during transmission, unless adequately protected by alternative physical measures (e.g., protective distribution systems).
b. Program Offices/System Owners shall ensure that the confidentiality of the information in systems under their purview is protected during transmission. For systems rated high, the system shall employ cryptographic mechanisms to prevent unauthorized disclosure of information during transmission, unless otherwise protected by adequately physical measures (e.g., protective

distribution systems).

4.5 Wireless Communications

Wireless communications are inherently insecure. Program Offices/System Owners implementing wireless capabilities must ensure that the transmission and storage of sensitive information are protected from compromise.

4.5.1 Wireless Local Area Networks

HUD Policy

a. The CISO shall approve the implementation and use of all Wireless Local Area Networks (WLAN) and wireless Access Points (AP) at a specified risk level and only after they have been certified and accredited.

b. The Deputy CIO for IT Operations shall ensure that all WLANs and WAPs have been configured in accordance with NIST SP 800-48, Wireless Network Security.

c. The Deputy CIO for IT Operations shall implement encryption and strong identification and authentication (e.g., Extensible Authentication Protocol with Wi-Fi Access Protection (WAP) or IEEE 802.11i) on WLANs and APs that have been rated moderate or high.

d. The CISO shall scan for rogue access points on HUD's network annually.

4.6 Hardware and Software

This section addresses the use and maintenance of computer equipment. It stresses the importance of individual accountability in protecting these resources. Equipment security encompasses workstations, laptops, other mobile computing devices, personally-owned equipment, and the maintenance of these items.

4.6.1 Workstations

All users must be instructed to log off or lock their workstations any time the workstations are left unattended. As an added precaution, users should also use a password-protected screensaver.

HUD Policy

a. All users shall ensure that their unattended workstations are either logged off or locked, or that a password-protected screensaver is used.

b. The Deputy CIO for IT Operations shall provide and implement password-protected screen savers on all workstations owned/leased by HUD. The screen saver shall automatically lock the workstation after ten minutes of inactivity. Program Offices/System Owners of systems rated moderate to high shall require that contractors and business partners who connect to the systems implement such a screen saver.

4.6.2 Copyrighted Software

Computer software purchased using HUD funds is HUD property and shall be protected as such. Only licensed and approved operating systems and applications may be used on HUD equipment.

HUD Policy

a. Program Offices/System Owners shall ensure that users abide by copyright and contract agreements related to HUD-provided software. For software and associated documentation protected by quantity licenses, the Program Offices/System Owners shall use tracking systems to control copying and distribution.

b. Program Offices/System Owners that use peer-to-peer file sharing technology on their information system shall control and monitor its use to ensure that this capability is not used for unauthorized distribution, display, performance, or reproduction of copyrighted work.

4.6.3 User-Installed Software/Downloads

User-installed software, including downloaded software, can contain viruses and other types of malicious code. In addition, such software can alter the HUD equipment configuration causing malfunctions and costly support calls. Users should be warned about such risks and instructed to refrain from installing any software on HUD equipment without proper approval.

HUD Policy

a. Users shall not install any software on HUD-owned or leased equipment without prior written approval from the Deputy CIO for IT Operations.

4.6.4 Personally-Owned Equipment and Software

Users shall not use personally owned equipment (e.g., laptop computers or personal digital devices [PDA]) or software to process, access, or store sensitive information. Such equipment also includes plug-in and wireless peripherals (e.g., Blackberry) that may employ removable media (e.g., CDs and DVDs), Universal Serial Bus (USB) flash (thumb) drives, external drives, and diskettes.

HUD Policy

a. Users shall not use personally-owned equipment and software to process, access, or store sensitive information without prior written approval from the Program Offices/System Owners.

b. Employees and contractors shall not connect equipment not owned or leased by HUD-to-HUD equipment or networks without prior written approval from the CISO.

c. The written approval shall include a terms and conditions statement that addresses at a minimum: (i) the types of applications that can be accessed from personally-owned information systems; (ii) the maximum FIPS 199 security category of information that can processed, stored, and transmitted; (iii) how other users of the personally-owned information system will be prevented from accessing federal information; (iv) the use of virtual private network (VPN) and firewall technologies; (v) the use of and protection against the vulnerabilities of wireless technologies; (vi) the maintenance of adequate physical security controls; (vii) the use of virus and spyware protection software; and (viii) how often the security capabilities of installed software are to be updated (e.g., operating system and other software security patches, virus definitions, firewall version updates, and spyware definitions).

4.6.5 Hardware and Software Maintenance

Program Offices/System Owners must be cognizant of the threats and vulnerabilities associated with hardware or software maintenance on IT systems. System maintenance requires either physical or logical access to the system. One of the most common methods hackers use to break into systems is through maintenance accounts that still have factory-set or easily guessed passwords. War-dialing techniques will also reveal maintenance ports that are not protected.

HUD Policy

a. Program Offices/System Owners shall confine access to system software and hardware to authorized personnel.

b. The Deputy CIO for IT Operations shall ensure that routine preventive and regular maintenance are performed on software and hardware according to manufacturer/vendor specifications and/or organizational requirements. For systems that have been rated moderate or high a log shall be maintained for such maintenance and include the following:

- Date and time of maintenance
- Name of individual performing the maintenance

Name of escort, if necessary
Description of maintenance performed
A list of equipment removed or replaced (including identification numbers, if applicable).

For systems rated high, the Deputy CIO for IT Operations shall use an automated mechanism to ensure that the maintenance is scheduled and conducted, as required.

c. The Deputy CIO for IT Operations shall ensure that an appropriate organizational official approves the removal of the information system or its components from the facility when repairs are necessary. The Deputy CIO for IT Operations shall ensure that the security features of the system are checked to ensure proper functioning when it is returned.

d. The Deputy CIO for IT Operations shall ensure that appropriate organization officials approve, control, and monitor the use of information system maintenance tools and maintain such tools on an ongoing basis.

e. The Deputy CIO for IT Operations shall ensure that maintenance ports are disabled by default and enabled only during maintenance.

f. The Deputy CIO for IT Operations shall ensure that the appropriate organizational officials approve, control, and monitor remotely executed maintenance and diagnostic activities. The Deputy CIO for IT Operations shall ensure that all sessions are terminated when remote maintenance is completed. If password-based authentication is used, the Deputy CIO for IT Operations shall ensure that passwords are changed following each maintenance service. For high-impact systems, the Deputy CIO for IT Operations shall ensure that logs for such activities are maintained and periodically reviewed.

g. The Deputy CIO for IT Operations shall ensure that only authorized individuals perform maintenance on information systems. If maintenance personnel need access to organizational information, they must be supervised by organizational personnel with authorized access to such information.

h. The Deputy CIO for IT Operations shall identify critical components that support systems rated moderate or high and ensure that maintenance support and parts are provided within 48 hours of failure.

i. The Deputy CIO for IT Operations shall ensure that all default vendor or factory-set administrator accounts and passwords shall be changed before installation or use on all systems owned or operated on behalf of HUD.

j. Program Offices/System Owners of information systems that have been rated high shall address the installation and use of remote diagnostic links in the system security plan.

k. The Deputy CIO for IT Operations shall ensure that remote diagnostic or maintenance services for information systems that have been rated high are only performed by a service or organization that implements for its own information system the same level of security as that implemented on the information system being serviced. If remote diagnostic or maintenance services are required from a service or organization that does not implement for its own information system the same level of security as that implemented on the system being serviced, the system being serviced is sanitized and physically separated from other information systems prior to the connection of the remote access line. If the information system cannot be sanitized (e.g., due to a system failure), remote maintenance is not allowed.

4.6.6 Personal Use of Government Office Equipment and HUD Information Systems/Computers

This section discusses HUD policies applicable to the personal use of government office equipment and HUD information systems. Policies governing personal use may be contained in several HUD management directives.

HUD Policy

a. HUD employees may use government office equipment and HUD information systems/computers for authorized purposes only. "Authorized use" includes limited personal use of HUD email and Internet services, so long as use does not interfere with official duties, cause degradation of network services, or violate the rules of behavior.

b. Contractors and other non-HUD employees are not authorized to use government office equipment or information systems/computers for personal use, unless limited personal use is specifically permitted by the governing contract or Memorandum of Agreement (MOA).

4.7 General IT Security

This section provides guidance in the areas of incident reporting, contingency planning, documentation, and backup procedures. It stresses the role of the user, as well as the security professional, in the implementation of the operational controls associated with these areas.

4.7.1 Security Incident and Violation Handling

Incidents can be accidental or malicious, can be caused by outside intruders or internal employees, and can cause significant disruptions to mission-critical business processes. These incidents can severely disrupt computer-supported operations, compromise the confidentiality of sensitive information, and diminish the integrity of critical data.

To help combat the disruptive short- and long-term effects of security incidents, direction from higher authority (e.g., OMB, FISMA, and Presidential directives) requires that each government agency implement and maintain a security incident reporting and handling capability.

The HUD Security Incident Reporting and Handling Program requires participation by all Program Offices/System Owners; thus, a CSIRC has been established. The CSIRC is the focal point for the implementation of HUD's incident response capability.

HUD Policy

a. The CISO shall establish and maintain a HUD CSIRC to prevent, detect, track, and respond to information security incidents and alerts in accordance with NIST SP 800-61, Computer Security Incident Handling Guide. Lessons learned from ongoing incident handling activities shall be incorporated into the procedures and implemented accordingly. For systems rated moderate or high, the CISO shall provide automated mechanisms to support the incident handling process.

b. Program Offices/System Owners of systems rated moderate or high shall ensure that security alerts, advisories, Intrusion Detection System (IDS) alerts, and vulnerabilities identified during vulnerability scans and penetration tests are tracked and responded to as security incidents.

c. The Deputy CIO for IT Operations shall test patches, service packs, and hot fixes for effectiveness and potential side effects prior to installation in accordance with NIST SP 800-40, Procedures for Handling Security Patches. The Deputy CIO for IT Operations

shall use automated mechanisms that require no user intervention to manage and install updates. The Deputy CIO for IT Operations shall employ an automated mechanism to determine periodically and upon demand the state of information system components with regard to flaw remediation.

d. The CSIRC, in conjunction with the Deputy CIO for IT Operations, shall provide a process to track and document information system security incidents on an ongoing basis. For systems rated high, the tracking of security incidents and the collection and analysis of incident information shall employ automated mechanisms.

e. Program Offices/System Owners shall ensure that personnel with incident response responsibilities receive training at least once a year. Incident response training for systems rated high shall incorporate simulated events to facilitate effective response by personnel in a crisis and employ automated mechanisms.

f. Program Offices/System Owners shall test the incident response capability for systems under their purview rated moderate or high once a year and document the test results. For high-impact systems the tests shall employ automated mechanisms.

g. ISSOs shall report significant computer security incidents to the CSIRC immediately upon identification and validation of the incident occurrence.

h. ISSOs shall report all incidents to the CSIRC in a Weekly Incident Report.

i. The CSIRC shall report significant computer security incidents to appropriate authorities, including the United States Computer Emergency Readiness Team (USCERT), upon identification and validation of the incident occurrence. The CSIRC shall use automated mechanisms to assist in the reporting of security incidents for systems rated moderate or high. The CSIRC shall report incident-related information to OMB, as required by FISMA.

j. The CSIRC, in conjunction with the Deputy CIO for IT Operations, shall provide users of information systems with support and assistance (e.g., help desk) for the handling and reporting of security incidents. For systems rated moderate or high, the CSIRC and the Deputy CIO for IT Operations shall employ automated mechanisms to increase the availability of incident response-related information and support.

4.7.2 Documentation

Documentation of IT systems involves the collection of detailed information, such as functionality, system mission, unique personnel requirements, type of data processed, architectural design, system interfaces, system boundaries, hardware and software components, system and network diagrams, asset costs, and system communications and facilities. This information is part of the configuration baseline of the system.

HUD Policy

a. Program Offices/System Owners shall ensure that adequate documentation for the information system and its constituent components is available, current, protected when required, and distributed to authorized personnel. Documentation includes but is not limited to:

- C&A and SDLC documentation
- Vendor-supplied documentation of purchased software and hardware
- Network diagrams
- Application documentation for in-house applications
- System build and configuration documentation, which includes

optimization of system security settings, when applicable
- User manuals
- Standard operating procedures

For systems that have been rated moderate or high, the documentation shall describe the functional properties of the security controls employed within the information system with sufficient detail to permit analysis and testing of the controls. For systems that have been rated high, the documentation shall describe the design and implementation details of the security controls employed within the information system with sufficient detail to permit analysis and testing of the controls, including functional interfaces among control components.

4.7.3 Information and Data Backup

Adhering to requirements regarding data backups can significantly reduce the risk that data will be compromised or lost in the event of a disaster or other interruption of service. A Backup Operations Plan should be included in the Contingency Plan.

The development of a data backup strategy begins early in the life cycle when the security categorization of the system is first considered. Several factors derived from the risk assessment and documented in the Contingency Plan will drive the data backup strategy. Frequency of backups will depend upon how often the data processed by the system(s) changes and how important those changes are. The risk assessment will drive this element of the backup strategy. Data backups need to be stored, both onsite and offsite, in a secure facility in fireproof and waterproof containers.

HUD Policy

a. Program Offices/System Owners shall ensure that a backup strategy and procedures are established, implemented, and tested in accordance with the Contingency Plan.

b. The Deputy CIO for IT Operations shall implement and enforce backup procedures for all sensitive IT systems, data, and information. The backups shall include user-level and system-level information.

c. The Deputy CIO for IT Operations shall store backups at a secure offsite location in accordance with the Contingency Plan.

d. The Deputy CIO for IT Operations shall test backup information quarterly for systems rated moderate and high.

e. The Deputy CIO for IT Operations shall test backup information as part of contingency planning for systems rated high.

f. For systems rated high, the Deputy CIO for IT Operations shall store backup copies of the operating system and other critical information systems software in a fire-rated container that is not collocated with the operational software or in a separate facility.

4.7.4 Input/Output Controls

Many security problems start with input validation issues. Information systems that fail to validate input can introduce "buffer overflow" vulnerabilities that could be exploited by an attacker. Checks for accuracy, completeness, and validity of information should be accomplished as close to the point of origin as possible. Rules for checking the valid syntax of information system inputs (e.g., character set, length, numerical range, and acceptable values) should be in place to ensure that inputs match specified definitions for format and content. Inputs passed to interpreters should be prescreened to ensure that the content is not unintentionally interpreted as commands.

On the output side, the structure and content of error messages

should be carefully considered by the organization. User error messages generated by the information system should provide timely and useful information to users without revealing information that could be exploited by adversaries. System error messages should be revealed only to authorized personnel (e.g., systems administrators and maintenance personnel). Sensitive information (e.g., account numbers, social security numbers, and credit card numbers) should not be listed in error logs or associated administrative messages.

HUD Policy

a. For systems rated moderate or high, the Program Offices/System Owners shall ensure that the information system checks information inputs for accuracy, completeness, and validity.

b. For systems rated moderate or high, the Program Offices/System Owners shall ensure the information system identifies and handles error conditions in an expeditious manner.

5.0 TECHNICAL POLICIES
5.1 Identification and Authentication

Authentication is the process of establishing confidence in user identities electronically presented to an information system. Individual authentication is the process of establishing an understood level of confidence that an identifier refers to a specific individual. Authentication focuses on confirming an individual's identity, based on the reliability of the individual's credentials.

Authentication of user identities is accomplished using passwords, tokens, PKI certificates, key cards, biometrics, or in the case of multifactor authentication, some combination therein. FIPS 201 and its attendant SP 800-73 and SP 800-76 specify a personal identity verification (PIV) card token for use in the unique identification and authentication of federal employees and contractors. NIST SP 800-63 provides guidance on remote electronic authentication. When information systems are accessed through local interfaces and contained within a controlled environment with physical access controls, the risk of using passwords as opposed to other forms of authentication, are somewhat mitigated. Thus, passwords that meet NIST SP 800-63 level 2 password requirements used locally in an environment with adequate physical access controls can be used in FIPS 199/SP 800-53 moderate-impact systems.

HUD Policy

a. Program Offices/System Owners shall ensure that user access is controlled and limited based on positive user identification and authentication mechanisms that support access control, least privilege, and system integrity in accordance with FIPS 201, Personal Identity Verification for Federal Employees and Contractors. For high-impact systems, the system shall employ multifactor authentication mechanisms.
b. HUD users shall not share identification or authentication materials of any kind; nor shall any HUD user allow any other person to operate any HUD system by employing the user's identity.
c. All user authentication materials shall be treated as sensitive material and shall carry a level of sensitivity as high as the most sensitive data to which that user is granted access using that authenticator.
d. The system ISSO shall ensure that USERIDs are disabled after a period of inactivity of no more than 90 days. For systems rated moderate to high, the system shall do this automatically.
e. Program Offices/System Owners shall ensure that user access is reviewed once a year.

5.1.1 E-Authentication

To successfully implement a government service electronically (or e-government), federal agencies must determine the required level of assurance in the authentication for each transaction. This is

accomplished through a risk assessment for each transaction.

The OMB has defined four levels of assurance in terms of the consequences for authentication errors and misuse of credentials. NIST has published technical guidance for federal agencies to support the ability of individuals to remotely authenticate to a federal system at different assurance levels.

HUD Policy

a. Program Offices/System Owners of IT systems that require authentication controls over the Internet between outside parties and HUD, the IT system shall utilize authentication mechanisms in accordance with NIST SP 800-63, Electronic Authentication Guide.

b. Program Offices/System Owners shall at a minimum comply with the following authentication requirements depending on system sensitivity in accordance with NIST SP 800-63: Low-impact systems must comply with the requirements for level 1 authentication systems Moderate-impact systems must comply with the requirements for level 2 authentication systems High-impact systems must comply with the requirements for level 3 authentication systems

5.1.2 Device and Application Authentication

Multi-tier systems can use middle- and back-end systems to connect to legacy systems and databases. In certain situations, this connection takes place using a generic ID and password that may contain full system privileges. Compromise of these IDs/Passwords can result in system misuse.

Networks that do not use device authentication are open to intrusions by attackers who have access to their physical location. Shared media networks and dynamic protocols, like Dynamic Host Configuration Protocol (DHCP), are susceptible to attacks from anyone with physical access to a network connection (e.g., network wall outlet). The attacker can plug in the device and start using it to capture packets of data or to start scanning the network for vulnerable systems.

To ensure that only approved devices can connect to the network and that approved applications can connect to back-end systems, the authenticators need to be protected from unauthorized disclosure and use.

The information system typically uses either shared known information (e.g., Media Access Control [MAC] or Transmission Control Protocol/Internet Protocol [TCP/IP] addresses), an organizational authentication solution (e.g., IEEE 802.1x and Extensible Authentication Protocol [EAP]), or a Radius server with EAP-Transport Layer Security (TLS) authentication to identify and authenticate devices on local and/or wide area networks (WAN).

HUD Policy

a. Program Offices/System Owners must use an IT Security Office-approved procedure, mechanism, or protocol to secure authenticators used for application, host, or device authentication.

5.1.3 Passwords

A password is a secret that a claimant memorizes and uses to authenticate the claimant's identity. Passwords are typically character strings.

Strong passwords have a minimum of eight alphanumeric characters with at least one uppercase letter, one lowercase letter, one digit, and one special character. Strong passwords do not have common words or permutations of the user name.

HUD Policy

a. In those systems where user identity is authenticated by password, the system ISSO shall determine and enforce appropriate measures to ensure that strong passwords are used.

b. In those systems where user identity is authenticated by password, the system ISSO shall determine and enforce the appropriate frequency for changing passwords; but in no case shall the frequency be less often than every 90 days.

c. Users shall not share personal passwords.

d. Users shall select strong passwords and not reuse old passwords.

e. Use of group passwords shall be limited to situations dictated by operational necessity or those critical for mission accomplishment. Use of a group USERID and password must be approved by the appropriate Authorizing Official.

f. In those systems where user identity is authenticated by password, the system shall ensure that users cannot reuse a password for at least eight iterations.

g. In those systems where user identity is authenticated by password, the system shall ensure that passwords are not displayed when entered.

h. In those systems where user identity is authenticated by password, the system shall protect passwords from unauthorized disclosure and modification when stored and transmitted.

i. System administrators shall replace all default passwords provided by the vendor.

j. In those systems where user identity is authenticated by password, the system ISSO shall develop and implement administrative procedures for initial password distribution, for lost/compromised passwords, and for revoking passwords.

The use of a password by more than one individual is discouraged throughout HUD; however, it is recognized that in certain circumstances (e.g., operation of crisis management or operations centers, watch teams, and other duty personnel) may require the use of group USERIDs and passwords.

5.2 Access Control

Users are responsible for protecting all HUD information to which they are granted access. Access controls restrict access to system objects, such as files, directories, and devices based upon the identity of the user or the group to which the user belongs. The purpose of access controls is to protect against the unauthorized disclosure, modification, or destruction of the data residing in these systems, as well as the applications themselves. Automated systems are vulnerable to fraudulent or malicious activity by individuals who have the authority or capability to access information not required to perform their job-related duties. Access control policy is designed to reduce the risk of an individual acting alone from engaging in such fraudulent or malicious behavior. The Principle of Least Privilege states that a user should only be able to access the system resources needed to fulfill the user's job responsibilities.

HUD Policy

a. Program Offices/System Owners shall ensure that their information systems implement access control measures to provide protection from

unauthorized alteration, loss, unavailability, or disclosure of information.

b. Program Offices/System Owners shall ensure that their information systems rated moderate to high, use an automated mechanism to support management of information system accounts. For information systems rated high, the automated mechanism shall track account creation, disabling, and termination to support audit of such actions and, as required, notify appropriate individuals.

c. Program Offices/System Owners shall ensure that access control follows the principle of least privilege and separation of duties and shall require that a user use unique identifiers on a system.

d. ISSOs shall ensure that temporary and emergency accounts are properly authorized and maintained. For systems rated high, these accounts shall be automatically disabled after 48 hours.

e. ISSOs shall ensure that guest/anonymous accounts are not used.

f. Program Offices/System Owners shall identify specific user actions, which can be performed on the information system without identification and authentication. For systems rated moderate to high, actions to be performed without identification and authentication will be permitted only to the extent necessary to accomplish mission objectives.

5.2.1 Automatic Account Lockout

Program Offices/System Owners shall configure each IT system to lock any user account immediately and automatically following a specified number of consecutive failed logon attempts, in such a way that:

* As long as the account remains locked, no logon of any kind will be permitted to that account, including the user to whom the account is assigned.
* The manual intervention of an appropriate security administrator is required to unlock the account.

HUD Policy

a. Program Offices/System Owners shall ensure that their information systems implement and enforce an account lockout policy that limits the number of consecutive failed logon attempts to three within a thirty-minute period.

b. Program Offices/System Owners shall ensure their information systems are configured to lock out a user account after three consecutive failed logon attempts.

5.2.2 Logon and Session Security

Program Offices/System Owners shall configure each IT system to deactivate any user session immediately and automatically following a specified period of inactivity, in such a way that will require the user to re-authenticate the user's identity before resuming interaction with the system.

Systems that provide the user at logon with information concerning the last connection and possible unsuccessful attempts provide the agency with another layer of defense by enlisting users in identifying and reporting unusual activity.

Highly sensitive systems should limit the number of sessions that a user can have active to prevent possible unauthorized disclosure, modification, and/or destruction of sensitive information.

HUD Policy

a. Program Offices/System Owners of systems that have been rated moderate or high shall ensure their systems time out user sessions after ten minutes of inactivity.

b. For systems rated high, the Program Offices/System Owners shall ensure that the system does not allow concurrent sessions.

5.2.3 Warning Banner

Successful prosecution of unauthorized access to HUD systems requires that users be notified prior to their entry into the systems that the data in the system is owned by HUD and that activities on the system are subject to monitoring. All multi-user computer systems will display a warning message when a user attempts to access the system, and prior to actually logging into a system, informing users that equipment is the property of the government, that the use of government property is for the conduct of government business only, and that the use of government equipment is subject to monitoring. Privacy Laws have explicit requirements to notify users about HUD's privacy policy prior to granting access to a system.

HUD Policy

a. The CISO shall provide a standard notification message for HUD systems that warns unauthorized users that they have accessed a U.S. Government system and can be punished. The wording shall also warn authorized users that they are subject to monitoring and recording and that use of the system indicates consent to such monitoring and recording.

b. IT systems internal to the HUD network shall display a warning banner stipulated by the HUD CISO and the Privacy Officer, when applicable. The warning banner shall require users to click through, indicating acknowledgment, prior to granting access to the system.

c. IT systems accessible to the public shall provide both a security and privacy statement approved by the CISO and the Privacy Officer at every entry point. The statement shall include a description of the authorized uses of the system.

5.3 Audit and Accountability

Audit trails maintain a record of system application and user activity. In conjunction with the appropriate tools and procedures, audit trails can assist in detecting security violations, performance problems, and application flaws.

Audit trails may be used as support for regular system operations or as a kind of insurance policy, or both. As an insurance policy, audit trails are maintained but are not used unless needed (e.g., after a system outage or suspected compromise). As a support for operations, audit trails are used to help system administrators ensure that the system or resources have not been harmed by hackers, insiders, or technical problems.

Audit trails help accomplish several security-related objectives, including individual accountability, event reconstruction, intrusion detection, and problem analysis.

Information systems that store or process personally identifiable information, personal health-related information, or financial information have specific audit requirements under the Privacy Act, Health Insurance Portability and Accountability Act, and the Sarbanes-Oxley Act.

HUD Policy

a. Program Offices/System Owners shall ensure that audit trails are sufficient in detail to facilitate the reconstruction of events if a system is compromised or if a malfunction occurs or is suspected. Audit trails shall include auditable events as specified in the system security plan and be reviewed accordingly. The audit trail shall contain at least the following information:

Type of event

Identity of the user, application, and device that triggered the event

The component of the information system (e.g., software component and hardware component) where the event occurred

Time and date of the event

Outcome (success or failure) of the event

For systems rated moderate to high, the audit function shall have the capability of providing more detailed information for audit events identified by type, location, or subject. For systems rated high, the system shall provide the capability for centralized management of audit records.

b. Program Offices/System Owners shall ensure that their audit trails and audit logs are protected from unauthorized modification, access, or destruction while online and during offline storage.

c. Program Offices/System Owners shall ensure that audit logs are recorded and retained in accordance with HUD records retention policies, but in no case shall the frequency be less than once a year for systems rated moderate to high.

d. Program Offices/System Owners shall develop and implement a process to periodically review audit records for inappropriate or unusual activity, investigate suspicious activity or suspected violations, and report findings to the appropriate officials. For systems rated moderate or high, the Program Offices/System Owners shall employ an automated mechanism to facilitate the review of audit records. Audit records related to activities of users with significant information systems roles and responsibilities shall be reviewed more frequently.

e. Program Offices/System Owners shall ensure that the system allocates sufficient audit record storage capacity and configures auditing to prevent such capacity being exceeded.

f. Program Offices/System Owners shall ensure that the system alerts the appropriate officials in the event of an audit failure or when audit capacity is close to being reached.

g. Program Offices/System Owners shall make a risk-based decision on which one of the following actions the system should take in the event of an audit failure or when audit capacity is being reached:

Shutdown the system

Overwrite the oldest audit records

Stop generating audit records

h. Program Offices/System Owners of information systems that have been rated moderate or high shall that utilize audit reduction, review, and reporting techniques while ensuring that original audit records needed to support after-the-fact investigations are not altered. Program Offices/System Owners of high-impact systems shall ensure the system provides the capability to automatically process audit records for events of interest based upon selectable, even criteria.

i. Program Offices/System Owners shall use automated mechanisms to integrate their audit procedures into HUD's incident response capability for systems rated moderate to high, which provides for centralized audit monitoring, analysis, and reporting.

j. Program Offices/System Owners shall ensure that information systems under their purview provide time stamps for use in audit record generation. The time stamps shall be generated using internal information system clocks that are synchronized system wide.

5.4 Network Security

5.4.1 Remote Access and Dial-In

Remote access controls are applicable to information systems other than public web servers or systems specifically designed for public

access. HUD restricts access achieved through dial-up connections (e.g., limiting dial-up access based upon source of request) or protects against unauthorized connections or subversion of authorized connections (e.g., using virtual private network [VPN] technology). HUD permits remote access for privileged functions (e.g., maintenance ports and system and device administration) only for compelling operational needs and during emergencies.

HUD Policy

a. The Deputy CIO for IT Operations shall provide remote access mechanisms that are centrally managed, monitored, and protected by strong authentication. The mechanisms shall have the capability to provide strong cryptographic mechanisms for authentication and protection of sensitive information during transmission. For access to systems rated moderate or high, the session shall be encrypted and access shall be managed through a managed access control point.

b. Program Offices/System Owners shall authorize and approve remote access methods for systems under their purview. The remote access methods shall only use mechanisms authorized by the Deputy CIO for IT Operations.

c. ISSOs shall authorize in writing users requiring remote access, including remote access for privileged functions.

d. Remote access administrators shall not add users to remote access mechanisms without written approval from the ISSO.

5.4.2 Network Security Monitoring

The increasingly important role of automated information system networks in government has fueled the need for more secure systems. Intrusion detection systems are gaining widespread recognition as important tools that improve computer network security. Although firewalls have traditionally been the first line of defense against would-be attackers, intrusion detection devices, working with firewalls, are becoming more popular for network security.

HUD Policy

a. The CSIRC shall use automated tools and mechanisms to monitor HUD's networks for security events.

b. The CISO, in coordination with IT Operations, shall select and implement intrusion detection and monitoring tools for HUD in accordance with NIST SP 800-31, Intrusion Detection Systems. The tools shall be part of a system-wide intrusion detection system that uses common protocols and supports near-real-time analysis of events in support of system-level attacks.

c. The CISO, in conjunction with the Deputy CIO for IT Operations, shall select and implement vulnerability scanning tools and techniques to scan information systems for vulnerabilities every month or when significant new vulnerabilities affecting HUD's infrastructure are identified and reported on systems rated low and moderate. Systems rated high shall be scanned once a week. For high-impact systems, the tools shall include the capability to update the list of vulnerabilities scanned. The list shall be updated every six months or when significant new vulnerabilities affecting the system are identified and reported.

d. The CISO, in conjunction with the Deputy CIO for IT Operations, shall perform annual penetration testing on network components.

5.4.3 Network Connectivity

Within HUD, boundary protection of IT resources is accomplished by the installation and operation of controlled interfaces (e.g., proxies, gateways, routers, firewall, and encrypted tunnels). Controlled interfaces, when used in concert with a variety of

additional security controls (e.g., intrusion detection systems, personnel background checks, security guards, data encryption, and physical security barriers), provide an added level of assurance that unauthorized personnel will be unable to access departmental automated systems.

By tracking and controlling data, deciding whether to pass, drop, reject, or encrypt the data, controlled interfaces have proven to be an effective means of securing a network.

HUD Policy

a. The Deputy CIO for IT Operations shall ensure that appropriate identification and authentication controls, audit logging, and access controls are implemented on every network component.

b. Program Offices/System Owners shall ensure that interconnections between sensitive IT systems under their purview and IT systems not controlled by HUD are established only through controlled interfaces. The controlled interfaces shall be accredited at the highest security level of information on the network.

c. The Deputy CIO for IT Operations shall ensure controlled interfaces are configured to prohibit any protocol or service that is not explicitly permitted. For high-impact systems, the Deputy CIO for IT Operations shall review and eliminate any unnecessary functions, ports, protocols, or services once a year.

d. The Deputy CIO for IT Operations shall ensure that a failure of the controlled interfaces does not result in any unauthorized release of information outside the information system boundary.

e. The Deputy CIO for IT Operations shall ensure that there is no public access to HUD's internal networks except as appropriately mediated through a proxy server.

f. The Deputy CIO for IT Operations shall ensure that alternate processing sites provide the same level of protection for network connections as the primary site.

g. The CISO shall establish connection criteria for allowing portable or mobile information systems access to HUD's networks.

h. The Deputy CIO for IT Operations shall ensure that portable or mobile information systems are not allowed access to HUD's networks without written approval and only after the devices meet the connection criteria established by the CISO.

5.4.4 Internet Security

The Internet is an excellent medium to publish and transmit information, thus providing substantial gains in productivity. Since the Internet is an open network available to everyone, including hackers and attackers, HUD must strike a balance that provides Internet connectivity to its constituents while maintaining an appropriate level of security.

HUD Policy

a. The Deputy CIO for IT Operations shall ensure that any direct connection of HUD networks to the Internet or to extranets occurs through controlled interfaces that have been certified and accredited.

b. The Deputy CIO for IT Operations shall ensure that publicly accessible information system components (e.g., public web servers) reside on separate sub-networks with separate physical network interfaces.

c. HUD employees or contractors shall not download or install mobile code (e.g., ActiveX or JavaScript) that has not been approved by the CISO.

d. The Deputy CIO for IT Operations shall ensure that controlled

interfaces protecting the network perimeter filter certain types of packets to protect devices on an organization's internal network from being directly affected by denial of service attacks.
e. The Deputy CIO for IT Operations shall ensure that publicly accessible information systems protect the integrity of the information and applications available to the public.

5.4.5 Personal Email Accounts

Personal email accounts often reside on insecure networks where they are subject to compromise, interception, and computer viruses.

HUD Policy

a. HUD employees or contractors shall not transmit sensitive HUD information to any personal email account that is not authorized to receive it.
b. HUD employees or contractors shall not access personal email accounts from internal HUD networks or with HUD-provided equipment.

5.5 Cryptography

Encryption is the process of changing plaintext into ciphertext for the purpose of security or privacy. There are two basic types of cryptography:

1. Secret key systems-also called symmetric systems
2. Public key systems-also called asymmetric systems

In secret key systems, the same key is used for both encryption and decryption; that is, all parties participating in the communication share a single key. In public key systems, there are two keys: a public key and a private key. The public key used for encryption is different from the private key used for decryption. The two keys are mathematically related, but the private key cannot be determined from the public key.

Refer to NIST SP 800-21, Guideline for Implementing Cryptography in the Federal Government, for more in-depth information on cryptography.

A digital signature is an electronic analogue of a written signature. The digital signature can be used to prove to a recipient or third party that the originator did in fact sign the message (i.e., the message originators cannot repudiate the message). Signature generation makes use of a private key to generate a digital signature. Signature verification makes use of a public key that corresponds to, but is not the same as, the private key. The security of a digital signature system depends on maintaining the secrecy of users' private keys.

Encryption can be used to do, but is not limited to, the following:

* Encrypt data while in storage (e.g., hard drives, diskettes, and tapes)
* Encrypt data while in transmission
* Encrypt individual files for transmission over an unsecured medium
* Encrypt email messages
* Guarantee the integrity of a file or message, and detect any modifications
* Provide the legally binding equivalent of a hand signature in digital form
* Support non-repudiation
* Support authentication, including strong authentication
* Support electronic financial transactions, including electronic funds transfers, automated teller machine transactions, cash cards, gift cards, and credit cards
* Provide copyright protection (e.g., for DVDs)

5.5.1 Encryption

The FIPS 199 security category (for integrity and confidentiality) of the information being transmitted should guide the decision on the use of cryptographic mechanisms.

HUD Policy

a. Program Offices/Systems Owners shall identify IT systems transmitting or storing sensitive information that may require protection based on a risk assessment. If encryption is required, the following methods are acceptable for encrypting sensitive information:

Products using triple Data Encryption Standard (3DES) or Advanced Encryption Standard (AES) algorithms that have been validated under FIPS 140-1 or FIPS 140-2. (All new systems should use AES because it is expected that triple DES will be phased out.)

Secure Sockets Layer Version 3.0 (SSL3.0) or Transport Layer Security Version 1.0 (TLS1.0)

National Security Agency (NSA) Type 2 or Type 1 encryption

b. The CISO and Deputy CIO for IT Operations shall ensure cryptographic key establishment and management is done in accordance with NIST SP 800-56, Recommendation on Key Establishment Schemes, and NIST SP 800-57, Recommendation on Key Management.

c. Program Offices/Systems Owners of systems rated moderate or high shall use encryption to implement the following controls:

Remote access

Wireless access

Cryptographic module authentication

Transmission integrity and confidentiality

d. Program Offices/System Owners and users shall ensure information rated moderate or high residing on portable or mobile systems use FIPS 140-1 or 140-2-approved encryption to protect information.

5.5.2 Public Key Infrastructure

A public key infrastructure (PKI) is an architecture that provides the means to bind public keys to their owners and helps in the distribution of reliable public keys in large heterogeneous networks. Public keys are bound to their owners by public key certificates. These certificates, which contain information such as the owner's name and the associated public key, are issued by a reliable certification authority (CA).

HUD Policy

a. The CISO, in conjunction with the Deputy CIO for IT Operations, shall select and implement a PKI for HUD in accordance with NIST SP 800-32, Introduction to Public Key Technology and the Federal PKI Infrastructure.

b. The CISO, in conjunction with the Deputy CIO for IT Operations, shall establish HUD's root CA and operate under an approved certificate policy and certificate practice statement. Any additional CAs within HUD must be subordinate to the HUD root.

c. Program Offices wishing to establish their own CA shall request approval from the CISO, be a subordinate to the HUD root, and operate under an approved certificate policy and certificate practices statement.

d. The CISO shall cross-certify the HUD root CA with the Federal Bridge. The certificate policies and practice statements of CAs subordinate to the HUD root must comply with the Federal Bridge Certificate Policy.

e. The CISO shall perform a yearly compliance audit of the root CA and all subordinate CAs.

f. The CISO, in conjunction with the Deputy CIO for IT Operations,

shall ensure that HUD's PKI can support the requirements for E-authentication in accordance with NIST SP-800-63, Electronic Authentication Guideline: Recommendation of the National Institute of Standards and Technology.

g. The CISO, in conjunction with the Deputy CIO for IT Operations, shall ensure that HUD's PKI can support the requirements for personal identification verification in accordance with NIST FIPS 201, Personal Identity Verification for Federal Employees and Contractors and Draft SP 800-73, Integrated Circuit Card for Personal Identity Verification.

5.5.3 Public Key/Private Key

A public key/private key pair is generated using the PKI. The user retains the private key. The issuing CA signs the public key, creating a public key certificate. These certificates are used by the PKI to validate a public key. Public key/private keys can be used in a public key cryptographic system to encrypt data. They also can be used to create digital signatures.

HUD Policy

a. The CISO, in conjunction with the Deputy CIO for IT Operations, shall ensure separate public/private key pairs are used for encryption and digital signature.

b. Users shall not disclose or allow the use of their private keys. If a user shares his or her private key, the user is accountable for all transactions signed with the user's private key.

c. Users shall be responsible for the security of their private keys.

5.6 Malicious Code Protection

Malicious code includes all and any programs (including macros and scripts) that are deliberately coded to cause an unexpected, and unwanted, event on a user's workstation. Malicious code includes viruses, worms, logic bombs, Trojan horses, web bugs, and in some cases "spyware."

Malicious code can be introduced several ways (e.g., email, file downloads, and web surfing). It can destroy the integrity and confidentiality of data and systems.

HUD Policy

a. The Deputy CIO for IT Operations shall implement a defense-in-depth strategy that:

Installs and centrally manages antivirus software at each critical information entry point (e.g., firewalls, email servers, and remote-access servers) and at each workstation, server, and mobile computing device. The software shall be configured to check all files automatically on access, downloads, and email.

Installs updates to antivirus software and signature files at each critical information entry point (e.g., firewalls, email servers, and remote-access servers) and at each workstation, server, and mobile computing device promptly without requiring that end users specifically request the update.

Configures the software to prevent users from disabling it or modifying configuration settings.

Installs security patches to servers and desktops promptly.

Automatically forwards alerts generated by anti-virus software to HUD's intrusion detection system.

b. The Deputy CIO for IT Operations shall implement appropriate file/protocol/content filtering to protect data and networks against malicious code in accordance with HUD's Internet usage policy.

c. The Deputy CIO for IT Operations shall install and centrally manage spam and spyware protection mechanisms at each critical

information entry point (e.g., firewalls, email servers, and remote-access servers) and at workstations, servers, and mobile computing devices connected to the network. The mechanism shall have the capability for automatic updates.

5.7 Miscellaneous

The following section addresses security requirements that did not belong to any other subcategory. Some of these requirements might apply to specific technologies. Examples of such technologies include video and audio conferencing and Voice over Internet Protocol (VoIP).

HUD Policy

a. Program Offices/System Owners of systems that have been rated moderate or high and use collaborative computing resources, like audio and video conferencing and electronic white boards, shall ensure that the collaborative computing resources cannot be activated remotely and provide explicit indication of use to the local user.

b. Program Offices/System Owners wishing to use VOIP in information systems under their purview must obtain approval from the CISO and Deputy CIO for IT Operations and follow the guidance in NIST SP 800-58, Security Considerations for VoIP Systems.

U.S. DEPARTMENT OF HOUSING AND URBAN DEVELOPMENT

INFORMATION TECHNOLOGY SECURITY POLICY

Handbook 2400.25, Rev. 1

(All previous versions are obsolete)

Table of Contents

1.0 INTRODUCTION

The Department of Housing and Urban Development (HUD) relies extensively on information technology (IT) to execute its mission and provide services to the American public and HUD's business partners. Given the prevalence of cyber threats today, HUD must manage its IT assets with due diligence and take the necessary steps to safeguard them while complying with federal mandates and the dictates of good stewardship.

Information security policies are an essential prerequisite to sound IT security. They are designed to preserve the confidentiality, integrity, availability, and value of assets, as well as ensure the continued delivery of services. They also establish the appropriate focus and standards for acceptable security practices across an organization. This policy is based on federal regulations and highlights HUD's goals and requirements for protecting its IT assets.

All HUD components must comply with the basic requirements of this policy and its associated operational standards and technical documentation. Each component must also determine any need for additional safeguards above this baseline level and implement them appropriately. Additional safeguards should be based on an assessment of risk and local conditions.

1.1 Purpose

This document establishes the information security policy for HUD. The policy prescribes responsibilities, practices, and conditions that directly or indirectly promote security in the development, operation, maintenance, and support of all HUD IT resources.

The policy identifies security practices that are appropriate to HUD's mission, provide cost-effective protection of HUD's IT, respond to security issues associated with contemporary technologies and risks, and are consistent with current applicable federal security laws, policies, and regulations.

1.2 Scope

This policy provides a comprehensive view of IT security considerations. It addresses technical security services, as well as the management and operational requirements for IT security, and it identifies all relevant security roles and responsibilities and affected organizations. In addition, the policy addresses security-relevant boundaries (e.g., interfaces with external systems and networks and any use of personal computing in the conduct of HUD's business). It also reflects the increasing requirements for internal and external security oversight from the HUD Office of Inspector General (OIG) and in response to the Federal Information Security Management Act (FISMA).

Since this policy is intended to provide a set of basic protection goals and standards, the procedural details normally found in operational and technical documentation are not within the scope of this document.

Information security policies conventionally require systems to provide various technical security services (e.g., authentication, access control, and intrusion detection); however, a comprehensive policy also identifies managerial and operational requirements, which recent regulations have emphasized. For example, federal departments are required to integrate security

planning into their Capital Planning and Investment Control (CPIC) process. Also, the Office of Management and Budget (OMB) requires periodic reports on the state of information security activities at all federal departments, and these reports have implications for acquiring and maintaining such information.

As a result, this policy has implications for more than security specialists and will affect System Owners and developers, practitioners of non-IT security disciplines, support operations personnel (e.g., security training and awareness personnel, contract managers), and personnel interacting with the HUD privacy advocate, OIG, external auditors, HUD Enterprise Architecture (EA) developers, and other agencies.

In addition, this information security policy applies to HUD Program Offices that have security-specific or security-relevant roles and responsibilities, such as system security planning, certification and accreditation (C&A), security audit, configuration management (CM), continuity of operations (COOP) activities, and security incident response. The policy also applies to all HUD employees, contractors, and service providers who must comply with day-to-day provisions of HUD policy (e.g., proper password choice and management, maintaining security awareness, incident reporting, and prompt system upgrades).

1.3 Authority for Policy

The authority for the issuance of this policy rests with the Office of Chief Information Officer. The Program Office that will subsequently issue and maintain this policy includes those responsible for the following:

- Information security policy development
- IT security review and evaluation
- Information security policy enforcement
- Conformance monitoring and evaluation, including the identification and monitoring of metrics where possible
- Interactions with associated policy elements, HUD business functions, system acquisition authorities, and external agencies
- Policy revisions, including interim updates and annual re-issuances, when required
- Policy waiver evaluations

Section 2.0 provides the detailed allocation of information security roles and responsibilities among HUD personnel.

1.4 Policy Basis

This policy is primarily based on recent federal laws, regulations, and guidance on information security (e.g., the rapidly growing series of National Institute of Standards and Technology [NIST] Special Publications [SP] on information security). In areas where federal guidelines are lacking or still evolving, the policy reflects established best security practices within the security community. The policy also incorporates previously published HUD information security policy and guidelines.

1.5 Relationship to Other Documents and Processes

As the primary information source for fundamental requirements for maintaining the confidentiality, integrity, and availability of IT resources, the policy identifies and characterizes a comprehensive set of basic protection goals without stipulating how the goals should be met (i.e., the specific technologies, mechanisms, or procedures involved). Procedural details, particularly technical details that are either changeable or applicable to one type of system (e.g., configuration for a particular operating system) are documented separately.

The information security policy may change from time to time. For example, the potential use of some newer technologies (e.g., wireless communications) can give rise to additional policy requirements. In such cases, the policy will outline the basic relevant security policy requirements; however, in general, the policy is free from low-level procedural and technical detail.

The requirements of this policy complement other agency measures for effective management of assets and regulatory compliance (e.g., with the federal privacy laws). References are made to those sources throughout this document.

Guidance on HUD information security standards, methodologies, procedures, and adaptations to ongoing legislation and federal regulations and standards will be expanded in a separate *Information Technology Security Handbook*. The handbook provides additional guidance on information security policy elements, examples of which might include password enforcement mechanisms, C&A procedures, and incident-response procedures.

Where necessary, the most detailed, procedure-intensive, or volatile IT security guidance will be issued in topic-specific guidelines. Generally, technical specialists are the principal users of such guidelines (e.g., specifications of product version-specific configuration settings that are consistent with security requirements or instructions for recovering from a virus attack).[1]

The information security policy, handbook, and set of detailed guidelines form an information security policy compendium as shown in Figure 1. This document compendium becomes the foundation for secure HUD information system design, operation, and maintenance. The figure also depicts mutual influences between information security policy and a variety of affiliated processes that information security relies upon or affects to some extent, including Quality Assurance (QA), COOP procedures, Critical Infrastructure Protection (CIP), and EA development.

Information security policy makes certain assumptions about protection measures that respond to other HUD security policies and practices (e.g., physical security and personnel security). For example, this policy presupposes reliable processes for confirming the credentials of prospective system users. Information security policy also presupposes the enforcement of suitable physical protection of the means of access to facilities housing HUD IT resources. However, since physical and personnel security policies are not exclusively or primarily concerned with IT resource protection, documents in the information security policy compendium refer to such separate policies or make assumptions about their provisions, as appropriate.

[1] Examples of topic areas being addressed in separate guidelines include security configuration guides for IT products, media sanitization techniques, and certification practice statements.

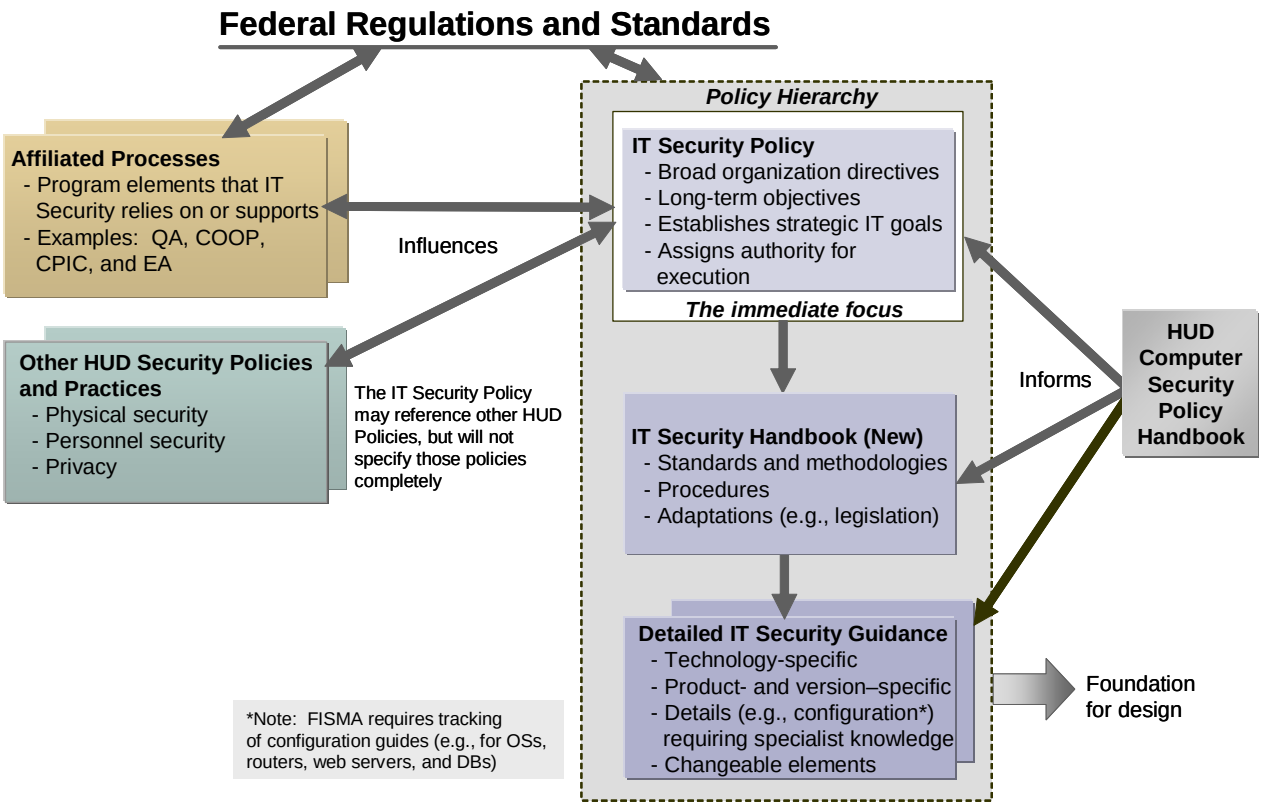

Figure 1. Security Policy Relationships

1.6 Document Organization

Section 2 describes the information security roles and responsibilities assigned to HUD personnel. The policies in Sections 3, 4, and 5 describe in more detail the management, operational, and technical areas of controls necessary to evaluate or assess compliance:

- **Management Controls**—focus on IT security system management and system risk management that consist of risk mitigation techniques and concerns normally addressed by management.
- **Operational Controls**—address security methods that focus primarily on the mechanisms implemented and executed by people. These controls are designed to improve the security of a particular system or group of systems. These controls frequently require technical or specialized expertise and often rely on management and technical controls.
- **Technical Controls**—focus on security controls that a computer system executes. These controls can provide automated protection for unauthorized access or misuse, facilitate detection of security violations, and support security requirements for applications and data.

Within individual policy requirements, this document includes, where applicable, references to federal standards and regulations that are sources of the policy requirements. These are

summarized in Appendix A. The inclusion of the references is intended to provide the policy user with additional information and to serve as a means of confirming the comprehensiveness of HUD's response to the standards and regulations.

1.7 Laws and Regulations

HUD has established a department-wide IT security policy based on the following Executive Orders (EO), public laws, and national policies:

- Electronic Government Act (P.L. 107–347), December 2002.
- Executive Order 13231, *Critical Infrastructure Protection in the Information Age*, October 16, 2001.
- Federal Information Security Management Act (FISMA) of 2002, November 25, 2002.
- FIPS Pub 140–1, *Security Requirements for Cryptographic Modules*, January 1994.
- FIPS Pub 140–2, *Security Requirements for Cryptographic Modules*, May 2001.
- FIPS Pub 199, *Standards for Security Categorization of Federal Information and Information Systems*, December 2003.
- FIPS Pub 200, *Minimum Security Requirements Controls for Federal Information and Information Systems* (projected for publication December 2005).
- FIPS Pub 201, *Personal Identity Verification for Federal Employees and Contractors*, February 2005.
- Homeland Security Presidential Directive (HSPD) 7, *Critical Infrastructure Identification, Prioritization, and Protection*, December 17, 2003.
- Office of Management and Budget Memorandum 03–19, *Reporting Instructions for the Federal Information Security Management Act and Updated Guidance on Quarterly IT Security Reporting*, August 2003.
- Office of Management and Budget Memorandum 03–22, *OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002*, September 2003.
- Office of Management and Budget Memorandum 04–04, *E-Authentication Guidance for Federal Agencies*, December 2003.
- Office of Management and Budget, Circular A-130, Appendix III, Transmittal Memorandum #4, *Management of Federal Information Resources*, November 2000.
- Paperwork Reduction Act of 1995 (P.L. 104-13), May 1995.
- Privacy Act of 1974, As Amended, 5 United States Code (U.S.C.) 552a, Public Law 93-579, Washington, D.C., July 14, 1987.
- Public Law 104–106, Clinger-Cohen Act of 1996 (formerly, Information Technology Management Reform Act [ITMRA]), February 10, 1996.
- Public Law 104–191 (H.R. 3103), Health Insurance Portability and Accountability Act of 1996.
- Public Law 107–296, Homeland Security Act of 2002.
- Various NIST Special Publications (SP).

1.8 Definitions

Following is a series of the key definitions applicable to the policies and procedures outlined in this document.

1.8.1 Sensitive Information

"Sensitive information" (defined by the Computer Security Act of 1987) is information to which access must be controlled and restricted in order to protect the national interest, the conduct of federal programs, and the privacy to which individuals are entitled under the Privacy Act (Section 552a of Title 5, U.S.C.), but is not specified by Executive Order or an act of Congress to be kept secret (i.e., classified as Top Secret, Secret, or Confidential) in the interest of national security or foreign policy. Examples of sensitive information include personal data (e.g., Social Security Number), trade secrets, system vulnerability information, pre-solicitation procurement documents (e.g., Statement of Work [SOW]), and law enforcement investigative methods. Sensitive information must be protected from loss, misuse, modification, and unauthorized access.

FIPS Pub 199, *Standards for Security Categorization of Federal Information and Information Systems*, was published in December 2003. It is now the mandatory standard for categorizing the sensitivity associated with federal information and information systems (except national security systems).

FIPS Pub 199 provides federal departments with a more detailed categorization of their information assets than the Computer Security Act of 1987 recognized. FIPS Pub 199 distinguishes among *low*, *moderate*, and *high* sensitivity categories and deals explicitly with integrity, availability, and confidentiality as security goals. Categories correspond to the different degrees of potential impact a security incident may have on a department's mission, assets, legal responsibilities, functions, or individuals.

1.8.2 Public Information

This type of information can be disclosed to the public without restriction, but requires protection against erroneous manipulation or alteration (e.g., a public website).

1.8.3 Information Technology

The Clinger-Cohen Act defines information technology as any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by an executive agency. For purposes of the preceding definition, "equipment" refers to that used by HUD or by a contractor under contract with HUD if that contractor (1) requires the use of such equipment or (2) requires the use, to a significant extent, of such equipment in the performance of a service or the furnishing of a product. The term "information technology" includes computers, ancillary equipment, software, firmware, and similar procedures, services (including support services), and related resources.

1.8.4 HUD Information Technology System

A HUD system is information technology that is (1) owned, leased, or operated by a Program Office, (2) operated by a contractor on behalf of HUD, or (3) operated by another federal, state, or local government agency on behalf of HUD. HUD systems include both general support systems and major applications.

1.8.4.1 *General Support System*

An interconnected set of information resources under the same direct management control that shares common functionality. It normally includes hardware, software, information, data, applications, communications, and people. A general support system can be, for example, a local area network (LAN) including smart terminals that support a branch office, an agency-wide backbone, a communications network, a departmental data processing center and its operating system and utilities, a tactical radio network, or a shared information-processing service organization. The Office of the Chief Information Officer is the Program Office responsible for most of these systems at HUD and the Deputy CIO for IT Operations is the System Owner for such systems.

1.8.4.2 *Major Application*

A major application is an information system that requires special attention to security due to the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of the information in the application. A major application may actually be made up of hardware, software, and firmware, but it is distinguishable from a general support system by the fact that it is a discreet application; whereas, general support systems may support multiple applications.

1.9 Exceptions

When a Program Office is unable to comply with policy, it may request an exception. Exceptions are generally limited to mission-specific systems that are not part of the HUD Enterprise Infrastructure. This request is made to the Chief Information Security Officer (CISO) through the Authorizing Official (AO) and must include the operational justification, risk acceptance, and risk mitigation measures.

2.0 ROLES AND RESPONSIBILITIES

Responsibility for protecting the confidentiality and integrity of HUD's information and technological resources is shared jointly by its employees, business partners, and contractors. However, in an effort to enable effective and complete implementation of this policy, specific duties have been assigned to individuals who will be fully accountable for fulfilling the associated requirements. This section describes the specific information security roles and responsibilities.

2.1 Secretary of the Department of Housing and Urban Development

The Secretary of HUD is responsible for ensuring that HUD IT systems and their data are protected in accordance with congressional and presidential directives. To that end, the Secretary will:

- Ensure the integrity, confidentiality, and availability of information and information systems.
- Ensure that HUD adheres to the requirements of its Information Security Program throughout the life cycle of each HUD system.
- Submit the results of independent evaluations performed by the HUD Inspector General (IG) to the Director of the OMB annually. These evaluations are to accompany HUD annual budget submissions.

2.2 Chief Information Officer

The HUD Chief Information Officer (CIO) will establish and oversee the department-wide Information Security Program and provide consulting assistance to all HUD offices for their individual programs. In addition, the CIO has the following information security responsibilities:

- Appoint, in writing, a federal employee to serve as the CISO.
- Participate in developing HUD performance plans, including descriptions of timeframes and budget, staffing, and training resources required to implement the departmentwide Information Security Program.
- Establish policy and oversight procedures to ensure that all information systems acquisition documents, including existing contracts, incorporate appropriate IT security requirements and comply with HUD IT security policies.
- Ensure that HUD's Information Security Program integrates fully into the HUD EA and CPIC processes.
- Ensure that Program Officials and/or System Owners understand and appropriately address risks, especially interconnectivity with other programs and systems outside their control.
- Review and evaluate the Information Security Program at least annually.

- Ensure that an IT Security Performance Metrics Program is developed, implemented, and funded.
- Report to the Secretary on matters relating to the security of HUD IT systems.
- Continuously strengthen the Information Security Program.
- Ensure that adequate resources are provided for the Information Security Program.
- Direct that all IT security requirements be followed.
- Accept responsibility for the Information Security Program successfully meeting all federal regulations.
- Ensure overall program success.

2.3 Chief Information Security Officer

The Chief Information Security Officer (CISO) reports directly to the CIO on matters pertaining to IT security within HUD. The CISO will perform the following duties:

- Serve as the departmentwide principal advisor on IT security matters.
- Issue department-wide IT security policy, guidance, and architecture requirements for all HUD IT systems and networks and provide oversight to ensure these policies are implemented.
- Serve as the principal departmental liaison with organizations outside HUD for matters relating to IT security.
- Review and approve the processes, techniques, and methodologies planned for use in certifying and accrediting HUD IT systems. These include security test and evaluation plans, contingency plans, and risk assessments.
- Carry out CISO responsibilities under FISMA.
- Possess the professional qualifications, including training and experience, required to administer the functions described.
- Head an office with the mission and resources required to assist in ensuring HUD compliance.
- Develop and maintain a HUD Information Security Program.
- Direct HUD's day-to-day management of the Information Security Program.
- Coordinate all security-related interactions among Program Offices involved in the Information Security Program, as well as those external to HUD.
- Support Information System Security Officers (ISSO) and participate in the selection of qualified staff from the Program Offices.
- Serve as a member in the Technology Investment Board Working Group.

2.4 Information System Security Officer

An ISSO shall be appointed in writing by the appropriate Program Official for each general support system and major application. The ISSO can be either a government employee or an

appropriately cleared support contractor. The ISSO is responsible for ensuring that management, operational, and technical controls for securing IT systems belonging to the Program Office are in place and followed. The ISSO will perform the following functions for the Program Office:

- Serve as the principal Point of Contact (POC) for all matters pertaining to the security of the IT systems for which the ISSO is responsible.
- Oversee the preparation of security plans, such as those required for C&A in coordination with the System Owner.
- Periodically review computer systems and networks to ascertain if changes have occurred that could adversely affect security.
- Ensure that system users receive initial computer security indoctrination and annual follow-on training, as required by applicable directives.
- Enforce an access control policy by which only authorized persons can gain access to HUD IT systems and networks.
- Immediately report any security violation, attempt to gain unauthorized access to sensitive data, virus infection, or other event affecting the security of HUD systems and networks to the appropriate Computer Security Incident Response Center (CSIRC).
- Enforce the capability to track user activity on a system and report any discrepancies or misuse of automated resources.
- Manage the IT Security Metrics Program for the IT system. Collect and analyze data and coordinate with the CISO, as appropriate.
- Implement IT security policies as directed by, and in coordination with, higher authority.
- Attend required role-based security training.

An ISSO can be assigned to more than one general support system or major application.

2.5 Contracting Officer, Government Technical Monitor, and Government Technical Representative

Contracting Officers, Government Technical Monitors (GTM), and Government Technical Representatives (GTR) are responsible for ensuring that security is properly and adequately addressed as part of system acquisition and other contracting activities. Specifically, these individuals will ensure that:

- New contracts include appropriate language and clauses to enforce HUD IT security policy and that existing contracts include appropriate language when modified.
- Any security clauses are developed and used in accordance with Departmental procurement policy, the HUD Acquisition Regulation (HUDAR) and Federal Acquisition Regulation (FAR).
- All new or modified HUD contracts include a clause requiring IT security awareness training and, where appropriate, role-based training for specific job categories with security responsibilities.

- All new or modified HUD contracts include a clause requiring contractor compliance with HUD computer security incident identification and reporting policy and procedures.
- IT security functional and assurance requirements are incorporated in information system procurement documents in accordance with HUD IT security policy.
- Contractors and subcontractors provide copies of their internal IT security plans and procedures to the CISO upon request.
- Existing and future contracts include requirements to have qualified security representatives (e.g., CISO, ISSO, or other designated HUD Program Office personnel) conduct site surveys at non-HUD facilities.

2.6 Help Desk

The help desk staff will:

- Assist HUD employees in technical security matters.
- Recognize and report security incidents to HUD CSIRC, engage resources for corrective action, and assist users in recovery.

2.7 Physical Security/Facilities Group/Security Officer

This generic title is used to identify the person or persons responsible for the physical security of the facility and the person or persons responsible for issuing badges and conducting required background checks for employees and contractors. In addition, the title is generic to cover outsourced computer services and operations.

The physical security staff and security officer will:

- Develop and enforce appropriate physical security controls.
- Identify and address the physical security needs of computer installations, office environments, and backup installations.
- Process and maintain personal background checks and security clearance records.
- Issue HUD Identification (ID) badges to employees and contractors in accordance with HSPD-12.

2.8 Deputy Chief Information Officer for Information Technology Operations

The Deputy CIO for IT Operations will:

- Monitor security technology developments and evaluate their usefulness for, or impact upon, HUD mission, architecture, and operations.
- Direct IT contingency planning.
- Work with the Program Offices, functional managers, and System Owners on technology and contingency planning issues.

- Own and secure the IT infrastructure (e.g., general support systems) that provides shared services across Program Offices.

2.9 Program Offices/System Owners

Program Offices, or System Owners, use IT to help fulfill the business requirements necessary to achieve the mission needs within their program area of responsibility. As such, they are responsible for the successful operation of IT systems within their program area and are ultimately accountable for the security of the IT systems and programs under their control. The Office of the Chief Information Officer is the Program Office responsible for most General Support Systems at HUD; the Deputy CIO for IT Operations is the System Owner for such systems. The Program Offices/System Owners will:

- Work closely with the CIO and other program and IT managers to ensure a complete understanding of risks, especially the increased risks resulting from interconnectivity with other programs and systems over which the Program Offices have little or no control.
- Prepare information system security plans and risk assessments for information systems under their purview.
- Ensure information systems under their purview are certified and accredited.
- Review, in consultation with the CISO, the IT system security within their program area at least annually.
- Manage the procurement and operation of their Program Office information systems.
- Assure adherence to information security policy in the design and operation of application systems.
- Coordinate with the Deputy CIO for IT Operations and the CISO on security matters involving HUD information architecture, as a whole.

2.10 HUD Managers, Supervisors, and Employees

All HUD personnel and support contractors who have been authorized access to sensitive data are responsible for protecting that data. These responsibilities include the following:

- Comply with IT security policy and apply its principles to daily work activities.
- Enforce IT security policy and ensure that employees and contractors comply with IT policies and procedures.
- Assume accountability for protecting sensitive information under their control in accordance with this policy.
- Attend annual IT Security Awareness training.
- Attend required role-based security training—pertains to those having a security-related role (e.g., system and network administrators).
- Report IT security incidents (e.g., virus and malicious code attacks) to the appropriate CSIRC according to established procedures.

- Cooperate with CSIRC Team members.
- Cooperate with Information Security Program representatives or other designated HUD Program Office personnel during security compliance reviews at HUD Program Office facilities and site surveys at non-HUD facilities.
- Ensure that IT security metrics data are collected in accordance with direction from the CISO and ISSO—Managers/Supervisors.
- Understand and comply with HUD policies, standards, and procedures regarding the protection of sensitive HUD information assets.

2.11 Authorizing Official

The Authorizing Official (AO) is a senior government management official with the authority to formally assume responsibility for operating an IT system at an acceptable level of risk. AOs control personnel, operations, maintenance, and budgets for their systems or field sites; therefore, AOs shall control the resources necessary to mitigate risks. An AO shall be assigned to each general support system and major application. The AO shall be a Senior Official who is the Program Assistant Secretary, Deputy Assistant Secretary, or equivalent Program Head.

The AO may assign a designated representative to act on the AO's behalf and be empowered to make certain decisions with regard to the planning and resourcing of security C&A activities, the acceptance of system security plans, and the determination of risk to agency operations, agency assets, and individuals. The only activity the AO cannot delegate is the security accreditation decision and signing the associated accreditation decision letter (i.e., the acceptability of risk to the agency).

AOs are responsible for the following:

- Reviewing and approving the corrective actions necessary to mitigate residual risks.
- Approving/disapproving system accreditation.
- Terminating system operations if security conditions warrant such action.

An AO can be responsible for more than one general support system or major application.

2.12 Certification Agent

A Certification Agent is assigned to each HUD IT system by an appropriate department-level official. Normally, the CISO is designated as the Certification Agent for all IT systems under the department's control.

To preserve the impartial and unbiased nature of security certification, the Certification Agent should be in a position that is independent from individuals directly responsible for information system development and day-to-day system operations. The Certification Agent should also be independent of those individuals responsible for correcting security deficiencies that are identified during security certification.

Certification Agents must be government employees and must be designated in writing at the department level. Designation letters shall be signed by the appropriate Under Secretary or Program Office Head. For each IT system, the Certification Agent shall:

- Ensure that a risk analysis is performed, that required C&A activities are completed, and that the results are documented.
- Prepare a *Security Evaluation Report* that clearly documents residual risks on the status of the certification for the AO.

A Certification Agent can be responsible for more than one general support system or major application.

3.0 MANAGEMENT POLICIES

3.1 Basic Requirements

In order to ensure the security of HUD information resources, basic security management principles must be followed. These principles are applicable throughout the department and form the cornerstone of the Information Security Program.

HUD Policy
a. Every HUD computing resource (e.g., desktops, laptops, servers, portable electronic devices, Commercial off-the-Shelf [COTS] software packages, and applications) shall be individually accounted for as part of a recognized information system inventory. The Office of Administration and Management Services (OAMS) shall maintain inventory accountability for all systems hardware and microcomputers with an acquisition cost of $500 or more. The Deputy CIO for IT Operations, in coordination with the Inspector General (IG), shall maintain a current system inventory for all commercial software and application systems used by HUD to process, store, and/or transmit information. This inventory shall be updated once a year.
b. Program Offices/System Owners shall prepare and maintain an active and effective Information Security Plan for each HUD information system under their purview. The Information System Security Plan is required prior to the start of certification and accreditation and it shall be reviewed and updated, if needed, once a year.
c. Program Offices shall designate an ISSO for every HUD information system under their purview.
d. Program Offices/System Owners shall conduct a privacy impact assessment on all systems under their purview that process personally identifiable information in accordance with OMB Memorandum 03-22 and the E-Government Act.
e. Program Offices/System Owners shall apply all mandated Health Insurance Portability and Accountability Act (HIPAA) Privacy and Security regulations to all systems under their purview that process personal health information.

3.1.1 Information and Information System Categorization

The FIPS Pub 199, *Standards for Security Categorization of Federal Information and Information Systems*, was published in February 2004. This publication is the mandatory standard for categorizing the sensitivity associated with all federal systems except those that deal with national security systems.

FIPS Pub 199 provides federal departments with a more detailed categorization of their information assets than was recognized under the Computer Security Act of 1987. This publication distinguishes among *low*, *moderate*, and *high* sensitivity categories, and deals explicitly with integrity, availability, and confidentiality as security goals. These categories correspond to different degrees of potential impact that a security incident may have on a department's mission, assets, legal responsibilities, functions, or individuals.

The NIST SP 800-60, *Guide for Mapping Types of Information and Information Systems to Security Categories*, provides guidance on assigning sensitivity categories to information systems.

HUD Policy
a. Program Offices/System Owners shall ensure that all systems and data under their purview have been categorized in accordance with FIPS Pub 199, *Standards for Security Categorization of Federal Information and Information Systems*.
b. Program Offices/System Owners shall use NIST SP 800-60, *Guide for Mapping Types of Information and Information Systems to Security Categories*, whenever possible, to assess sensitivity categories of systems and data under their purview.

3.2 Capital Planning and Investment Control

The implementation of IT security and capital planning practices within the federal government is driven by a combination of legislation, rules and regulations, and agency-specific policies. FISMA is the overarching legislation behind the integration of IT security and capital planning. FISMA codifies specific responsibilities of federal agency officials, ensures that agency resources are protected, ensures that risk is effectively managed, and requires agencies to incorporate IT security into the life cycle of their information systems. The agency must also determine the costs and timeframes associated with mitigating the weaknesses identified in the Plans of Action and Milestones (POA&M). These costs are captured in HUD's annual OMB Exhibit 300—the funding vehicle submitted to OMB to secure an operating budget.

HUD has a comprehensive CPIC in place to address the CPIC Process. The IT Investment Management Process addresses all the necessary aspects to develop and manage HUD's IT portfolio in support of its lines of business. HUD also has a management infrastructure in place to coordinate the CPIC process. It consists of two committees: The Technology Investment Board Executive Committee and the Technology Investment Board Working Group (WG).

HUD Policy
a. Program Officials shall include IT security requirements in their capital planning and investment business cases in accordance with NIST SP 800-65, *Integrating IT Security into the Capital Planning and Investment Control Process.*
b. Program Officials shall ensure that IT security requirements are adequately funded and documented in accordance with current OMB budgetary guidance and NIST SP 800-65.
c. The CISO shall certify in writing that adequate security funding is included for all IT infrastructure projects, as appropriate, for the projects' System Development Life Cycle (SDLC) phase.
d. The Technology Investment Board Executive Committee shall not approve any capital investment in which the IT security requirements are not adequately defined and funded.

3.3 Contractors and Outsourced Operations

Computer security requirements must be incorporated in contractual documents that involve the acquisition, development, and/or operation and maintenance (O&M) of computer resources. These requirements must be applied at the beginning of a project or acquisition and in all follow-on contracts or purchasing agreements involving the acquisition of computer resources. Computer resources include hardware, software, maintenance, and other associated IT products and services.

The use of contractors is essential to the success of HUD. Contractors fill a vital role in the daily operations of the department and they too have a responsibility to protect the information they

process. To ensure the security of the information in their charge, contractors must adhere to the same rules and regulations as government employees.

HUD Policy
a. The Office of Procurement and Contracts (OPC) and Contracting Officers (CO) shall ensure that all solicitation documents, SOWs, and applicable contract vehicles identify and document the specific security requirements for IT services and operations that are required of the contractor. • The security requirements shall include how sensitive information is to be handled and protected at the contractor's site. The requirements shall apply to any information stored, processed, or transmitted using the contractor's computer systems, as well as background investigations, clearances, and/or required facility security. • The SOWs and contracts shall require that at the end of the contract, the contractor must return all information and IT resources provided during the life of the contract and must certify that all HUD information has been purged from any contractor-owned system used to process HUD information.
b. OPC and COs shall ensure that all solicitation documents, SOWs, and applicable contract vehicles contain a statement requiring contractors to adhere to HUD IT security policies.
c. The CISO and Program Offices that outsource IT security services shall do so in accordance with NIST SP 800-35, *Guide to Information Technology Security Services*.
d. Program Offices/System Owners shall conduct reviews in accordance with NIST SP 800-26, *Security Self-Assessment Guide for Information Technology Systems,* and NIST SP 800-53, *Recommended Security Controls for Federal Information Systems*, once a year to ensure that contract IT security requirements are implemented and enforced for systems under their purview.

3.4 Performance Measures and Metrics

Security metrics are collected measures of the adequacy of in-place HUD security policies, procedures, and controls. At several organizational levels, the routine collection and review of security metrics help identify new security goals and justify investment in them. NIST SP 800–55, *Security Metrics for Information Technology Systems*, July 2003, provides guidance in the identification and use of security metrics. NIST prescribes the use of readily obtainable quantifiable measures that are capable of repeatable collection to measure progress toward defined security goals. NIST 800-55 defines security metrics of three types:

1. Implementation metrics—used to evaluate compliance with security policy
2. Effectiveness metrics—used to evaluate the effectiveness of security services
3. Impact metrics—used to measure the effect of security events on business or mission

HUD Policy
a. The CIO shall ensure that development, adequate resource assignment, and effective operations of the HUD Security Metrics Program are in accordance with NIST SP 800-55, *Security Metrics for Information Technology Systems*.
b. The CIO, in conjunction with the CISO, shall work with Program Offices, System Owners, and other personnel with information security responsibilities to assure understanding of and compliance with the Metrics Program and to define and track suitable performance measures.
c. Program Offices shall provide the CISO with semiannual data on their progress in implementing IT security performance measures.

3.5 Critical Infrastructure Protection

Critical Infrastructure Protection (CIP) is concerned with providing and maintaining adequate levels of security and redundancy to assure the performance of a minimal set of government and human-related services vital to the protection of people, the stability of the national economy, and the security of the nation. Homeland Security Presidential Directive (HSPD) 7, *Critical Infrastructure Identification, Prioritization, and Protection*, dated December 17, 2003, stipulates that the national goal is to assure that any interruption or manipulation of these critical national infrastructures is brief, infrequent, manageable, geographically isolated, and minimally detrimental to the welfare of the United States. EO 13231 and its amendments (i.e., EO 13284, EO 13286, and EO 13316), *Critical Infrastructure Protection in the Information Age*, reaffirms the need to take continual actions to secure information systems, emergency preparedness communications, and physical assets. It is HUD's policy to have in place a comprehensive and effective program and methodology to identify and protect HUD's national critical assets.

HUD Policy
a. The CIO, in coordination with the Program Offices, shall identify all critical assets in accordance with HSPD 7, *Critical Infrastructure Identification, Prioritization, and Protection,* to determine the interdependencies of these critical assets and develop and implement a CIP Risk Management Plan to ensure that these assets are adequately protected.
b. The CISO shall conduct yearly vulnerability assessments of IT resources that have been identified as part of HUD's critical infrastructure.
c. In the event that the primary and/or alternate telecommunications services are provided by a wireline carrier, the Deputy CIO for IT Operations shall request Telecommunications Service Priority (TSP) for all telecommunications services used for national security emergency preparedness.

3.6 Information Technology Contingency Planning

Information technology contingency planning refers to the interim measures needed to recover IT services following an emergency or system disruption. Interim measures may include the relocation of IT systems and operations to an alternate site, the recovery of IT functions using alternate equipment, or the performance of IT functions using manual methods.

The IT contingency planning is an integral part of CIP and COOP planning; therefore, this policy supports CIP and COOP. The planning is also closely related to the Business Impact Analysis (BIA) portion of COOP. The BIA identifies, among other things, the impact on business-function missions, if the system is unavailable for a specific amount of time. The IT Contingency Plan will consider the CIP, COOP Plans, and BIAs in establishing processing priorities.

HUD Policy
a. The CISO shall develop, document, and maintain a standard HUD-wide process for IT contingency planning in accordance with NIST SP 800-34, *Contingency Planning Guide for Information Technology Systems.*
b. Program Offices/System Owners shall develop contingency plans for information systems under their purview in accordance with NIST SP 800-34. For systems rated moderate or high, Program Offices/System Owners shall coordinate with the Program Office responsible for CIP and COOP.

HUD Policy
c. Program Offices/System Owners shall review contingency plans once a year, update them, and communicate any changes to the Program Office responsible for COOP and CIP, if applicable.
d. Program Offices/System Owners shall ensure that all personnel involved in IT contingency planning efforts are identified and trained in the procedures and logistics of IT contingency planning and implementation for systems under purview rated moderate or high. Refresher training shall be provided annually. For systems rated high, the training shall include simulated events.
e. Program Offices/System Owners shall ensure that plans for systems rated moderate or high are tested/exercised at least annually. Testing should be coordinated with elements responsible for COOP, CIP, and incident response. For systems rated high, the Program Offices/System Owners shall ensure testing at the alternate processing site.
f. The Deputy CIO for IT Operations shall provide an alternate site for storing system backup information. The alternate site must be geographically separated from the primary storage site for backup information of systems rated moderate or high. For systems rated high, the storage site shall: • Be configured to facilitate timely and effective recovery operations • Identify potential accessibility problems in the event of an area-wide disruption or disaster and outline explicit mitigation actions
g. The Deputy CIO for IT Operations shall provide an alternate processing site for systems rated moderate or high and ensure that the equipment and supplies required to resume operations are either available at the alternate site or contracts are in place to support delivery to the site. The alternate site shall: • Be geographically separated from the primary processing site • Be reviewed to identify potential accessibility problems in the event of an area-wide disruption or disaster and outline explicit mitigation actions • Have priority-of-service provisions in accordance with HUD's availability requirements For systems rated high, the site shall be fully configured to support a minimum required operational capability and ready to use as the operational site.
h. The Deputy CIO for IT Operations shall provide for primary and alternate telecommunications services to support systems rated moderate and high. The Deputy CIO for IT Operations shall also initiate the necessary agreement to permit the resumption of system operations for critical business within 24 hours when primary telecommunications are unavailable. The Deputy CIO for IT Operations shall ensure that: • Agreements contain priority-of-service provisions in accordance with HUD's availability requirements • Alternate service does not share a single point of failure with the primary service For systems rated high, the Deputy CIO for IT Operations shall ensure that: • Providers of alternate sites are sufficiently separated from primary service providers so they are not susceptible to the same hazards • Providers of primary and alternate services have adequate contingency plans
i. The Deputy CIO for IT Operations shall ensure that HUD has mechanisms with supporting procedures to allow the information system to be recovered and reconstituted to the systems original state after a disruption or failure. For systems rated high, the Deputy CIO for IT Operations shall ensure that the systems are fully recovered and reconstituted as part of the contingency plan test.

3.7 System Development Life Cycle

All federal information systems, including operational systems, systems under development, and systems undergoing modification or upgrade, are in some phase of what is commonly referred to

as the SDLC. Many activities during a system's life cycle have cost, schedule, and performance implications. In addition to the functional requirements levied on an information system, security requirements must also be considered. When fully implemented, the information system must be able to meet its functional requirements and do so in a manner that is secure enough to protect agency operations, assets, and individuals.

In accordance with the provisions of FISMA, agencies are required to have an agency-wide Information Security Program and that program must be effectively integrated into the SDLC.

HUD Policy
a. Program Offices/System Owners shall ensure that security is integrated into the SDLC from IT system inception to system disposal through adequate and effective management, personnel, operations, and technical control mechanisms in accordance with NIST SP 800-64, *Security Considerations in the Information System Development Life Cycle.*
b. Program Offices/System Owners shall ensure information systems that have been rated moderate or high are designed and implemented using security engineering principles in accordance with NIST SP 800-27 Rev A, *Engineering Principles for Information Technology Security (A Baseline for Achieving Security)*.
c. Program Offices/System Owners shall ensure information systems that have been rated moderate or high physically or logically separate user interface services (e.g., public web pages) from information storage and management services (e.g., database management). Separation may be accomplished using different computers, different central processing units, different instances of the operating system, different network addresses, combinations of these methods, or other methods as appropriate.

3.8 Configuration Management

Configuration Management's (CM) primary concern is managing the configuration of all hardware and software elements of IT systems and networks and the security implications when changes occur. The initial configuration of the system or network must be documented in detail and all subsequent changes to any components must be controlled through a complete and robust CM process. Configuration Management has security implications in three areas to ensure:

- The configuration in which the system or network is actually installed and operated is consistent with the one under which its security C&A was performed.
- Any subsequent changes have been approved, including an analysis of any potential security implications.
- All recommended and approved security patches are properly installed.

HUD Policy
a. Program Offices/System Owners shall prepare Configuration Management Plans for all IT systems and networks under their purview. The plan must include a baseline configuration. For moderate to high-impact systems, the system shall use automated mechanisms to maintain an up-to-date, complete, accurate, and readily available baseline configuration. The baseline is updated during installations.
b. Program Offices/System Owners shall establish, implement, and enforce change management and CM controls on all IT systems and networks under their purview. Changes to the information system must be documented and they must include emergency change procedures. For high-impact systems, the system shall use automated mechanisms to:

HUD Policy
• Document proposed changes • Notify appropriate approval authorities • Highlight approvals that have not been received in a timely manner • Inhibit changes until necessary approvals are received • Document completed changes
c. IT security patches shall be installed in accordance with Configuration Management Plans or from direction of higher authorities.
d. Program Offices/System Owners shall monitor and audit changes to information systems under their purview and conduct security impact analysis as required by NIST SP 800-37 and check the security features of the system to ensure the features are still functioning properly.
e. Program Offices/System Owners shall ensure that changes to the information system are restricted to a limited number of personnel who require access for their job responsibilities. For high-impact systems, the system shall use an automated mechanism to enforce the restrictions and provide audit information.
f. Program Offices/System Owners shall ensure that security settings have been set to their most restrictive values consistent with operational requirements. For COTS packages, Program Offices/System Owners shall consult NIST SP 800-70, *Security Configuration Checklists Program for IT Products* for the Configuration Checklist and configure the system accordingly. For high-impact systems, the system shall use automated mechanisms to centrally apply and verify configuration settings.
g. Program Offices/System Owners of systems that have been rated high shall ensure that their software and information are protected against unauthorized changes. The Program Offices/System Owners shall use automated tools to monitor the integrity of such information and software. Acceptable methods for COTS packages include, but are not limited to, parity checks, cyclical redundancy checks, and cryptographic hashes.
h. Program Offices/System Owners of systems under development that have been rated high shall ensure that the system developer creates and implements a configuration management plan that controls changes to the system during development, tracks security flaws, requires authorization of changes, and provides documentation of the plan and its implementation.
i. Program Offices/System Owners of systems under development that have been rated moderate or high shall ensure that the system developer creates a security test and evaluation plan, implements the plan, and documents the results. Developmental security test results should only be used when no security relevant modifications of the information system have been made subsequent to developer testing and after selective verification of developer test results.

3.9 Risk Management and Risk Assessment

Risk assessment is a process of identifying system security risks and determining the probability of occurrence, resulting impact, and additional safeguards that would mitigate this impact. Risk management is a process that allows Program Officials to balance the operational and economic costs of protective measures to achieve gains in mission capability by protecting the IT systems and data that support their organization's missions. It is the total process of managing risks to agency operations, agency assets, or individuals resulting from the operation of an information system. It includes risk assessment and Cost-Benefit Analysis (CBA); as well as the selection, implementation, testing, and security evaluation of safeguards. This overall system security review considers both effectiveness and efficiency, including the impact on the mission and constraints due to policy, regulations, and laws.

As a preliminary risk assessment, Program Offices/System Owners shall ensure that all systems and data under their purview have been categorized in accordance with FIPS 199, *Standards for the Security Categorization of Federal Information and Information Systems*.

HUD Policy
a. Program Offices/System Owners shall ensure that all systems under their purview have been subjected to a current risk assessment in accordance with the NIST SP 800-30, *Risk Management Guide for Information Technology Systems*. Risk assessments are required prior to the start of C&A.
b. Program Offices/System Owners shall conduct a risk assessment every three years and when a significant change is planned for any system under their purview.
c. Program Offices/System Owners shall conduct an "e-authentication risk assessment" of the transactional systems under their purview that provide government services using the Internet. The risk assessment shall be conducted in accordance with OMB guidance under OMB-04-04, *E-Authentication Guidance for Federal Agencies.*

3.10 Certification and Accreditation

Security accreditation is the official management decision given by a senior agency official to authorize the operation of an information system and to explicitly accept the risk to agency operations, agency assets, or individuals based on the implementation of an agreed-upon set of security controls. By accrediting an information system, the Authorizing Official accepts responsibility for the security of the system and is fully accountable for any adverse impacts to the agency if a breach of security occurs.

Security certification is a comprehensive assessment of the suitability and effectiveness of management, operational and technical security controls in an information system. This assessment is made in support of security accreditation to determine the extent to which the controls are being implemented correctly, operating as intended, and producing the desired outcome with respect to meeting system security requirements. The results of the security certification are used to reassess the risks and update the system security plan, thus providing the factual basis for an AO to render a security accreditation decision.

Completing a security accreditation ensures that an information system will be operated with appropriate management review, that there exists ongoing monitoring of security controls, and that reaccreditations occurs periodically in accordance with federal or HUD policy, including when there is a significant change to the system or its operational environment.

HUD Policy
a. Program Offices/System Owners shall follow the guidelines contained in NIST SP 800-37, *Guidelines for the Security Certification and Accreditation of Federal Information Technology Systems*, in certifying and accrediting their information systems.
b. Program Offices/System Owners shall ensure that whenever changes are made to IT systems, networks, or to their physical environment, interfaces, or user-community makeup, the impact on the security of the information processed is reviewed via a documented security-impact analysis as required by NIST SP 800-37.
c. Program Offices/System Owners shall ensure that systems are certified and accredited at their initial operating capability every three years thereafter and whenever a significant change occurs in accordance with NIST 800-37.

HUD Policy
d. Existing accreditations completed before the issuance of this policy shall remain in effect if the accreditation complied fully with the policy in effect at the time of accreditation, no significant deficiencies have been identified, and the system configuration has not changed since accreditation.
e. Program Offices shall update their POA&Ms on a quarterly basis for systems under their purview as required by OMB.
f. Program Offices/System Owners shall conduct an annual security review of systems under their purview in accordance with NIST SP 800-26, *Security Self-Assessment Guide for Information Technology Systems,* and NIST SP 800-53, *Recommended Security Controls for Federal Information Systems*. The results of such reviews shall be included in the annual FISMA report to OMB.
g. Program Offices/System Owners shall conduct vulnerability assessments and/or security testing to identify vulnerabilities in IT systems under their purview. These assessments shall be conducted yearly and when significant changes are made to the IT systems.
h. Program Offices/System Owners shall authorize and monitor all connections between systems under their purview and other systems outside the accreditation boundary. The connection(s) shall be documented in an Interconnection Security Agreement in accordance with NIST SP 800-47, *Security Guide for Interconnecting Information Technology Systems*.
i. The CISO shall implement a standard C&A methodology for all HUD systems.
j. Program Offices/System Owners shall use this methodology for all C&As.

3.11 Incidents, Violations, and Disciplinary Action

Individual accountability is a cornerstone of an effective security policy. If individuals are not held accountable for their actions, there is little incentive for compliance. Program Office heads are responsible for holding personnel accountable for intentional transgressions and for taking corrective actions when security incidents and violations occur. Corrective action does not necessarily mean disciplinary action. Sometimes remedial training is more appropriate. Each Program Office must determine how best to address each individual case.

An incident is a violation or imminent threat of violation of information security policies, acceptable use policies, or standard computer security practices. Incidents may result from intentional or unintentional actions. Inappropriate uses of HUD computer resources are also considered security incidents.

HUD Policy
a. HUD employees may be subject to disciplinary action for failure to comply with HUD security policies, whether or not the failure results in criminal prosecution. IT security-related violations are addressed in U.S. Department of Housing and Urban Development Ethics Letters 92-1, *Standards of Conduct and Principles of Ethical Service for Federal Employees.*
b. HUD contractors and external users who fail to comply with department security policies shall be subject to having their access to HUD IT systems and facilities terminated, whether or not the failure results in criminal prosecution.
c. Any person who improperly discloses sensitive information shall be subject to criminal and civil penalties and sanctions under a variety of laws (e.g., the Privacy Act).

4.0 OPERATIONAL POLICIES

4.1 Personnel

HUD systems face threats from many sources, including the actions of HUD employees, external users, and contractor personnel. The intentional and unintentional actions of these individuals can potentially harm or disrupt HUD systems and their facilities. These actions can result in the destruction or modification of the data being processed, denial of service (DoS) to the end users, and unauthorized disclosure of data, potentially jeopardizing HUD's mission. Therefore, it is highly important that stringent safeguards be taken to reduce the risk associated with these types of threats.

HUD Policy
a. Program Offices shall designate the position sensitivity level for all government positions that use, develop, operate, or maintain IT systems under their purview and shall determine risk levels for each contractor position in accordance with the Office of Personnel Management (OPM) policy and guidance. Position sensitivity levels and risk levels shall be reviewed periodically in accordance with OPM guidance.
b. Program Offices shall ensure that the incumbents of these positions have favorably adjudicated background investigations commensurate with the defined position's sensitivity levels. Screening shall be consistent with: (i) 5 Code of Federal Regulations (CFR) 731.106(a); (ii) OPM policy, regulations, and guidance; (iii) organizational policy, regulations, and guidance; (iv) FIPS 201 and its attendant SP 800-73 and 800-76; and (v) the criteria established for the risk designation of the assigned position.
c. Program Offices/System Owners shall ensure that no employee is granted access to HUD systems without having a favorably adjudicated Minimum Background Investigation (MBI), as defined in HUD's *Personnel Security Program* for systems under their purview.
d. Program Offices/System Owners shall ensure that no contractor employee is granted access to HUD systems under their purview without having a favorably adjudicated background Investigation, as defined in HUD's Handbook 732.3, *Personnel Security/Suitability*. Exceptions may be granted by the CISO.
e. Program Offices/System Owners shall ensure that no government employee is granted access to HUD systems processing sensitive information under their purview who is not a citizen of the United States. Exceptions may be granted at the Program Office level and must be reported to the CISO and the security officer.
f. Program Offices/System Owners shall ensure that no contractor employee is granted access to HUD systems processing sensitive information under their purview who is not a citizen of the United States, a national of the United States (see 8 U.S.C. 1408), or an alien lawfully admitted to the United States for permanent residence. Exceptions may be granted at the Program Office level and reported to the CISO and the security officer.

4.1.1 Rules of Behavior

Rules of behavior are part of a comprehensive program to provide complete information security guidelines. The rules of behavior establish standards of behavior in recognition of the fact that knowledgeable users are the foundation of a successful Information Security Program. These guidelines are established to hold users accountable for their actions and responsible for IT security.

HUD Policy
a. The CISO shall define generic rules of behavior for all IT systems.
b. Program Offices/System Owners shall define additional rules of behavior for all IT systems under their purview, when necessary.
c. ISSOs shall ensure that users of systems sign the rules of behavior and are given training regarding the rules of behavior and the disciplinary actions that may result if the rules are violated.

4.1.2 Access to Sensitive Information

To protect sensitive information and limit the damage that can result from accident, error, or unauthorized use, the principle of least privilege must be applied. The principle of least privilege requires that users be granted the most restrictive set of privileges (or lowest clearance) needed to perform authorized tasks (i.e., users should be able to access only the system resources needed to fulfill their job responsibilities).

The application of this principle ensures that access to sensitive information is granted only to those users with a valid need to know.

HUD Policy
a. Program Offices/System Owners shall ensure that users of IT systems supporting their programs have a validated requirement to access these systems.
b. Program Offices/System Owners shall ensure that users of IT systems under their purview have approved access requests prior to granting access to the systems.

4.1.3 Separation of Duties Policy

Separation of duties is designed to prevent a single individual from being able to disrupt or corrupt a critical security process. This separation is necessary for adequate internal control of sensitive IT systems.

HUD Policy
a. Program Offices/System Owners shall divide and separate duties and responsibilities of critical IT system functions among different individuals to minimize the possibility that any one individual would have the necessary authority or systems access to be able to engage in fraudulent or criminal activity.

4.1.4 Training and Awareness

A key objective of an effective Information Security Program is to ensure that all employees and contractors understand their roles and responsibilities and are adequately trained to perform them. HUD cannot protect the confidentiality, integrity, and availability of its IT systems and the information they contain without the knowledge and active participation of its employees and contractors in the implementation of sound security principles.

HUD Policy
a. The CISO shall establish an IT security awareness and training program in accordance with NIST 800 SP 800-50, *Building an Information Technology Security Awareness and Training Program*. The program shall be consistent with CFR 930.301.

HUD Policy
b. Program Offices/System Owners shall establish additional system-specific security training for sensitive systems under their purview, when necessary.
c. Program Offices/System Owners shall ensure that HUD personnel and contractors accessing HUD IT systems receive initial training in security awareness and accepted security practices as part of their orientation. They shall sign the rules of behavior and receive refresher training by May 31 of each year.
d. Program Offices/System Owners shall ensure that HUD personnel and contractors with significant security responsibilities (e.g., ISSOs and system administrators) receive annual specialized training specific to their security responsibilities. The level of training shall be commensurate with the individual's duties and responsibilities and promote a consistent understanding of the principles and concepts of IT system security.
e. Program Offices shall maintain training records that include the individual names and positions, types of training received, and cost of training.
f. Unless a waiver is granted by the CISO, user accounts and access privileges, including access to email, will be disabled for those HUD employees who have not received annual refresher training.
g. Program Offices shall prepare and submit an IT Security Professional Training Plan to the CISO by September 1 of each year.
h. Program Offices shall prepare and submit awareness and training statistics semiannually to the CISO. These statistics shall include the (1) total number of personnel and the total number of personnel who received awareness training and (2) total number of IT security personnel and the total number who were trained.

4.1.5 Separation from Duty

This section addresses HUD's policy for an employee or contractor who terminates employment or transfers to another organization.

HUD Policy
a. Program Offices/System Owners shall implement procedures to ensure that system accesses are revoked or reassigned when HUD or contractor employees either change their employer or are reassigned to other duties. The procedures shall include: • Exit interviews • Process for returning all organizational information and system-related property (e.g., keys and ID cards) • Access by appropriate personnel to official records created by the terminated/transferred employee/contractor that are stored on organizational information systems • Formal notification to the facilities group or security officer

4.2 IT Physical Security

HUD security personnel and users must address physical security as an integral element in the effective implementation of an Information Security Program. Physical security represents the first line of defense against intruders and adversaries attempting to gain access to HUD facilities and or information systems.

4.2.1 General Physical Access

General physical access controls restrict the entry and exit of personnel from a protected area, such as an office building, data center, or room containing IT equipment. They include the protection of sensitive data and systems while in rest, as well as while away from the protection of HUD facilities. These controls protect against threats associated with the physical environment. It is important to review the effectiveness of general physical access controls in each area during business hours and at other times. Effectiveness depends not only on the characteristics of the controls used but also on their implementation and operation.

Homeland Security Presidential Directive 12 mandates government-wide standard for secure and reliable forms of identification issued by the federal government to its employees and contractors (including contractor employees). Program Offices responsible for issuing ID badges at HUD shall consult FIPS 201 and its attendant SP 800-73 and SP 800-76 for specific guidance.

HUD Policy
a. The facilities group or security officer shall ensure that access to HUD buildings, rooms, work areas, and spaces is limited to authorized personnel. Controls shall be in place for deterring, detecting, monitoring, restricting, and regulating access to specific areas at all times.
b. The facilities group or security officer shall ensure that all visitors sign in and out when entering and leaving the facility. Visitor logs shall be reviewed at closeout, maintained on file, and available for further review for one year. Contractors' access shall be limited to those work areas requiring their presence. Records of their ingress and egress shall also be maintained for one year. For systems rated moderate or high, the maintenance and review of access logs shall use automated mechanisms.
c. For systems rated moderate or high, the facilities group or security officer shall ensure that all visitors are escorted.
d. For systems rated moderate or high, individuals within HUD shall employ appropriate security controls at alternate work sites in accordance with NIST SP 800-46, *Security for Telecommuting and Broadband Communications*. These individuals shall report security problems to HUD's Computer Security Incident Response Center (CSIRC).
e. Program Offices and users shall ensure that unattended laptops in offices are secured via a locking cable, locked office, or a locked cabinet or desk.

4.2.2 Facilities Housing Information Technology Assets

Facilities supporting large-scale IT operations (e.g., enterprise servers and telecommunication facilities) require additional environmental and physical controls as determined by a risk analysis.

Section 4.2.1 provides policies for both general physical access and sensitive facilities. For facilities supporting large-scale IT operations, all of the following physical security controls also must be addressed. The risk assessment shall specifically document the rationale for not incorporating any such physical security controls.

HUD Policy
a. The Deputy CIO for IT Operations shall ensure that facilities processing, transmitting, or storing sensitive information incorporate physical protection measures. These facilities include data centers, wiring closets, server rooms at non-HUD facilities, contractor facilities housing HUD IT systems, and in some cases, areas designated as publicly accessible inside HUD facilities.

HUD Policy
b. The facilities group or security officer shall ensure that lists of personnel authorized to access these facilities are current and shall issue appropriate credentials. Access shall be promptly removed for personnel no longer needing it.
c. The Official responsible for approving initial access to these facilities shall review and approve access lists and authorization credentials once a year.
d. The facilities group or security officer shall control all access points with physical access devices and/or guards. Keys, combinations, and other access devices shall be secured and inventoried every six months and changed any time the keys are lost, combinations are compromised, or individuals are terminated or transferred.
e. The facilities group or security officer shall develop and implement procedures to ensure that only authorized individuals can reenter the facility after emergency-related events.
f. For systems rated moderate or high, the Program Offices/System Owners shall ensure that physical access to devices displaying information is controlled to prevent unauthorized disclosure.
g. The facilities group or security officer shall monitor physical access to detect and respond to incidents. Logs shall be reviewed daily for apparent security violations or suspicious activities and responded to accordingly. For systems rated moderate or high, the monitoring shall be in real-time for intrusion alarms and surveillance equipment. For systems rated high, the monitoring shall use automated mechanisms to recognize intrusions and to take appropriate action.
h. For systems rated moderate or high, the facilities group or security officer shall ensure that power equipment and cabling are protected from damage and destruction.
i. For specific locations within a facility containing concentrations of information system resources (e.g., data centers and server rooms), the facilities group or security officer shall provide for the capability of shutting off power to any IT component that may be malfunctioning (e.g., due to an electrical fire) or threatened (e.g., due to a water leak) without endangering personnel by requiring them to approach the equipment.
j. For specific locations within a facility containing concentrations of information system resources (e.g., data centers and server rooms), the facilities group or security officer shall maintain a redundant air-cooling system.
k. The facilities group or security officer shall provide short-term UPS to facilitate an orderly shutdown in the event of a primary power source loss.
l. The facilities group or security officer shall provide a long-term alternate power supply to maintain minimal operational capability for systems rated moderate or high in the event of an extended loss of the primary power source.
m. The facilities group or security officer shall provide automatic emergency lighting systems that activate in the event of a power outage or disruption and cover emergency exits and evacuation routes.
n. The facilities group or security officer shall provide fire suppression and detection devices/systems that can be activated in the event of fire. The devices/systems shall include, but are not limited to: • Sprinkler systems • Handheld fire extinguishers • Fixed fire hoses • Smoke detectors
o. For systems rated moderate or high, the facilities group or security officer shall provide fire suppression devices/systems that activate automatically in the event of fire.
p. For systems rated high, the facilities group or security officer shall provide fire suppression devices/systems that automatically notify any activation to the organization and emergency responders in the event of fire.

HUD Policy
q. The facilities group or security officer shall ensure that facilities containing information systems monitor and maintain acceptable levels of temperature and humidity.
r. The facilities group or security officer shall ensure that the information systems contained in the facility are protected from water damage resulting from broken plumbing lines or other sources of water leakage by ensuring that master shutoff valves are accessible, working properly, and known to key personnel. For systems rated high, the shutoff shall use automatic mechanisms in the event of a significant water leak.
s. The facilities group or security officer shall ensure that the facility has procedures to control the entering and exiting of information system-related items and maintains appropriate records. Delivery and removal of these items shall be authorized by an appropriate HUD official. If possible, the delivery area shall be separate from the system and media library area.

4.3 Media Controls

Information resides in many forms and can be stored in many different ways. Media controls are protective measures specifically designed to safeguard electronic data and hardcopy information. This policy addresses the protection, marking, sanitization, production input/output, and disposal of media containing sensitive information. Media destruction and disposal should be accomplished in an environmentally approved manner. The National Security Agency (NSA) provides media destruction guidance at http://www.nsa.gov/ia/government/mdg.cfm.

Proper storage of hardcopy and magnetic media enhances protection against unauthorized disclosure. There are additional security risks associated with the portability of removable storage media. Loss, theft, or physical damage to disks and other removable media can compromise the confidentiality, integrity, or availability of the data contained in these devices.

HUD Policy
a. Program Offices/System Owners shall establish procedures to ensure that sensitive information in printed form or digital media cannot be accessed, removed, or stolen by unauthorized individuals.
b. Program Offices/System Owners and users shall ensure that all media containing sensitive information rated moderate or high is appropriately marked with the sensitivity of the information stored on the media. At a minimum, printed output that is not otherwise appropriately marked shall have a cover sheet and digital media shall be labeled with the distribution limitations, handling caveats, and applicable security markings, if any, of the information. Systems rated high shall use an automated marking mechanism.
c. Program Offices/System Owners and users shall control access to and securely store all information system media (i.e., both paper and digital) containing sensitive information rated moderate or high, including backup and removable media, in a secure location when not in use.
The following policy statements apply only to media that contain information that has been rated moderate or high.
d. Program Offices/System Owners shall ensure that any sensitive information stored on media that will be surplused or returned to the manufacturer shall be purged from the media before disposal.
e. Disposal shall be performed using approved sanitization methods in accordance with NIST SP 800-36, *Guide to Selecting Information Security Products.*
f. Program Offices/System Owners shall maintain records certifying that such sanitization was performed.

HUD Policy
g. Program Offices/System Owners shall establish procedures to ensure that sensitive information stored on any media is transferred to an authorized individual upon the termination or reassignment of an employee or contractor.
h. Program Offices/System Owners shall ensure that sensitive information is purged from the hard drives of any workstation or server returned to the equipment surplus pool or transferred to another individual.
i. Program Offices/System Owners shall ensure that media (e.g., paper, diskettes, and removable disk drives) containing sensitive information is destroyed in such a manner that all sensitive information on that media cannot be recovered by ordinary means. Examples of appropriate methods are crosscut shredders, degaussing, and approved disk-wiping software.
j. Program Offices/System Owners shall maintain records certifying that such destruction was performed.
k. Program Offices/System Owners shall establish procedures to ensure that sensitive information in printed form or digital media can only be picked up, received, transferred, or delivered to authorized individuals.
The following policy statements apply only to media that contain information that has been rated high.
l. Program Offices/System Owners shall ensure that access to media storage areas is controlled through guard stations or automated mechanisms that ensure only authorized access. All access and access attempts shall be audited.

4.4 Data Communications

4.4.1 Telecommunications Protection Techniques

Extreme caution should be exercised when telecommunications protection techniques (e.g., protective distribution systems) are being considered as alternatives to the use of encryption. While such technologies may represent a lower-cost approach, they may not provide an adequate level of protection.

The FIPS 199 security category (for integrity) of the information being transmitted should guide the decision on the use of cryptographic mechanisms. NSTISSI No. 7003 contains guidance on the use of Protective Distribution Systems.

HUD Policy
a. Program Offices/System Owners shall ensure that the integrity of the information in systems under their purview is protected during transmission. For systems rated high, the system shall employ cryptographic mechanisms to ensure recognition of changes to information during transmission, unless adequately protected by alternative physical measures (e.g., protective distribution systems).
b. Program Offices/System Owners shall ensure that the confidentiality of the information in systems under their purview is protected during transmission. For systems rated high, the system shall employ cryptographic mechanisms to prevent unauthorized disclosure of information during transmission, unless otherwise protected by adequately physical measures (e.g., protective distribution systems).

4.5 Wireless Communications

Wireless communications are inherently insecure. Program Offices/System Owners implementing wireless capabilities must ensure that the transmission and storage of sensitive information are protected from compromise.

4.5.1 Wireless Local Area Networks

HUD Policy
a. The CISO shall approve the implementation and use of all Wireless Local Area Networks (WLAN) and wireless Access Points (AP) at a specified risk level and only after they have been certified and accredited.
b. The Deputy CIO for IT Operations shall ensure that all WLANs and WAPs have been configured in accordance with *NIST SP 800-48, Wireless Network Security.*
c. The Deputy CIO for IT Operations shall implement encryption and strong identification and authentication (e.g., Extensible Authentication Protocol with Wi-Fi Access Protection (WAP) or IEEE 802.11i) on WLANs and APs that have been rated moderate or high.
d. The CISO shall scan for rogue access points on HUD's network annually.

4.6 Hardware and Software

This section addresses the use and maintenance of computer equipment. It stresses the importance of individual accountability in protecting these resources. Equipment security encompasses workstations, laptops, other mobile computing devices, personally-owned equipment, and the maintenance of these items.

4.6.1 Workstations

All users must be instructed to log off or lock their workstations any time the workstations are left unattended. As an added precaution, users should also use a password-protected screensaver.

HUD Policy
a. All users shall ensure that their unattended workstations are either logged off or locked, or that a password-protected screensaver is used.
b. The Deputy CIO for IT Operations shall provide and implement password-protected screen savers on all workstations owned/leased by HUD. The screen saver shall automatically lock the workstation after ten minutes of inactivity. Program Offices/System Owners of systems rated moderate to high shall require that contractors and business partners who connect to the systems implement such a screen saver.

4.6.2 Copyrighted Software

Computer software purchased using HUD funds is HUD property and shall be protected as such. Only licensed and approved operating systems and applications may be used on HUD equipment.

HUD Policy
a. Program Offices/System Owners shall ensure that users abide by copyright and contract agreements related to HUD-provided software. For software and associated documentation protected by quantity licenses, the Program Offices/System Owners shall use tracking systems to control copying and distribution.
b. Program Offices/System Owners that use peer-to-peer file sharing technology on their information system shall control and monitor its use to ensure that this capability is not used for unauthorized distribution, display, performance, or reproduction of copyrighted work.

4.6.3 User-Installed Software/Downloads

User-installed software, including downloaded software, can contain viruses and other types of malicious code. In addition, such software can alter the HUD equipment configuration causing malfunctions and costly support calls. Users should be warned about such risks and instructed to refrain from installing any software on HUD equipment without proper approval.

HUD Policy
a. Users shall not install any software on HUD-owned or leased equipment without prior written approval from the Deputy CIO for IT Operations.

4.6.4 Personally-Owned Equipment and Software

Users shall not use personally owned equipment (e.g., laptop computers or personal digital devices [PDA]) or software to process, access, or store sensitive information. Such equipment also includes plug-in and wireless peripherals (e.g., Blackberry) that may employ removable media (e.g., CDs and DVDs), Universal Serial Bus (USB) flash (thumb) drives, external drives, and diskettes.

HUD Policy
a. Users shall not use personally-owned equipment and software to process, access, or store sensitive information without prior written approval from the Program Offices/System Owners.
b. Employees and contractors shall not connect equipment not owned or leased by HUD-to-HUD equipment or networks without prior written approval from the CISO.
c. The written approval shall include a terms and conditions statement that addresses at a minimum: (i) the types of applications that can be accessed from personally-owned information systems; (ii) the maximum FIPS 199 security category of information that can processed, stored, and transmitted; (iii) how other users of the personally-owned information system will be prevented from accessing federal information; (iv) the use of virtual private network (VPN) and firewall technologies; (v) the use of and protection against the vulnerabilities of wireless technologies; (vi) the maintenance of adequate physical security controls; (vii) the use of virus and spyware protection software; and (viii) how often the security capabilities of installed software are to be updated (e.g., operating system and other software security patches, virus definitions, firewall version updates, and spyware definitions).

4.6.5 Hardware and Software Maintenance

Program Offices/System Owners must be cognizant of the threats and vulnerabilities associated with hardware or software maintenance on IT systems. System maintenance requires either physical or logical access to the system. One of the most common methods hackers use to break

into systems is through maintenance accounts that still have factory-set or easily guessed passwords. War-dialing techniques will also reveal maintenance ports that are not protected.

HUD Policy
a. Program Offices/System Owners shall confine access to system software and hardware to authorized personnel.
b. The Deputy CIO for IT Operations shall ensure that routine preventive and regular maintenance are performed on software and hardware according to manufacturer/vendor specifications and/or organizational requirements. For systems that have been rated moderate or high a log shall be maintained for such maintenance and include the following: • Date and time of maintenance • Name of individual performing the maintenance • Name of escort, if necessary • Description of maintenance performed • A list of equipment removed or replaced (including identification numbers, if applicable). For systems rated high, the Deputy CIO for IT Operations shall use an automated mechanism to ensure that the maintenance is scheduled and conducted, as required.
c. The Deputy CIO for IT Operations shall ensure that an appropriate organizational official approves the removal of the information system or its components from the facility when repairs are necessary. The Deputy CIO for IT Operations shall ensure that the security features of the system are checked to ensure proper functioning when it is returned.
d. The Deputy CIO for IT Operations shall ensure that appropriate organization officials approve, control, and monitor the use of information system maintenance tools and maintain such tools on an ongoing basis.
e. The Deputy CIO for IT Operations shall ensure that maintenance ports are disabled by default and enabled only during maintenance.
f. The Deputy CIO for IT Operations shall ensure that the appropriate organizational officials approve, control, and monitor remotely executed maintenance and diagnostic activities. The Deputy CIO for IT Operations shall ensure that all sessions are terminated when remote maintenance is completed. If password-based authentication is used, the Deputy CIO for IT Operations shall ensure that passwords are changed following each maintenance service. For high-impact systems, the Deputy CIO for IT Operations shall ensure that logs for such activities are maintained and periodically reviewed.
g. The Deputy CIO for IT Operations shall ensure that only authorized individuals perform maintenance on information systems. If maintenance personnel need access to organizational information, they must be supervised by organizational personnel with authorized access to such information.
h. The Deputy CIO for IT Operations shall identify critical components that support systems rated moderate or high and ensure that maintenance support and parts are provided within 48 hours of failure.
i. The Deputy CIO for IT Operations shall ensure that all default vendor or factory-set administrator accounts and passwords shall be changed before installation or use on all systems owned or operated on behalf of HUD.
j. Program Offices/System Owners of information systems that have been rated high shall address the installation and use of remote diagnostic links in the system security plan.

HUD Policy
k. The Deputy CIO for IT Operations shall ensure that remote diagnostic or maintenance services for information systems that have been rated high are only performed by a service or organization that implements for its own information system the same level of security as that implemented on the information system being serviced. If remote diagnostic or maintenance services are required from a service or organization that does not implement for its own information system the same level of security as that implemented on the system being serviced, the system being serviced is sanitized and physically separated from other information systems prior to the connection of the remote access line. If the information system cannot be sanitized (e.g., due to a system failure), remote maintenance is not allowed.

4.6.6 Personal Use of Government Office Equipment and HUD Information Systems/Computers

This section discusses HUD policies applicable to the personal use of government office equipment and HUD information systems. Policies governing personal use may be contained in several HUD management directives.

HUD Policy
a. HUD employees may use government office equipment and HUD information systems/computers for authorized purposes only. "Authorized use" includes limited personal use of HUD email and Internet services, so long as use does not interfere with official duties, cause degradation of network services, or violate the rules of behavior.
b. Contractors and other non-HUD employees are not authorized to use government office equipment or information systems/computers for personal use, unless limited personal use is specifically permitted by the governing contract or Memorandum of Agreement (MOA).

4.7 General IT Security

This section provides guidance in the areas of incident reporting, contingency planning, documentation, and backup procedures. It stresses the role of the user, as well as the security professional, in the implementation of the operational controls associated with these areas.

4.7.1 Security Incident and Violation Handling

Incidents can be accidental or malicious, can be caused by outside intruders or internal employees, and can cause significant disruptions to mission-critical business processes. These incidents can severely disrupt computer-supported operations, compromise the confidentiality of sensitive information, and diminish the integrity of critical data.

To help combat the disruptive short- and long-term effects of security incidents, direction from higher authority (e.g., OMB, FISMA, and Presidential directives) requires that each government agency implement and maintain a security incident reporting and handling capability.

The HUD Security Incident Reporting and Handling Program requires participation by all Program Offices/System Owners; thus, a CSIRC has been established. The CSIRC is the focal point for the implementation of HUD's incident response capability.

HUD Policy
a. The CISO shall establish and maintain a HUD CSIRC to prevent, detect, track, and respond to information security incidents and alerts in accordance with NIST SP 800-61, *Computer Security Incident Handling Guide*. Lessons learned from ongoing incident handling activities shall be incorporated into the procedures and implemented accordingly. For systems rated moderate or high, the CISO shall provide automated mechanisms to support the incident handling process.
b. Program Offices/System Owners of systems rated moderate or high shall ensure that security alerts, advisories, Intrusion Detection System (IDS) alerts, and vulnerabilities identified during vulnerability scans and penetration tests are tracked and responded to as security incidents.
c. The Deputy CIO for IT Operations shall test patches, service packs, and hot fixes for effectiveness and potential side effects prior to installation in accordance with NIST SP 800-40, *Procedures for Handling Security Patches*. The Deputy CIO for IT Operations shall use automated mechanisms that require no user intervention to manage and install updates. The Deputy CIO for IT Operations shall employ an automated mechanism to determine periodically and upon demand the state of information system components with regard to flaw remediation.
d. The CSIRC, in conjunction with the Deputy CIO for IT Operations, shall provide a process to track and document information system security incidents on an ongoing basis. For systems rated high, the tracking of security incidents and the collection and analysis of incident information shall employ automated mechanisms.
e. Program Offices/System Owners shall ensure that personnel with incident response responsibilities receive training at least once a year. Incident response training for systems rated high shall incorporate simulated events to facilitate effective response by personnel in a crisis and employ automated mechanisms.
f. Program Offices/System Owners shall test the incident response capability for systems under their purview rated moderate or high once a year and document the test results. For high-impact systems the tests shall employ automated mechanisms.
g. ISSOs shall report significant computer security incidents to the CSIRC immediately upon identification and validation of the incident occurrence.
h. ISSOs shall report all incidents to the CSIRC in a Weekly Incident Report.
i. The CSIRC shall report significant computer security incidents to appropriate authorities, including the United States Computer Emergency Readiness Team (USCERT), upon identification and validation of the incident occurrence. The CSIRC shall use automated mechanisms to assist in the reporting of security incidents for systems rated moderate or high. The CSIRC shall report incident-related information to OMB, as required by FISMA.
j. The CSIRC, in conjunction with the Deputy CIO for IT Operations, shall provide users of information systems with support and assistance (e.g., help desk) for the handling and reporting of security incidents. For systems rated moderate or high, the CSIRC and the Deputy CIO for IT Operations shall employ automated mechanisms to increase the availability of incident response-related information and support.

4.7.2 Documentation

Documentation of IT systems involves the collection of detailed information, such as functionality, system mission, unique personnel requirements, type of data processed, architectural design, system interfaces, system boundaries, hardware and software components, system and network diagrams, asset costs, and system communications and facilities. This information is part of the configuration baseline of the system.

HUD Policy
a. Program Offices/System Owners shall ensure that adequate documentation for the information system and its constituent components is available, current, protected when required, and distributed to authorized personnel. Documentation includes but is not limited to: • C&A and SDLC documentation • Vendor-supplied documentation of purchased software and hardware • Network diagrams • Application documentation for in-house applications • System build and configuration documentation, which includes optimization of system security settings, when applicable • User manuals • Standard operating procedures For systems that have been rated moderate or high, the documentation shall describe the functional properties of the security controls employed within the information system with sufficient detail to permit analysis and testing of the controls. For systems that have been rated high, the documentation shall describe the design and implementation details of the security controls employed within the information system with sufficient detail to permit analysis and testing of the controls, including functional interfaces among control components.

4.7.3 Information and Data Backup

Adhering to requirements regarding data backups can significantly reduce the risk that data will be compromised or lost in the event of a disaster or other interruption of service. A Backup Operations Plan should be included in the Contingency Plan.

The development of a data backup strategy begins early in the life cycle when the security categorization of the system is first considered. Several factors derived from the risk assessment and documented in the Contingency Plan will drive the data backup strategy. Frequency of backups will depend upon how often the data processed by the system(s) changes and how important those changes are. The risk assessment will drive this element of the backup strategy. Data backups need to be stored, both onsite and offsite, in a secure facility in fireproof and waterproof containers.

HUD Policy
a. Program Offices/System Owners shall ensure that a backup strategy and procedures are established, implemented, and tested in accordance with the Contingency Plan.
b. The Deputy CIO for IT Operations shall implement and enforce backup procedures for all sensitive IT systems, data, and information. The backups shall include user-level and system-level information.
c. The Deputy CIO for IT Operations shall store backups at a secure offsite location in accordance with the Contingency Plan.
d. The Deputy CIO for IT Operations shall test backup information quarterly for systems rated moderate and high.
e. The Deputy CIO for IT Operations shall test backup information as part of contingency planning for systems rated high.
f. For systems rated high, the Deputy CIO for IT Operations shall store backup copies of the operating system and other critical information systems software in a fire-rated container that is not collocated with the operational software or in a separate facility.

4.7.4 Input/Output Controls

Many security problems start with input validation issues. Information systems that fail to validate input can introduce "buffer overflow" vulnerabilities that could be exploited by an attacker. Checks for accuracy, completeness, and validity of information should be accomplished as close to the point of origin as possible. Rules for checking the valid syntax of information system inputs (e.g., character set, length, numerical range, and acceptable values) should be in place to ensure that inputs match specified definitions for format and content. Inputs passed to interpreters should be prescreened to ensure that the content is not unintentionally interpreted as commands.

On the output side, the structure and content of error messages should be carefully considered by the organization. User error messages generated by the information system should provide timely and useful information to users without revealing information that could be exploited by adversaries. System error messages should be revealed only to authorized personnel (e.g., systems administrators and maintenance personnel). Sensitive information (e.g., account numbers, social security numbers, and credit card numbers) should not be listed in error logs or associated administrative messages.

HUD Policy
a. For systems rated moderate or high, the Program Offices/System Owners shall ensure that the information system checks information inputs for accuracy, completeness, and validity.
b. For systems rated moderate or high, the Program Offices/System Owners shall ensure the information system identifies and handles error conditions in an expeditious manner.

5.0 TECHNICAL POLICIES

5.1 Identification and Authentication

Authentication is the process of establishing confidence in user identities electronically presented to an information system. Individual authentication is the process of establishing an understood level of confidence that an identifier refers to a specific individual. Authentication focuses on confirming an individual's identity, based on the reliability of the individual's credentials.

Authentication of user identities is accomplished using passwords, tokens, PKI certificates, key cards, biometrics, or in the case of multifactor authentication, some combination therein. FIPS 201 and its attendant SP 800-73 and SP 800-76 specify a personal identity verification (PIV) card token for use in the unique identification and authentication of federal employees and contractors. NIST SP 800-63 provides guidance on remote electronic authentication. When information systems are accessed through local interfaces and contained within a controlled environment with physical access controls, the risk of using passwords as opposed to other forms of authentication, are somewhat mitigated. Thus, passwords that meet NIST SP 800-63 level 2 password requirements used locally in an environment with adequate physical access controls can be used in FIPS 199/SP 800-53 moderate-impact systems.

HUD Policy
a. Program Offices/System Owners shall ensure that user access is controlled and limited based on positive user identification and authentication mechanisms that support access control, least privilege, and system integrity in accordance with FIPS 201, *Personal Identity Verification for Federal Employees and Contractors*. For high-impact systems, the system shall employ multifactor authentication mechanisms.
b. HUD users shall not share identification or authentication materials of any kind; nor shall any HUD user allow any other person to operate any HUD system by employing the user's identity.
c. All user authentication materials shall be treated as sensitive material and shall carry a level of sensitivity as high as the most sensitive data to which that user is granted access using that authenticator.
d. The system ISSO shall ensure that USERIDs are disabled after a period of inactivity of no more than 90 days. For systems rated moderate to high, the system shall do this automatically.
e. Program Offices/System Owners shall ensure that user access is reviewed once a year.

5.1.1 E-Authentication

To successfully implement a government service electronically (or e-government), federal agencies must determine the required level of assurance in the authentication for each transaction. This is accomplished through a risk assessment for each transaction.

The OMB has defined four levels of assurance in terms of the consequences for authentication errors and misuse of credentials. NIST has published technical guidance for federal agencies to support the ability of individuals to remotely authenticate to a federal system at different assurance levels.

HUD Policy
a. Program Offices/System Owners of IT systems that require authentication controls over the Internet between outside parties and HUD, the IT system shall utilize authentication mechanisms in accordance with NIST SP 800-63, *Electronic Authentication Guide*.
b. Program Offices/System Owners shall at a minimum comply with the following authentication requirements depending on system sensitivity in accordance with NIST SP 800-63: • Low-impact systems must comply with the requirements for level 1 authentication systems • Moderate-impact systems must comply with the requirements for level 2 authentication systems • High-impact systems must comply with the requirements for level 3 authentication systems

5.1.2 Device and Application Authentication

Multi-tier systems can use middle- and back-end systems to connect to legacy systems and databases. In certain situations, this connection takes place using a generic ID and password that may contain full system privileges. Compromise of these IDs/Passwords can result in system misuse.

Networks that do not use device authentication are open to intrusions by attackers who have access to their physical location. Shared media networks and dynamic protocols, like Dynamic Host Configuration Protocol (DHCP), are susceptible to attacks from anyone with physical access to a network connection (e.g., network wall outlet). The attacker can plug in the device and start using it to capture packets of data or to start scanning the network for vulnerable systems.

To ensure that only approved devices can connect to the network and that approved applications can connect to back-end systems, the authenticators need to be protected from unauthorized disclosure and use.

The information system typically uses either shared known information (e.g., Media Access Control [MAC] or Transmission Control Protocol/Internet Protocol [TCP/IP] addresses), an organizational authentication solution (e.g., IEEE 802.1x and Extensible Authentication Protocol [EAP]), or a Radius server with EAP-Transport Layer Security (TLS) authentication to identify and authenticate devices on local and/or wide area networks (WAN).

HUD Policy
a. Program Offices/System Owners must use an IT Security Office-approved procedure, mechanism, or protocol to secure authenticators used for application, host, or device authentication.

5.1.3 Passwords

A password is a secret that a claimant memorizes and uses to authenticate the claimant's identity. Passwords are typically character strings.

Strong passwords have a minimum of eight alphanumeric characters with at least one uppercase letter, one lowercase letter, one digit, and one special character. Strong passwords do not have common words or permutations of the user name.

HUD Policy
a. In those systems where user identity is authenticated by password, the system ISSO shall determine and enforce appropriate measures to ensure that strong passwords are used.
b. In those systems where user identity is authenticated by password, the system ISSO shall determine and enforce the appropriate frequency for changing passwords; but in no case shall the frequency be less often than every 90 days.
c. Users shall not share personal passwords.
d. Users shall select strong passwords and not reuse old passwords.
e. Use of group passwords shall be limited to situations dictated by operational necessity or those critical for mission accomplishment. Use of a group USERID and password must be approved by the appropriate Authorizing Official.
f. In those systems where user identity is authenticated by password, the system shall ensure that users cannot reuse a password for at least eight iterations.
g. In those systems where user identity is authenticated by password, the system shall ensure that passwords are not displayed when entered.
h. In those systems where user identity is authenticated by password, the system shall protect passwords from unauthorized disclosure and modification when stored and transmitted.
i. System administrators shall replace all default passwords provided by the vendor.
j. In those systems where user identity is authenticated by password, the system ISSO shall develop and implement administrative procedures for initial password distribution, for lost/compromised passwords, and for revoking passwords.

The use of a password by more than one individual is discouraged throughout HUD; however, it is recognized that in certain circumstances (e.g., operation of crisis management or operations centers, watch teams, and other duty personnel) may require the use of group USERIDs and passwords.

5.2 Access Control

Users are responsible for protecting all HUD information to which they are granted access. Access controls restrict access to system objects, such as files, directories, and devices based upon the identity of the user or the group to which the user belongs. The purpose of access controls is to protect against the unauthorized disclosure, modification, or destruction of the data residing in these systems, as well as the applications themselves. Automated systems are vulnerable to fraudulent or malicious activity by individuals who have the authority or capability to access information not required to perform their job-related duties. Access control policy is designed to reduce the risk of an individual acting alone from engaging in such fraudulent or malicious behavior. The Principle of Least Privilege states that a user should only be able to access the system resources needed to fulfill the user's job responsibilities.

HUD Policy
a. Program Offices/System Owners shall ensure that their information systems implement access control measures to provide protection from unauthorized alteration, loss, unavailability, or disclosure of information.

HUD Policy
b. Program Offices/System Owners shall ensure that their information systems rated moderate to high, use an automated mechanism to support management of information system accounts. For information systems rated high, the automated mechanism shall track account creation, disabling, and termination to support audit of such actions and, as required, notify appropriate individuals.
c. Program Offices/System Owners shall ensure that access control follows the principle of least privilege and separation of duties and shall require that a user use unique identifiers on a system.
d. ISSOs shall ensure that temporary and emergency accounts are properly authorized and maintained. For systems rated high, these accounts shall be automatically disabled after 48 hours.
e. ISSOs shall ensure that guest/anonymous accounts are not used.
f. Program Offices/System Owners shall identify specific user actions, which can be performed on the information system without identification and authentication. For systems rated moderate to high, actions to be performed without identification and authentication will be permitted only to the extent necessary to accomplish mission objectives.

5.2.1 Automatic Account Lockout

Program Offices/System Owners shall configure each IT system to lock any user account immediately and automatically following a specified number of consecutive failed logon attempts, in such a way that:

- As long as the account remains locked, no logon of any kind will be permitted to that account, including the user to whom the account is assigned.
- The manual intervention of an appropriate security administrator is required to unlock the account.

HUD Policy
a. Program Offices/System Owners shall ensure that their information systems implement and enforce an account lockout policy that limits the number of consecutive failed logon attempts to three within a thirty-minute period.
b. Program Offices/System Owners shall ensure their information systems are configured to lock out a user account after three consecutive failed logon attempts.

5.2.2 Logon and Session Security

Program Offices/System Owners shall configure each IT system to deactivate any user session immediately and automatically following a specified period of inactivity, in such a way that will require the user to re-authenticate the user's identity before resuming interaction with the system.

Systems that provide the user at logon with information concerning the last connection and possible unsuccessful attempts provide the agency with another layer of defense by enlisting users in identifying and reporting unusual activity.

Highly sensitive systems should limit the number of sessions that a user can have active to prevent possible unauthorized disclosure, modification, and/or destruction of sensitive information.

HUD Policy
a. Program Offices/System Owners of systems that have been rated moderate or high shall ensure their systems time out user sessions after ten minutes of inactivity.
b. For systems rated high, the Program Offices/System Owners shall ensure that the system does not allow concurrent sessions.

5.2.3 Warning Banner

Successful prosecution of unauthorized access to HUD systems requires that users be notified prior to their entry into the systems that the data in the system is owned by HUD and that activities on the system are subject to monitoring. All multi-user computer systems will display a warning message when a user attempts to access the system, and prior to actually logging into a system, informing users that equipment is the property of the government, that the use of government property is for the conduct of government business only, and that the use of government equipment is subject to monitoring.

Privacy Laws have explicit requirements to notify users about HUD's privacy policy prior to granting access to a system.

HUD Policy
a. The CISO shall provide a standard notification message for HUD systems that warns unauthorized users that they have accessed a U.S. Government system and can be punished. The wording shall also warn authorized users that they are subject to monitoring and recording and that use of the system indicates consent to such monitoring and recording.
b. IT systems internal to the HUD network shall display a warning banner stipulated by the HUD CISO and the Privacy Officer, when applicable. The warning banner shall require users to click through, indicating acknowledgment, prior to granting access to the system.
c. IT systems accessible to the public shall provide both a security and privacy statement approved by the CISO and the Privacy Officer at every entry point. The statement shall include a description of the authorized uses of the system.

5.3 Audit and Accountability

Audit trails maintain a record of system application and user activity. In conjunction with the appropriate tools and procedures, audit trails can assist in detecting security violations, performance problems, and application flaws.

Audit trails may be used as support for regular system operations or as a kind of insurance policy, or both. As an insurance policy, audit trails are maintained but are not used unless needed (e.g., after a system outage or suspected compromise). As a support for operations, audit trails are used to help system administrators ensure that the system or resources have not been harmed by hackers, insiders, or technical problems.

Audit trails help accomplish several security-related objectives, including individual accountability, event reconstruction, intrusion detection, and problem analysis.

Information systems that store or process personally identifiable information, personal health-related information, or financial information have specific audit requirements under the Privacy Act, Health Insurance Portability and Accountability Act, and the Sarbanes-Oxley Act.

HUD Policy
a. Program Offices/System Owners shall ensure that audit trails are sufficient in detail to facilitate the reconstruction of events if a system is compromised or if a malfunction occurs or is suspected. Audit trails shall include auditable events as specified in the system security plan and be reviewed accordingly. The audit trail shall contain at least the following information: • Type of event • Identity of the user, application, and device that triggered the event • The component of the information system (e.g., software component and hardware component) where the event occurred • Time and date of the event • Outcome (success or failure) of the event For systems rated moderate to high, the audit function shall have the capability of providing more detailed information for audit events identified by type, location, or subject. For systems rated high, the system shall provide the capability for centralized management of audit records.
b. Program Offices/System Owners shall ensure that their audit trails and audit logs are protected from unauthorized modification, access, or destruction while online and during offline storage.
c. Program Offices/System Owners shall ensure that audit logs are recorded and retained in accordance with HUD records retention policies, but in no case shall the frequency be less than once a year for systems rated moderate to high.
d. Program Offices/System Owners shall develop and implement a process to periodically review audit records for inappropriate or unusual activity, investigate suspicious activity or suspected violations, and report findings to the appropriate officials. For systems rated moderate or high, the Program Offices/System Owners shall employ an automated mechanism to facilitate the review of audit records. Audit records related to activities of users with significant information systems roles and responsibilities shall be reviewed more frequently.
e. Program Offices/System Owners shall ensure that the system allocates sufficient audit record storage capacity and configures auditing to prevent such capacity being exceeded.
f. Program Offices/System Owners shall ensure that the system alerts the appropriate officials in the event of an audit failure or when audit capacity is close to being reached.
g. Program Offices/System Owners shall make a risk-based decision on which one of the following actions the system should take in the event of an audit failure or when audit capacity is being reached: • Shutdown the system • Overwrite the oldest audit records • Stop generating audit records
h. Program Offices/System Owners of information systems that have been rated moderate or high shall that utilize audit reduction, review, and reporting techniques while ensuring that original audit records needed to support after-the-fact investigations are not altered. Program Offices/System Owners of high-impact systems shall ensure the system provides the capability to automatically process audit records for events of interest based upon selectable, even criteria.
i. Program Offices/System Owners shall use automated mechanisms to integrate their audit procedures into HUD's incident response capability for systems rated moderate to high, which provides for centralized audit monitoring, analysis, and reporting.
j. Program Offices/System Owners shall ensure that information systems under their purview provide time stamps for use in audit record generation. The time stamps shall be generated using internal information system clocks that are synchronized system wide.

5.4 Network Security

5.4.1 Remote Access and Dial-In

Remote access controls are applicable to information systems other than public web servers or systems specifically designed for public access. HUD restricts access achieved through dial-up connections (e.g., limiting dial-up access based upon source of request) or protects against unauthorized connections or subversion of authorized connections (e.g., using virtual private network [VPN] technology). HUD permits remote access for privileged functions (e.g., maintenance ports and system and device administration) only for compelling operational needs and during emergencies.

HUD Policy
a. The Deputy CIO for IT Operations shall provide remote access mechanisms that are centrally managed, monitored, and protected by strong authentication. The mechanisms shall have the capability to provide strong cryptographic mechanisms for authentication and protection of sensitive information during transmission. For access to systems rated moderate or high, the session shall be encrypted and access shall be managed through a managed access control point.
b. Program Offices/System Owners shall authorize and approve remote access methods for systems under their purview. The remote access methods shall only use mechanisms authorized by the Deputy CIO for IT Operations.
c. ISSOs shall authorize in writing users requiring remote access, including remote access for privileged functions.
d. Remote access administrators shall not add users to remote access mechanisms without written approval from the ISSO.

5.4.2 Network Security Monitoring

The increasingly important role of automated information system networks in government has fueled the need for more secure systems. Intrusion detection systems are gaining widespread recognition as important tools that improve computer network security. Although firewalls have traditionally been the first line of defense against would-be attackers, intrusion detection devices, working with firewalls, are becoming more popular for network security.

HUD Policy
a. The CSIRC shall use automated tools and mechanisms to monitor HUD's networks for security events.
b. The CISO, in coordination with IT Operations, shall select and implement intrusion detection and monitoring tools for HUD in accordance with NIST SP 800-31, *Intrusion Detection Systems*. The tools shall be part of a system-wide intrusion detection system that uses common protocols and supports near-real-time analysis of events in support of system-level attacks.
c. The CISO, in conjunction with the Deputy CIO for IT Operations, shall select and implement vulnerability scanning tools and techniques to scan information systems for vulnerabilities every month or when significant new vulnerabilities affecting HUD's infrastructure are identified and reported on systems rated low and moderate. Systems rated high shall be scanned once a week. For high-impact systems, the tools shall include the capability to update the list of vulnerabilities scanned. The list shall be updated every six months or when significant new vulnerabilities affecting the system are identified and reported.

HUD Policy
d. The CISO, in conjunction with the Deputy CIO for IT Operations, shall perform annual penetration testing on network components.

5.4.3 Network Connectivity

Within HUD, boundary protection of IT resources is accomplished by the installation and operation of controlled interfaces (e.g., proxies, gateways, routers, firewall, and encrypted tunnels). Controlled interfaces, when used in concert with a variety of additional security controls (e.g., intrusion detection systems, personnel background checks, security guards, data encryption, and physical security barriers), provide an added level of assurance that unauthorized personnel will be unable to access departmental automated systems.

By tracking and controlling data, deciding whether to pass, drop, reject, or encrypt the data, controlled interfaces have proven to be an effective means of securing a network.

HUD Policy
a. The Deputy CIO for IT Operations shall ensure that appropriate identification and authentication controls, audit logging, and access controls are implemented on every network component.
b. Program Offices/System Owners shall ensure that interconnections between sensitive IT systems under their purview and IT systems not controlled by HUD are established only through controlled interfaces. The controlled interfaces shall be accredited at the highest security level of information on the network.
c. The Deputy CIO for IT Operations shall ensure controlled interfaces are configured to prohibit any protocol or service that is not explicitly permitted. For high-impact systems, the Deputy CIO for IT Operations shall review and eliminate any unnecessary functions, ports, protocols, or services once a year.
d. The Deputy CIO for IT Operations shall ensure that a failure of the controlled interfaces does not result in any unauthorized release of information outside the information system boundary.
e. The Deputy CIO for IT Operations shall ensure that there is no public access to HUD's internal networks except as appropriately mediated through a proxy server.
f. The Deputy CIO for IT Operations shall ensure that alternate processing sites provide the same level of protection for network connections as the primary site.
g. The CISO shall establish connection criteria for allowing portable or mobile information systems access to HUD's networks.
h. The Deputy CIO for IT Operations shall ensure that portable or mobile information systems are not allowed access to HUD's networks without written approval and only after the devices meet the connection criteria established by the CISO.

5.4.4 Internet Security

The Internet is an excellent medium to publish and transmit information, thus providing substantial gains in productivity. Since the Internet is an open network available to everyone, including hackers and attackers, HUD must strike a balance that provides Internet connectivity to its constituents while maintaining an appropriate level of security.

HUD Policy
a. The Deputy CIO for IT Operations shall ensure that any direct connection of HUD networks to the Internet or to extranets occurs through controlled interfaces that have been certified and accredited.
b. The Deputy CIO for IT Operations shall ensure that publicly accessible information system components (e.g., public web servers) reside on separate sub-networks with separate physical network interfaces.
c. HUD employees or contractors shall not download or install mobile code (e.g., ActiveX or JavaScript) that has not been approved by the CISO.
d. The Deputy CIO for IT Operations shall ensure that controlled interfaces protecting the network perimeter filter certain types of packets to protect devices on an organization's internal network from being directly affected by denial of service attacks.
e. The Deputy CIO for IT Operations shall ensure that publicly accessible information systems protect the integrity of the information and applications available to the public.

5.4.5 Personal Email Accounts

Personal email accounts often reside on insecure networks where they are subject to compromise, interception, and computer viruses.

HUD Policy
a. HUD employees or contractors shall not transmit sensitive HUD information to any personal email account that is not authorized to receive it.
b. HUD employees or contractors shall not access personal email accounts from internal HUD networks or with HUD-provided equipment.

5.5 Cryptography

Encryption is the process of changing plaintext into ciphertext for the purpose of security or privacy. There are two basic types of cryptography:

1. Secret key systems—also called symmetric systems
2. Public key systems—also called asymmetric systems

In secret key systems, the same key is used for both encryption and decryption; that is, all parties participating in the communication share a single key. In public key systems, there are two keys: a public key and a private key. The public key used for encryption is different from the private key used for decryption. The two keys are mathematically related, but the private key cannot be determined from the public key.

Refer to NIST SP 800-21, *Guideline for Implementing Cryptography in the Federal Government,* for more in-depth information on cryptography.

A digital signature is an electronic analogue of a written signature. The digital signature can be used to prove to a recipient or third party that the originator did in fact sign the message (i.e., the message originators cannot repudiate the message). Signature generation makes use of a private key to generate a digital signature. Signature verification makes use of a public key that corresponds to, but is not the same as, the private key. The security of a digital signature system depends on maintaining the secrecy of users' private keys.

Encryption can be used to do, but is not limited to, the following:

- Encrypt data while in storage (e.g., hard drives, diskettes, and tapes)
- Encrypt data while in transmission
- Encrypt individual files for transmission over an unsecured medium
- Encrypt email messages
- Guarantee the integrity of a file or message, and detect any modifications
- Provide the legally binding equivalent of a hand signature in digital form
- Support non-repudiation
- Support authentication, including strong authentication
- Support electronic financial transactions, including electronic funds transfers, automated teller machine transactions, cash cards, gift cards, and credit cards
- Provide copyright protection (e.g., for DVDs)

5.5.1 Encryption

The FIPS 199 security category (for integrity and confidentiality) of the information being transmitted should guide the decision on the use of cryptographic mechanisms.

HUD Policy
a. Program Offices/Systems Owners shall identify IT systems transmitting or storing sensitive information that may require protection based on a risk assessment. If encryption is required, the following methods are acceptable for encrypting sensitive information: • Products using triple Data Encryption Standard (3DES) or Advanced Encryption Standard (AES) algorithms that have been validated under FIPS 140-1 or FIPS 140-2. (All new systems should use AES because it is expected that triple DES will be phased out.) • Secure Sockets Layer Version 3.0 (SSL3.0) or Transport Layer Security Version 1.0 (TLS1.0) • National Security Agency (NSA) Type 2 or Type 1 encryption
b. The CISO and Deputy CIO for IT Operations shall ensure cryptographic key establishment and management is done in accordance with NIST SP 800-56, *Recommendation on Key Establishment Schemes,* and NIST SP 800-57, *Recommendation on Key Management*.
c. Program Offices/Systems Owners of systems rated moderate or high shall use encryption to implement the following controls: • Remote access • Wireless access • Cryptographic module authentication • Transmission integrity and confidentiality
d. Program Offices/System Owners and users shall ensure information rated moderate or high residing on portable or mobile systems use FIPS 140-1 or 140-2-approved encryption to protect information.

5.5.2 Public Key Infrastructure

A public key infrastructure (PKI) is an architecture that provides the means to bind public keys to their owners and helps in the distribution of reliable public keys in large heterogeneous networks. Public keys are bound to their owners by public key certificates. These certificates,

which contain information such as the owner's name and the associated public key, are issued by a reliable certification authority (CA).

HUD Policy
a. The CISO, in conjunction with the Deputy CIO for IT Operations, shall select and implement a PKI for HUD in accordance with NIST SP 800-32, *Introduction to Public Key Technology and the Federal PKI Infrastructure*.
b. The CISO, in conjunction with the Deputy CIO for IT Operations, shall establish HUD's root CA and operate under an approved certificate policy and certificate practice statement. Any additional CAs within HUD must be subordinate to the HUD root.
c. Program Offices wishing to establish their own CA shall request approval from the CISO, be a subordinate to the HUD root, and operate under an approved certificate policy and certificate practices statement.
d. The CISO shall cross-certify the HUD root CA with the Federal Bridge. The certificate policies and practice statements of CAs subordinate to the HUD root must comply with the Federal Bridge Certificate Policy.
e. The CISO shall perform a yearly compliance audit of the root CA and all subordinate CAs.
f. The CISO, in conjunction with the Deputy CIO for IT Operations, shall ensure that HUD's PKI can support the requirements for E-authentication in accordance with NIST SP-800-63, *Electronic Authentication Guideline: Recommendation of the National Institute of Standards and Technology.*
g. The CISO, in conjunction with the Deputy CIO for IT Operations, shall ensure that HUD's PKI can support the requirements for personal identification verification in accordance with NIST FIPS 201, *Personal Identity Verification for Federal Employees and Contractors* and Draft SP 800-73, *Integrated Circuit Card for Personal Identity Verification.*

5.5.3 Public Key/Private Key

A public key/private key pair is generated using the PKI. The user retains the private key. The issuing CA signs the public key, creating a public key certificate. These certificates are used by the PKI to validate a public key. Public key/private keys can be used in a public key cryptographic system to encrypt data. They also can be used to create digital signatures.

HUD Policy
a. The CISO, in conjunction with the Deputy CIO for IT Operations, shall ensure separate public/private key pairs are used for encryption and digital signature.
b. Users shall not disclose or allow the use of their private keys. If a user shares his or her private key, the user is accountable for all transactions signed with the user's private key.
c. Users shall be responsible for the security of their private keys.

5.6 Malicious Code Protection

Malicious code includes all and any programs (including macros and scripts) that are deliberately coded to cause an unexpected, and unwanted, event on a user's workstation. Malicious code includes viruses, worms, logic bombs, Trojan horses, web bugs, and in some cases "spyware."

Malicious code can be introduced several ways (e.g., email, file downloads, and web surfing). It can destroy the integrity and confidentiality of data and systems.

HUD Policy
a. The Deputy CIO for IT Operations shall implement a defense-in-depth strategy that: • Installs and centrally manages antivirus software at each critical information entry point (e.g., firewalls, email servers, and remote-access servers) and at each workstation, server, and mobile computing device. The software shall be configured to check all files automatically on access, downloads, and email. • Installs updates to antivirus software and signature files at each critical information entry point (e.g., firewalls, email servers, and remote-access servers) and at each workstation, server, and mobile computing device promptly without requiring that end users specifically request the update. • Configures the software to prevent users from disabling it or modifying configuration settings. • Installs security patches to servers and desktops promptly. • Automatically forwards alerts generated by anti-virus software to HUD's intrusion detection system.
b. The Deputy CIO for IT Operations shall implement appropriate file/protocol/content filtering to protect data and networks against malicious code in accordance with HUD's Internet usage policy.
c. The Deputy CIO for IT Operations shall install and centrally manage spam and spyware protection mechanisms at each critical information entry point (e.g., firewalls, email servers, and remote-access servers) and at workstations, servers, and mobile computing devices connected to the network. The mechanism shall have the capability for automatic updates.

5.7 Miscellaneous

The following section addresses security requirements that did not belong to any other subcategory. Some of these requirements might apply to specific technologies. Examples of such technologies include video and audio conferencing and Voice over Internet Protocol (VoIP).

HUD Policy
a. Program Offices/System Owners of systems that have been rated moderate or high and use collaborative computing resources, like audio and video conferencing and electronic white boards, shall ensure that the collaborative computing resources cannot be activated remotely and provide explicit indication of use to the local user.
b. Program Offices/System Owners wishing to use VOIP in information systems under their purview must obtain approval from the CISO and Deputy CIO for IT Operations and follow the guidance in NIST SP 800-58, *Security Considerations for VoIP Systems*.

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.[2] 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.

The second mapping table does the same type of mapping as the first table but it follows the chronological order of the policy. In some instances, there is no mapping between HUD's policy and NIST SP 800-53. In these cases, the table will map to newer regulations or to best practices.

2 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 Section Number	Control Name	NIST 800-53 Control #	ISO/IEC 17799	NIST 800-26	GAO FISCAM
Access Control					
5.2a 5.4.3a	Access Control Policy and Procedures	AC-1	9.1.1 9.4.1	15 16	——
4.1.5a 5.1d 5.1e 5.2a 5.2b 5.2e	Account Management	AC-2 AC-2 (1) AC-2 (3) AC-2 (4)	9.2.1 9.2.2	6.1.8 15.1.1 15.1.4 15.1.8 15.2.2 16.1.3 16.1.5 16.2.12	AC-2.1 AC-2.2 AC-3.2 SP-4.1
4.6.5a 5.4.3a	Access and Information Flow Control	AC-3 AC-3 (1)	9.2.4 9.4.6 9.4.8	15.1.1 16.1.1 16.1.2 16.1.3 16.1.7 16.1.9 16.2.7 16.2.10 16.2.11 16.2.15	AC-2 AC-3.2
5.4.3b	Information Flow Enforcement	AC-4	9.4.6 9.4.8	——	——
5.2c 4.1.3a	Separation of Duties	AC-5	8.1.4	6.1.1 6.1.2 6.1.3 15.2.1 16.1.2 17.1.5	SD-1.2
3.1e 5.2c	Least Privilege	AC-6	9.2.2	16.1.2 16.1.3 17.1.5	AC-3.2
5.2.1a 5.2.1b	Unsuccessful Logon Attempts	AC-7	9.5.2	15.1.14	AC-3.2
5.2.3a 5.2.3b 5.2.3c	System Use Notification	AC-8	9.5.2	16.2.13 17.1.9	AC-3.2
Optional Control	Previous Logon Notification	AC-9	9.5.2	——	AC-3.2
5.2.2b	Concurrent Session Control	AC-10	——	——	——
4.6.1a 4.6.1b	Session Lock	AC-11	——	16.1.4	AC-3.2
5.2.2a	Session Termination	AC-12	9.5.7	16.1.4 16.2.6	AC-3.2
5.3d	Supervision and Review Access Control	AC-13 AC-13 (1)	9.2.4	7.1.10 11.2.2 16.1.10 17.1.6 17.1.7	AC-4 AC-4.3 SS-2.2

HUD Policy Section Number	Control Name	NIST 800-53 Control #	ISO/IEC 17799	NIST 800-26	GAO FISCAM
5.2f	Permitted Actions without Identification or Authentication	AC-14 AC-14 (1)	——	16.2.12	——
4.3b	Automated Marking	AC-15	5.2.2	8.2.4 16.1.6	AC-3.2
Optional Control	Automated Labeling	AC-16	5.2.2	16.1.6	AC-3.2
5.4.1a 5.4.1b 5.4.1c 5.4.1d 5.5.1c	Remote Access	AC-17 AC-17 (1) AC-17 (2) AC-17 (3)	9.4.3 9.4.4	16.2.12 16.2.4 16.2.8	AC-3.2
4.5.1a 4.5.1b 4.5.1c 4.5.1d 5.5.1c	Wireless Access Restrictions AC-18 (2)—Optional Control	AC-18 AC-18 (1)	——	——	——
5.5.1d 5.4.3g 5.4.3h	Access Control for Portable and Mobile Systems	AC-19 AC-19 (1)	9.5.1 9.8.1	7.3.1 7.3.2	——
4.6.4a 4.6.4b 4.6.4c	Personally-Owned Information Systems	AC-20	7.2.5 7.3.1 9.8.1	10.2.13	——
Awareness and Training					
4.1.4a	Security Awareness and Training Policy and Procedures	AT-1	——	13	——
4.1.4c	Security Awareness	AT-2	6.3.1 9.8.1 11.1.4 12.1.4	13.1.4 13.1.5	——
4.1.4b 4.1.4c	Security Training	AT-3	4.2.2 6.2.1 6.3.1 8.3.1 9.8.1	13.1 13.1.5	——
4.1.4e 4.1.4h	Security Training Records	AT-4	——	13.1.2	——
Audit and Accountability					
5.3a	Audit and Accountability Policy and Procedures	AU-1	——	17	——
5.3a 5.3c 5.3i	Auditable Events AU-2 (2)—Optional Control	AU-2 AU-2 (1) AU-2 (2)	11.1.2	17.1.1 17.1.2 17.1.4	——
5.3a 5.3i	Content of Audit Records	AU-3 AU-3 (1) AU-3 (2)	9.7.2	17.1.1	——
5.3e	Audit Storage Capacity	AU-4	9.7.2	——	——
5.3f 5.3g	Audit Processing	AU-5 AU-5 (1)	9.7.2	——	——
5.3d 5.3i	Audit Monitoring, Analysis, and Reporting AU-6 (2)—Optional Control	AU-6 AU-6 (1)	9.7.2	17.1.1	——

HUD Policy Section Number	Control Name	NIST 800-53 Control #	ISO/IEC 17799	NIST 800-26	GAO FISCAM
5.3h	Audit Reduction and Report Generation	AU-7 AU-7 (1)	——	17.1.2 17.1.7	——
5.3j	Time Stamps	AU-8	9.7.3	——	——
5.3b	Protection of Audit Information AU-9 (1)—Optional Control	AU-9	12.3.2	17.1.3 17.1.4	——
Optional Control	Non-repudiation	AU-10	10.3.4	15.1.2 17.1.1	——
5.3c	Audit Retention	AU-11	10.7.1 12.1.3	17.1.4	——
Certification, Accreditation, and Security Assessments					
3.10a 3.10b 3.10c 3.10d	C&A and Security Assessment Policy and Procedures	CA-1	——	2 4	——
3.10f	Security Assessment	CA-2	4.1.7	2.1.1 2.1.2 2.1.3 2.1.4	SP-5.1
3.10h	Information System Connections	CA-3	——	1.1.1 3.2.9 4.1.2 4.1.8 12.2.3	CC-2.1
3.10a 3.10b	Security Certification	CA-4	——	3.2.3 3.2.5 4.1.1 4.1.6 11.2.8 12.2.5	CC-2.1
3.10e	Plan of Action and Milestones	CA-5	——	1.2.3 2.2.1 4.2.1	SP-5.1 SP-5.2
3.10a 3.10b 3.10c	Security Accreditation	CA-6	——	4.1.1 4.1.7 4.1.8 12.2.5	——
3.10g	Continuous Monitoring	CA-7	9.7.2 12.2.1	10.2.1	——
Configuration Management					
3.8a 4.6.4b 4.6.5a 4.6.5e 4.6.5i	Configuration Management Policy and Procedures	CM-1	——	——	——
3.8a	Baseline Configuration	CM-2 CM-2 (1) CM-2 (2)	——	1.1.1 10.1.4 10.2.7 10.2.8 10.2.9	CC-2.3 CC-3.1 SS-1.2

HUD Policy Section Number	Control Name	NIST 800-53 Control #	ISO/IEC 17799	NIST 800-26	GAO FISCAM
3.8b	Configuration Change Control	CM-3 CM-3 (1)	8.1.2 10.4.1 10.5.1	10.2.2 10.2.3 10.2.10 10.2.11	SS-3.2 CC-2.2
3.8d	Monitoring Configuration Changes	CM-4	8.1.2	10.2.1 10.2.4	SS-3.1 SS-3.2 CC-2.1
3.8e	Access Restrictions for Change	CM-5 CM-5 (1)	——	6.1.3 6.1.4 10.1.1 10.1.4 10.1.5	SD-1.1 SS-1.2 SS-2.1
3.8f 3.10g	Configuration Settings	CM-6 CM-6 (1)	——	10.2.6	——
5.4.3c	Least Functionality	CM-7 CM-7 (1)	9.4.2	10.3.1	——
Contingency Planning					
3.6a	Contingency Planning Policy and Procedures	CP-1	3.1.1	9.	——
3.6b	Contingency Plan	CP-2 CP-2 (1)	11.1.3	4.1.4 9.1.1 9.2 9.2.1 9.2.2 9.2.3 9.2.10 12.1.8	SC-3.1 SC-1.1
3.6d 3.6e	Contingency Training	CP-3 CP-3 (1)	11.1.3 11.1.4	9.3.2	SC-2.3
3.6e	Contingency Plan Testing	CP-4 (1) CP-4 (2)	11.1.5	4.1.4 9.3.3	SC-3.1
3.6c	Contingency Plan Update	CP-5	11.1.5	9.3.1 9.3.3 10.2.12	SC-2.1 SC-3.1
3.6f	Alternate Storage Sites	CP-6 CP-6 (1) CP-6 (2) CP-6 (3)	8.4.1	9.2.4 9.2.5 9.2.7 9.2.9	SC-2.1 SC-3.1
3.6g	Alternate Processing Sites	CP-7 CP-7 (1) CP-7 (2) CP-7 (3) CP-7 (4)	11.1.4	9.1.3 9.2.4 9.2.5 9.2.7 9.2.9	SC-2.1 SC-3.1
3.6h 3.5c	Telecommunications Services	CP-8 CP-8 (1) CP-8 (2) CP-8 (3) CP-8 (4)	11.1.4	——	——

HUD Policy Section Number	Control Name	NIST 800-53 Control #	ISO/IEC 17799	NIST 800-26	GAO FISCAM
4.7.3a 4.7.3b 4.7.3c 4.7.3d 4.7.3e 4.7.3f	Information System Backup	CP-9 (1) CP-9 (2) CP-9 (3)	8.4.1	9.2.6 9.2.9 12.1.9	SC-2.1
3.6i	Information System Recovery and Reconstitution	CP-10 CP-10 (1)	11.4.1	9.2.8	SC-2.1
Identification and Authentication					
5.1a	Identification and Authentication Policy and Procedures	IA-1	——	11.2.3	——
5.1.1a	User Identification and Authentication	IA-2 IA-2 (1)	9.5.3	15.1	——
5.1.2a	Device Authentication and Application Authentication	IA-3	9.4.4 9.5.1 9.8.1	16.2.7	——
5.1a 5.1b	Identifier Management	IA-4	9.5.3	15.1.1 15.2.2 16.1.5 15.1.8	AC-2.1 AC-3.2 SP-4.1
5.1b 5.1.3a 5.1.3b 5.1.3c 5.1.3d 5.1.3e 5.1.3f 5.1.3g 5.1.3h 5.1.3i 5.1.3j 5.1.1b	Authenticator Management	IA-5	——	15.1.7 15.1.10 15.1.11 15.1.12 15.1.13	AC-3.2
5.1.3g	Authenticator Feedback	IA-6	——	——	——
5.1.1a 5.5.1c 5.5.2f 5.5.2g	Cryptographic Module Authentication	IA-7	——	16.1.7	——
Incident Response					
4.7.1a	Incident Response Policy and Procedures	IR-1	3.1.1	14	——
4.7.1e	Incident Response Training	IR-2 IR-2 (1) IR-2 (2)	6.3.1	14.1.4	SP-3.4
4.7.1f	Incident Response Testing	IR-3 IR-3 (1)	——	——	——
4.7.1a	Incident Handling	IR-4 IR-4 (1)	8.1.3	14.1.1 14.1.2 14.1.6	SP-3.4
4.7.1d	Incident Monitoring	IR-5 IR-5 (1)	8.1.3	14.1.3	——

HUD Policy Section Number	Control Name	NIST 800-53 Control #	ISO/IEC 17799	NIST 800-26	GAO FISCAM
4.7.1i 4.7.1g 4.7.1h	Incident Reporting	IR-6 IR-6 (1)	8.1.3	14.1.1 14.1.2 14.1.3 14.2.1 14.2.3	——
4.7.1a 4.7.1j	Incident Response Assistance	IR-7 IR-7 (1)	——	8.1.1 14.1.1	SP-3.4
Maintenance					
4.6.5b	System Maintenance Policy and Procedures	MA-1	8.1.1	10	——
4.6.5b 4.6.5c	Periodic Maintenance	MA-2 MA-2 (1) MA-2 (2)	7.2.4	10.1.1 10.1.3 10.2.1	SS-3.1
4.6.5d	Maintenance Tools	MA-3	——	10.1.3 11.2.4	——
4.6.5f 4.6.5j 4.6.5k	Remote Maintenance	MA-4 MA-4 (1) MA-4 (2)	9.4.5	10.1.1	SS-3.1
4.6.5g	Maintenance Personnel	MA-5	7.2.4	10.1.1 10.1.3	SS-3.1
4.6.5h	Timely Maintenance	MA-6	——	9.1.2	SC-1.2
Media Protection					
4.3a	Media Protection Policy and Procedures	MP-1	8.6.1	8	——
4.3a 4.3l	Media Access	MP-2 MP-2 (1)	8.6.1	8.2.1 8.2.2 8.2.3 8.2.6 8.2.7	——
4.3b	Media Labeling	MP-3	——	8.2.5 8.2.6 10.2.9	——
4.3c	Media Storage	MP-4	8.6.3 12.3.1	7.1.4 8.2.1 8.2.2 8.2.9	AC-3.1
4.3k	Media Transport	MP-5	8.7.2	8.2.2 8.2.4	——
4.3d 4.3e 4.3f 4.3h 4.3i	Media Sanitization	MP-6	8.6.1	3.2.11 3.2.12 3.2.13 8.2.8 8.2.9	AC-3.4
4.3i 4.3j	Media Destruction and Disposal	MP-7	7.2.6 8.6.2	3.2.11 3.2.12 3.2.13 8.2.10	AC-3.4
Physical and Environmental Protection					
4.2.1a	Physical and Environmental Protection Policy and Procedures	PE-1	——	7	——

HUD Policy Section Number	Control Name	NIST 800-53 Control #	ISO/IEC 17799	NIST 800-26	GAO FISCAM
4.2.2b 4.2.2c	Physical Access Authorizations	PE-2	——	7.1.1 7.1.2	AC-3.1
4.2.2a 4.2.2d 4.2.2e	Physical Access Control	PE-3	7.1.2 7.1.5	7.1.1 7.1.2 7.1.5 7.1.6	AC-3.1
Optional Control	Access Control for Transmission Medium	PE-4	——	7.2.2	——
4.2.2f	Access Control for Display Medium	PE-5	——	7.2.1	——
4.2.2g	Monitoring Physical Access	PE-6 PE-6 (1) PE-6 (2)	7.2.3	7.1.9	AC-4
4.2.1b 4.2.1c	Visitor Control	PE-7 PE-7 (1)	7.1.2	7.1.7	AC-3.1
4.2.1b	Access Logs	PE-8 PE-8 (1)	7.1.2	7.1.9	AC-4
4.2.2h	Power Equipment and Cabling PE-9 (1)—Optional Control	PE-9	7.2.3	7.1.16	SC-2.2
4.2.2i	Emergency Shutoff	PE-10	7.2.2	——	——
4.2.2k 4.2.2l	Emergency Power PE-11 (2)—Optional Control	PE-11 (1)	7.2.2	7.1.18	SC-2.2
4.2.2m	Emergency Lighting	PE-12	7.2.2	——	——
4.2.2n 4.2.2o 4.2.2p	Fire Protection	PE-13 PE-13 (1) PE-13 (2)	7.2.1	7.1.12	SC-2.2
4.2.2q	Temperature and Humidity Controls	PE-14	——	7.1.14 7.1.15	SC-2.2
4.2.2r	Water Damage Protection	PE-15	7.2.1	7.1.17	SC-2.2
4.2.2s	Delivery and Removal	PE-16	7.1.5	7.1.3 7.1.11	AC-3.1
4.2.1d	Alternate Work Site	PE-17	9.8.2	——	——
Planning					
3.1b	Security Planning Policy and Procedures	PL-1	——	5	——
3.1b	System Security Plan	PL-2	——	5.1.1 5.1.2	SP-2.1
3.1b	System Security Plan Update	PL-3	——	5.2.1	SP-2.1
4.1.1a 4.1.1b 4.1.1c	Rules of Behavior	PL-4	——	4.1.3	——
3.1d	Privacy Impact Assessment	PL-5	12.1.4	——	——
Personnel Security					
3.1.1a	Personnel Security Policy and Procedures	PS-1	——	6	——
4.1a	Position Categorization	PS-2	——	6.1.1 6.1.2	SD-1.2
4.1b 4.1c 4.1d	Personnel Screening	PS-3	6.1.2	6.2.1 6.2.2 6.2.3 6.2.4	SP-4.1
4.1.5a	Personnel Termination	PS-4	——	6.1.7	SP-4.1

HUD Policy Section Number	Control Name	NIST 800-53 Control #	ISO/IEC 17799	NIST 800-26	GAO FISCAM
4.1.5a	Personnel Transfer	PS-5	——	6.1.7	SP-4.1
4.1.1a 4.1.1b 4.1.1c 4.1.2a 4.1.2b	Access Agreements	PS-6	6.1.3	6.1.5 6.2.2	SP-4.1
3.3a 3.3d	Third-Party Personnel Security	PS-7	4.2.2	6.2.2	SP-4.1
3.11a 3.11b 3.11c	Personnel Sanctions	PS-8	6.3.5 9.2.1	6.1.5	——
Risk Assessment					
3.9a	Risk Assessment Policy and Procedures	RA-1	——	1	——
3.1.1a	Security Categorization	RA-2	5.2.1	1.1.3 3.1.1	SP-1 AC-1.1 AC-1.2
3.9a	Risk Assessment	RA-3	INTRO	1.1.2 1.1.4 1.1.5 1.1.6 1.2.1 1.2.3 4.1.7 7.1.13 7.1.19	SP-1
3.9b	Risk Assessment Update	RA-4	INTRO	1.1.2	SP-1
5.4.2c	Vulnerability Scanning RA-5 (3)—Optional Control	RA-5 RA-5 (1) RA-5 (2)	——	10.3.2 14.2.1	——
System and Services Acquisition					
3.2a 3.2b	System and Services Acquisition Policy and Procedures	SA-1	——	3	——
3.2a 3.2b	Allocation of Resources	SA-2	8.2.1	3.1.2 3.1.3 3.1.5	——
3.2c 3.7a	Life Cycle Support	SA-3	——	3.1	——
3.2d 3.3a 3.3b	Acquisitions	SA-4	10.1.1	3.1.6 3.1.7 3.1.9 3.1.11 3.1.12	——
4.7.2a	Information System Documentation	SA-5 SA-5 (1) SA-5 (2)	8.6.4	3.2.2 3.2.3 3.2.4 3.2.8 12.1.6	CC-2.1
4.6.2a 4.6.2b	Software Usage Restrictions	SA-6	12.1.2	10.2.10 10.2.13	SS-3.2 SP-2.1
4.6.3a	User Installed Software	SA-7	10.4.1	10.2.10	SS-3.2

HUD Policy Section Number	Control Name	NIST 800-53 Control #	ISO/IEC 17799	NIST 800-26	GAO FISCAM
3.7b	Security Design Principles	SA-8	——	3.2.1	——
3.3b 3.3c 3.3d	Outsourced Information System Services	SA-9	4.2.1	12.2.3	——
3.8h	Developer Configuration Management	SA-10	10.5.1 10.5.2		CM-3
3.8i	Developer Security Testing	SA-11	10.5.1 10.5.2	3.2.1 3.2.2 10.2.5 12.1.5	CM-3
System and Communications Protection					
4.4	System and Communications Policy and Procedures	SC-1	——	——	——
3.7c	Application Partitioning	SC-2	——	——	——
DOD Control	Security Function Isolation	SC-3	——	——	——
DOD Control	Information Remnants *Media sanitization is covered in Section 4.3	SC-4	——	3.2.12	AC-3.4
5.4.4d	Denial of Service Protection SC-5 (1) (2)—Optional Controls	SC-5	8.1.3	——	——
DOD Control	Resource Priority	SC-6	——	9.1.3 11.2.7	SC-1.3
5.4.3b 5.4.3d 5.4.3e 5.4.3f 5.4.4a 5.4.4b	Boundary Protection	SC-7 SC-7 (1)	9.4.6	16.2.2 16.2.7 16.2.8 16.2.9 16.2.10 16.2.11 16.2.14	AC-3.2
4.4.1a 5.5.1c	Transmission Integrity	SC-8 SC-8 (1)	8.7.3	11.2.1 11.2.4 11.2.9 16.2.14	AC-3.2
4.4.1b 5.5.1c	Transmission Confidentiality	SC-9 SC-9 (1)	——	——	——
5.2.2a	Network Disconnect	SC-10	——	16.2.6	AC-3.2
5.1.3h Optional Control	Trusted Path	SC-11	——	——	——
5.5.1b	Cryptographic Key Establishment and Management	SC-12	10.3.5	16.1.7 16.1.8	——
5.5.1a	Use of Validated Cryptography	SC-13	——	16.1.7 16.1.8	——
5.4.4e	Public Access Protections	SC-14	8.7.6	16.3.1	——
5.7a	Collaborative Computing	SC-15	——	——	——
Optional Control	Transmission of Security Parameters	SC-16	5.2.2 8.7.1	16.1.6	AC-3.2
5.2.2b	Public Key Infrastructure Certificates	SC-17	10.3.5	——	——
5.4.4a	Mobile Code	SC-18	——	——	——
5.7b	Voice Over Internet Protocol	SC-19	——	——	——

HUD Policy Section Number	Control Name	NIST 800-53 Control #	ISO/IEC 17799	NIST 800-26	GAO FISCAM
System and Information Integrity					
4.7.1c 5.6a 5.6b	System and Information Integrity Policy and Procedures	SI-1	——	11.	——
4.7.1c	Flaw Remediation SI-2 (1) (2)—Optional Controls but have been included in policy as a best practice	SI-2 SI-2 (1) SI-2 (2)	10.4.1	10.3.2 11.1.1 11.1.2 11.2.2 11.2.7	SS-2.2
5.6a	Malicious Code Protection	SI-3 SI-3 (1) SI-3 (2)	8.3.1	11.1.1 11.1.2	——
4.7.1b 5.4.2a 5.4.2b 5.6a	Intrusion Detection Tools and Techniques SI-4 (1) (2)—Optional Controls but have been included in policy as a best practice. SI-4 (3) (4)—Optional Controls	SI-4 SI-4 (1) SI-4 (2)	9.7.2	11.2.5 11.2.6	——
4.7.1b 5.6a	Security Alerts and Advisories	SI-5	——	14.1.1 14.1.2 14.1.5	SP-3.4
3.10g 4.7.1c	Security Functionality Verification SI-6 (2)—Optional Control	SI-6 SI-6 (1)	——	11.2.1 11.2.2	SS-2.2
3.8g	Software and Information Integrity	SI-7	10.2.1 10.2.2 10.2.4	11.2.1 11.2.4	——
5.6c	Spam and Spyware Protection SI-8 (1) (2)—Optional Controls but have been included in policy as a best practice.	SI-8 SI-8 (1) SI-8 (2)	——	——	——
4.1.2a 4.1.2b	Information Input Restrictions	SI-9	10.2.1	——	SD-1
4.7.4a	Information Input Accuracy, Completeness, and Validity	SI-10 SI-10 (1)	——	——	——
4.7.4b	Error Handling	SI-11	——	——	——
4.3a 4.3g	Information Output Handling and Retention	SI-12	——	——	——

HUD Information Technology Security Policy to NIST 800-53 Mapping

HUD Policy Section Number	Control Name	NIST 800-53 Control #	ISO/IEC 17799	NIST 800-26	GAO FISCAM	Other
Management Policies						
3.1a	Basic Requirements	——	——	——	——	FISMA -2004 A.3.d, e, f
3.1b	Basic Requirements	PL-1	——	5	——	——
		PL-2	——	5.1.1 5.1.2	SP-2.1	——
		PL-3	——	5.2.1	SP-2.1	——
3.1c	Basic Requirements	——	——	——	——	Best Practice NIST SP 800-18
3.1d	Basic Requirements	PL-5	12.1.4	——	——	——
3.1e	Basic Requirements	AC-6	9.2.2	16.1.2 16.1.3 17.1.5	AC-3.2	HIPPA
3.1.1a	Information and Information System Categorization	RA-2	5.2.1	1.1.3 3.1.1	SP-1 AC-1.1 AC-1.2	——
3.1.1b	Information and Information System Categorization	——	——	——	——	Best Practice FIPS 199
3.2a	Capital Planning and Investment Control	SA-1	——	3	——	——
		SA-2	8.2.1	3.1.2 3.1.3 3.1.5	——	——
3.2b	Capital Planning and Investment Control	SA-1	——	3	——	——
		SA-2	8.2.1	3.1.2 3.1.3 3.1.5	——	——
3.2c	Capital Planning and Investment Control	——	——	——	——	FISMA-2004 A.2.b, A.3.g
3.2d	Capital Planning and Investment Control	——	——	——	——	FISMA 2004 A.3.g
3.3a	Contractors and Outsourced Operations	PS-7	4.2.2	6.2.2	SP-4.1	——
		SA-4	10.1.1	3.1.6 3.1.7 3.1.9 3.1.11 3.1.12	——	——
3.3b	Contractors and Outsourced Operations	SA-4	10.1.1	3.1.6 3.1.7 3.1.9 3.1.11 3.1.12	——	——
		SA-9	4.2.1	12.2.3	——	——
3.3c	Contractors and Outsourced Operations	SA-9	4.2.1	12.2.3	——	——
3.3d	Contractors and Outsourced Operations	PS-7	4.2.2	6.2.2	SP-4.1	FISMA-2004 A.2.c, A.3.a, b
		SA-9	4.2.1	12.2.3	——	——

HUD Policy Section Number	Control Name	NIST 800-53 Control #	ISO/IEC 17799	NIST 800-26	GAO FISCAM	Other
3.4a	Performance Measures and Metrics	——	——	——	——	Best Practice
3.4b	Performance Measures and Metrics	——	——	——	——	Best Practice
3.4c	Performance Measures and Metrics	——	——	——	——	NIST SP 800-35
3.5a	Critical Infrastructure Protection	——	——	——	——	PDD-63
3.5b	Critical Infrastructure Protection	——	——	——	——	PDD-63
3.5c	Critical Infrastructure Protection	CP-8	——	——	——	PDD-63
3.6a	Information Technology Contingency Planning	CP-1	3.1.1	9	——	——
3.6b	Information Technology Contingency Planning	CP-2 CP-2 (1)	11.1.3	4.1.4 9.1.1 9.2 9.2.1 9.2.2 9.2.3 9.2.10 12.1.8	SC-3.1 SC-1.1	FISMA-2004 A.2.d
3.6c	Information Technology Contingency Planning	CP-5	11.1.5	9.3.1 9.3.3 10.2.12	SC-2.1 SC-3.1	——
3.6d	Information Technology Contingency Planning	CP-3 CP-3 (1)	11.1.3 11.1.4	9.3.2	SC-2.3	——
3.6e	Information Technology Contingency Planning	CP-3 CP-3 (1)	11.1.3 11.1.4	9.3.2	SC-2.3	FISMA-2004 A.2.e
		CP-4 (1) CP-4 (2)	11.1.5	4.1.4 9.3.3	SC-3.1	——
3.6f	Information Technology Contingency Planning	CP-6 CP-6 (1) CP-6 (2) CP-6 (3)	8.4.1	9.2.4 9.2.5 9.2.7 9.2.9	SC-2.1 SC-3.1	——
3.6g	Information Technology Contingency Planning	CP-7 CP-7 (1) CP-7 (2) CP-7 (3) CP-7 (4)	11.1.4	9.1.3 9.2.4 9.2.5 9.2.7 9.2.9	SC-2.1 SC-3.1	——
3.6h	Information Technology Contingency Planning	CP-8 CP-8 (1) CP-8 (2) CP-8 (3) CP-8 (4)	11.1.4	——	——	——
3.6i	Information Technology Contingency Planning	CP-10 CP-10 (1)	11.4.1	9.2.8	SC-2.1	——
3.7a	System Development Life Cycle	SA-3	——	3.1	——	FISMA
3.7b	System Development Life Cycle	SA-8	——	3.2.1	——	——

HUD Policy Section Number	Control Name	NIST 800-53 Control #	ISO/IEC 17799	NIST 800-26	GAO FISCAM	Other
3.7c	System Development Life Cycle	SC-2	——	——	——	——
3.8a	Configuration Management	CM-1	——	——	——	——
		CM-2 CM-2 (1) CM-2 (2)	——	1.1.1 10.1.4 10.2.7 10.2.8 10.2.9	CC-2.3 CC-3.1 SS-1.2	——
3.8b	Configuration Management	CM-3 CM-3 (1)	8.1.2 10.4.1 10.5.1	10.2.2 10.2.3 10.2.10 10.2.11	SS-3.2 CC-2.2	——
3.8c	Configuration Management	——	——	——	——	Best Practice
3.8d	Configuration Management	CM-4	8.1.2	10.2.1 10.2.4	SS-3.1 SS-3.2 CC-2.1	——
3.8e	Configuration Management	CM-5 CM-5 (1)	——	6.1.3 6.1.4 10.1.1 10.1.4 10.1.5	SD-1.1 SS-1.2 SS-2.1	——
3.8f	Configuration Management	CM-6 CM-6 (1)	——	10.2.6	——	FISMA-2004 D.1, D.2
3.8g	Configuration Management	SI-7	10.2.1 10.2.2 10.2.4	11.2.1 11.2.4	——	——
3.8h	Configuration Management	SA-10	10.5.1 10.5.2	——	CM-3	——
3.8i	Configuration Management	SA-11	10.5.1 10.5.2	3.2.1 3.2.2 10.2.5 12.1.5	CM-3	——
3.9a	Risk Management and Risk Assessment	RA-1	——	1	——	——
		RA-3	INTRO	1.1.2 1.1.4 1.1.5 1.1.6 1.2.1 1.2.3 4.1.7 7.1.13 7.1.19	SP-1	——
3.9b	Risk Management and Risk Assessment	RA-4	INTRO	1.1.2	SP-1	——

HUD Policy Section Number	Control Name	NIST 800-53 Control #	ISO/IEC 17799	NIST 800-26	GAO FISCAM	Other
3.9c	Risk Management and Risk Assessment	——	——	——	——	OMB guidance OMB-04-04, *E-Authentication Guidance for Federal Agencies* FISMA-2004 A.3.h
3.10a	Certification and Accreditation	CA-1	——	2 4	——	——
		CA-4	——	3.2.3 3.2.5 4.1.1 4.1.6 11.2.8 12.2.5	CC-2.1	——
		CA-6	——	4.1.1 4.1.7 4.1.8 12.2.5	——	——
3.10b	Certification and Accreditation	CA-1	——	2 4	——	——
		CA-4	——	3.2.3 3.2.5 4.1.1 4.1.6 11.2.8 12.2.5	CC-2.1	——
		CA-6	——	4.1.1 4.1.7 4.1.8 12.2.5	——	——
3.10c	Certification and Accreditation	CA-1	——	2 4	——	FISMA-2004 A.2.a
		CA-6	——	4.1.1 4.1.7 4.1.8 12.2.5	——	——
3.10d	Certification and Accreditation	CA-1	——	2 4	——	——
3.10e	Certification and Accreditation	CA-5	——	1.2.3 2.2.1 4.2.1	SP-5.1 SP-5.2	——
3.10f	Certification and Accreditation SI-6 (1) (2)—TBD	CA-2	4.1.7	2.1.1 2.1.2 2.1.3 2.1.4	SP-5.1	FISMA-2004 A.2.c

HUD Policy Section Number	Control Name	NIST 800-53 Control #	ISO/IEC 17799	NIST 800-26	GAO FISCAM	Other
3.10g	Certification and Accreditation	CA-7	9.7.2 12.2.1	10.2.1	——	——
		CM-6 (1)	——	10.2.6	——	——
		SI-6	——	11.2.1 11.2.2	SS-2.2	——
3.10h	Certification and Accreditation	CA-3	——	1.1.1 3.2.9 4.1.2 4.1.8 12.2.3	CC-2.1	——
3.10i	Certification and Accreditation	——	——	——	——	HUD Policy
3.10j	Certification and Accreditation	——	——	——	——	HUD Policy
3.11a	Incidents, Violations, and Disciplinary Action	PS-8	6.3.5 9.2.1	6.1.5	——	——
3.11b	Incidents, Violations, and Disciplinary Action	PS-8	6.3.5 9.2.1	6.1.5	——	——
3.11c	Incidents, Violations, and Disciplinary Action	PS-8	6.3.5 9.2.1	6.1.5	——	——
Operational Policies						
4.1a	Personnel	PS-2	——	6.1.1 6.1.2	SD-1.2	——
4.1b	Personnel	PS-3	6.1.2	6.2.1 6.2.2 6.2.3 6.2.4	SP-4.1	——
4.1c	Personnel	PS-3	6.1.2	6.2.1 6.2.2 6.2.3 6.2.4	SP-4.1	——
4.1d	Personnel	PS-3	6.1.2	6.2.1 6.2.2 6.2.3 6.2.4	SP-4.1	——
4.1e	Personnel	——	——	——	——	HUD Policy
4.1f	Personnel	——	——	——	——	HUD Policy
4.1.1a	Rules of Behavior	PL-4	——	4.1.3	——	——
		PS-6	6.1.3	6.1.5 6.2.2	SP-4.1	——
4.1.1b	Rules of Behavior	PL-4	——	4.1.3	——	——
		PS-6	6.1.3	6.1.5 6.2.2	SP-4.1	——
4.1.1c	Rules of Behavior	PL-4	——	4.1.3	——	——
		PS-6	6.1.3	6.1.5 6.2.2	SP-4.1	——
4.1.2a	Access to Sensitive Information	PS-6	6.1.3	6.2.2	SP-4.1	——
		SI-9	12.2.1 12.2.2	——	SD-1	——

HUD Policy Section Number	Control Name	NIST 800-53 Control #	ISO/IEC 17799	NIST 800-26	GAO FISCAM	Other
4.1.2b	Access to Sensitive Information	PS-6	6.1.3	6.1.5 6.2.2	SP-4.1	——
		SI-9	12.2.1 12.2.2		SD-1	——
4.1.3a	Separation of Duties Policy	AC-5	8.1.4	6.1.1 6.1.2 6.1.3 15.2.1 16.1.2 17.1.5	SD-1.2	OMB A-130 Appendix III
4.1.4a	Training and Awareness	AT-1	——	13	——	——
4.1.4b	Training and Awareness	AT-3	4.2.2 6.2.1 6.3.1 8.3.1 9.8.1	13.1 13.1.5	——	——
4.1.4c	Training and Awareness	AT-3	4.2.2 6.2.1 6.3.1 8.3.1 9.8.1	13.1 13.1.5	——	FISMA-2004 G.1.b
		AT-2	6.3.1 9.8.1 11.1.4 12.1.4	13.1.4 13.1.5	——	——
4.1.4d	Training and Awareness	AT-3		13.1.5		FISMA-2004 G.1.b
4.1.4e	Training and Awareness	AT-4	——	13.1.2	——	FISMA-2004 G.1.b, d, e, f
4.1.4f	Training and Awareness	AT-4	——	——	——	HUD Policy
4.1.4g	Training and Awareness	——	——	——	——	Best Practice
4.1.4h	Training and Awareness	AT-4	——	13.1.2	——	FISMA 2004 G.1.a, b, c, d
4.1.5a	Separation from Duty	AC-2 (1) AC-2 (3) AC-2 (4)	9.2.1 9.2.2	6.1.8 15.1.1 15.1.4 15.1.8 15.2.2 16.1.3 16.1.5 16.2.12	AC-2.1 AC-2.2 AC-3.2 SP-4.1	——
		PS-4	——	6.1.7	SP-4.1	——
		PS-5	——	6.1.7	SP-4.1	——
4.2.1a	General Physical Access	PE-1 PE-3	——	7	——	——
4.2.1b	General Physical Access	PE-7 PE-7 (1)	7.1.2	7.1.7	AC-3.1	——
		PE-8 PE-8 (1)	7.1.2	7.1.9	AC-4	——

HUD Policy Section Number	Control Name	NIST 800-53 Control #	ISO/IEC 17799	NIST 800-26	GAO FISCAM	Other
4.2.1c	General Physical Access	PE-7 PE-7 (1)	7.1.2	7.1.7	AC-3.1	——
4.2.1d	General Physical Access	PE-17	9.8.2	——	——	——
4.2.1e	General Physical Access	——	——	——	——	Best Practice
4.2.2a	Facilities Housing Information Technology Assets	PE-3	7.1.2 7.1.5	7.1.1 7.1.2 7.1.5 7.1.6	AC-3.1	——
4.2.2b	Facilities Housing Information Technology Assets	PE-2	——	7.1.1 7.1.2	AC-3.1	——
4.2.2c	Facilities Housing Information Technology Assets	PE-2	——	7.1.1 7.1.2	AC-3.1	——
4.2.2d	Facilities Housing Information Technology Assets	PE-3	7.1.2 7.1.5	7.1.1 7.1.2 7.1.5 7.1.6	AC-3.1	——
4.2.2e	Facilities Housing Information Technology Assets	PE-3	7.1.2 7.1.5	7.1.1 7.1.2 7.1.5 7.1.6	AC-3.1	——
4.2.2f	Facilities Housing Information Technology Assets	PE-5	——	7.2.1	——	——
4.2.2g	Facilities Housing Information Technology Assets	PE-6 PE-6 (1) PE-6 (2)	7.2.3	7.1.9	AC-4	——
4.2.2h	Facilities Housing Information Technology Assets	PE-9	7.2.3	7.1.16	SC-2.2	——
4.2.2i	Facilities Housing Information Technology Assets	PE-10	7.2.2	——	——	——
4.2.2j	Facilities Housing Information Technology Assets	——	——	——	SC-2.2	——
4.2.2k	Facilities Housing Information Technology Assets	PE-11 (1)	7.2.2	7.1.18	SC-2.2	——
4.2.2l	Facilities Housing Information Technology Assets	PE-11 (1)	7.2.2	7.1.18	SC-2.2	——
4.2.2m	Facilities Housing Information Technology Assets	PE-12	7.2.2	——	——	——
4.2.2n	Facilities Housing Information Technology Assets	PE-13 PE-13 (1) PE-13 (2)	7.2.1	7.1.12	SC-2.2	——

HUD Policy Section Number	Control Name	NIST 800-53 Control #	ISO/IEC 17799	NIST 800-26	GAO FISCAM	Other
4.2.2o	Facilities Housing Information Technology Assets	PE-13 PE-13 (1) PE-13 (2)	7.2.1	7.1.12	SC-2.2	——
4.2.2p	Facilities Housing Information Technology Assets	PE-13 PE-13 (1) PE-13 (2)	7.2.1	7.1.12	SC-2.2	——
4.2.2q	Facilities Housing Information Technology Assets	PE-14	——	7.1.14 7.1.15	SC-2.2	——
4.2.2r	Facilities Housing Information Technology Assets	PE-15	7.2.1	7.1.17	SC-2.2	——
4.2.2s	Facilities Housing Information Technology Assets	PE-16	7.1.5	7.1.3 7.1.11	AC-3.1	——
4.3a	Media Controls	MP-1	8.6.1	8	——	——
		MP-2 MP-2 (1)	8.6.1	8.2.1 8.2.2 8.2.3 8.2.6 8.2.7	——	——
		SI-12	10.7.3 12.2.4	——	——	——
4.3b	Media Controls	MP-3	——	8.2.5 8.2.6 10.2.9	——	——
		AC-15	5.2.2	8.2.4 16.1.6	AC-3.2	——
4.3c	Media Controls	MP-4	8.6.3 12.3.1	7.1.4 8.2.1 8.2.2 8.2.9	AC-3.1	——
4.3d	Media Controls	MP-6	8.6.1	3.2.11 3.2.12 3.2.13 8.2.8 8.2.9	AC-3.4	——
4.3e	Media Controls	MP-6	8.6.1	3.2.11 3.2.12 3.2.13 8.2.8 8.2.9	AC-3.4	——
4.3f	Media Controls	MP-6	8.6.1	3.2.11 3.2.12 3.2.13 8.2.8 8.2.9	AC-3.4	——
4.3g	Media Controls	SI-12	10.7.3 12.2.4	——	——	——

HUD Policy Section Number	Control Name	NIST 800-53 Control #	ISO/IEC 17799	NIST 800-26	GAO FISCAM	Other
4.3h	Media Controls	MP-6	8.6.1	3.2.11 3.2.12 3.2.13 8.2.8 8.2.9	AC-3.4	——
4.3i	Media Controls	MP-6	8.6.1	3.2.11 3.2.12 3.2.13 8.2.8 8.2.9	AC-3.4	——
		MP-7	7.2.6 8.6.2	3.2.11 3.2.12 3.2.13 8.2.10	AC-3.4	——
4.3j	Media Controls	MP-7	7.2.6 8.6.2	3.2.11 3.2.12 3.2.13 8.2.10	AC-3.4	——
4.3k	Media Controls	MP-5	8.7.2	8.2.2 8.2.4	——	——
4.3l	Media Controls	MP-2 MP-2 (1)	8.6.1	8.2.1 8.2.2 8.2.3 8.2.6 8.2.7	——	——
4.4	Data Communications	SC-1	——	——	——	——
4.4.1a	Telecommunications Protection Techniques	SC-8 SC-8 (1)	8.7.3	11.2.1 11.2.4 11.2.9 16.2.14	AC-3.2	——
4.4.1b	Telecommunications Protection Techniques	SC-9 SC-9 (1)	——	——	——	——
4.5.1a	Wireless Local Area Networks	AC-18 AC-18 (1)	——	——	——	——
4.5.1b	Wireless Local Area Networks	AC-18 AC-18 (1)	——	——	——	——
4.5.1c	Wireless Local Area Networks	AC-18 AC-18 (1)	——	——	——	——
4.5.1d	Wireless Local Area Networks	AC-18 AC-18 (1)	——	——	——	——
4.6.1a	Workstations	AC-11	——	16.1.4	AC-3.2	——
4.6.1b	Workstations	AC-11	——	16.1.4	AC-3.2	——
4.6.2a	Copyrighted Software	SA-6	12.1.2	10.2.10 10.2.13	SS-3.2 SP-2.1	——
4.6.2b	Copyrighted Software	SA-6	12.1.2	10.2.10 10.2.13	SS-3.2 SP-2.1	——
4.6.3a	User-Installed Software/Downloads	SA-7	10.4.1	10.2.10	SS-3.2	——

HUD Policy Section Number	Control Name	NIST 800-53 Control #	ISO/IEC 17799	NIST 800-26	GAO FISCAM	Other
4.6.4a	Personally-Owned Equipment and Software	AC-20	7.2.5 7.3.1 9.8.1	10.2.13	——	——
4.6.4b	Personally-Owned Equipment and Software	CM-1 AC-20	7.2.5 7.3.1 9.8.1	10.2.13	——	——
4.6.4c	Personally-Owned Equipment and Software	AC-20	7.2.5 7.3.1 9.8.1	10.2.13	——	——
4.6.5a	Hardware and Software Maintenance	CM-1	——	——	——	——
		AC-3 AC-3 (1)	9.2.4 9.4.6 9.4.8	15.1.1 16.1.1 16.1.2 16.1.3 16.1.7 16.1.9 16.2.7 16.2.10 16.2.11 16.2.15	AC-2 AC-3.2	Best Practice
4.6.5b	Hardware and Software Maintenance	MA-1	8.1.1	10	——	——
		MA-2 MA-2 (1) MA-2 (2)	7.2.4	10.1.1 10.1.3 10.2.1	SS-3.1	Best Practice
4.6.5c	Hardware and Software Maintenance	MA-2 MA-2 (1)	7.2.4	10.1.1 10.1.3 10.2.1	SS-3.1	Best Practice
4.6.5d	Hardware and Software Maintenance	MA-3	——	10.1.3 11.2.4	——	——
4.6.5e	Hardware and Software Maintenance	CM-1	——	——	——	——
4.6.5f	Hardware and Software Maintenance	MA-4 MA-4 (1)	9.4.5	10.1.1	SS-3.1	——
4.6.5g	Hardware and Software Maintenance	MA-5	7.2.4	10.1.1 10.1.3	SS-3.1	——
4.6.5h	Hardware and Software Maintenance	MA-6	——	9.1.2	SC-1.2	——
4.6.5i	Hardware and Software Maintenance	CM-1	——	——	——	——
4.6.5j	Hardware and Software Maintenance	MA-4 MA-4 (2)	9.4.5	10.1.1	SS-3.1	——
4.6.5k	Hardware and Software Maintenance	MA-4 MA-4(2)	9.4.5	10.1.1	SS-3.1	——
4.6.6a	Personal Use of Government Office Equipment and HUD Information Systems/Computers	——	——	——	——	Best Practice

HUD Policy Section Number	Control Name	NIST 800-53 Control #	ISO/IEC 17799	NIST 800-26	GAO FISCAM	Other
4.6.6b	Personal Use of Government Office Equipment and HUD Information Systems/Computers	——	——	——	——	Best Practice
4.7.1a	Security Incident and Violation Handling	IR-14	3.1.1	14	——	——
		IR-4 IR-4 (1)	8.1.3	14.1.1 14.1.2 14.1.6	SP-3.4	FISMA-2004 E.1.a
		IR-7 IR-7 (1)	——	8.1.1 14.1.1	SP-3.4	——
4.7.1b	Security Incident and Violation Handling	SI-4 SI-4 (1) SI-4 (2)	9.7.2	11.2.5 11.2.6	——	——
		SI-5	——	14.1.1 14.1.2 14.1.5	SP-3.4	——
4.7.1c	Security Incident and Violation Handling	SI-1	——	11.	——	——
		SI-6(1)	——	11.2.1 11.2.2	SS-2.2	——
		SI-2 SI-2 (1) SI-2 (2)	10.4.1	10.3.2 11.1.1 11.1.2 11.2.2 11.2.7	SS-2.2	——
4.7.1d	Security Incident and Violation Handling	IR-5 IR-5 (1)	8.1.3	14.1.3	——	FISMA-2004 F.1.a, b, c F.2.c
4.7.1e	Security Incident and Violation Handling	IR-2 IR-2 (1) IR-2 (2)	6.3.1	14.1.4	SP-3.4	——
4.7.1f	Security Incident and Violation Handling	IR-3 IR-3 (1)	——	——	——	——
4.7.1g	Security Incident and Violation Handling	IR-6 IR-6 (1)	8.1.3	14.1.1 14.1.2 14.1.3 14.2.1 14.2.3	——	——
4.7.1h	Security Incident and Violation Handling	IR-6 IR-6 (1)	8.1.3	14.1.1 14.1.2 14.1.3 14.2.1 14.2.3	——	FISMA 2004 E.1.b, c F.1.b, c
4.7.1i	Security Incident and Violation Handling	IR-6 IR-6 (1)	8.1.3	14.1.1 14.1.2 14.1.3 14.2.1 14.2.3	——	——
4.7.1j	Security Incident and Violation Handling	IR-7 IR-7 (1)	——	8.1.1 14.1.1	SP-3.4	——

HUD Policy Section Number	Control Name	NIST 800-53 Control #	ISO/IEC 17799	NIST 800-26	GAO FISCAM	Other
4.7.2a	Documentation (Manuals and Network Diagrams)	SA-5 SA-5 (1) SA-5 (2)	8.6.4	3.2.2 3.2.3 3.2.4 3.2.8 12.1.6	CC-2.1	——
4.7.3a	Information and Data Backup	CP-9 (1) CP-9 (2) CP-9 (3)	8.4.1	9.2.6 9.2.9 12.1.9	SC-2.1	——
4.7.3b	Information and Data Backup	CP-9 (1) CP-9 (2) CP-9 (3)	8.4.1	9.2.6 9.2.9 12.1.9	SC-2.1	——
4.7.3c	Information and Data Backup	CP-9 (1) CP-9 (2) CP-9 (3)	8.4.1	9.2.6 9.2.9 12.1.9	SC-2.1	——
4.7.3d	Information and Data Backup	CP-9 (1) CP-9 (2) CP-9 (3)	8.4.1	9.2.6 9.2.9 12.1.9	SC-2.1	——
4.7.3e	Information and Data Backup	CP-9 (1) CP-9 (2) CP-9 (3)	8.4.1	9.2.6 9.2.9 12.1.9	SC-2.1	——
4.7.3f	Information and Data Backup	CP-9 (1) CP-9 (2) CP-9 (3)	8.4.1	9.2.6 9.2.9 12.1.9	SC-2.1	——
4.7.4a	Input/Output Controls	SI-10 SI-10 (1)	——	——	——	——
4.7.4b	Input/Output Controls	SI-11	——	——	——	——
Technical Policies						
5.1a	Identification and Authentication	IA-4	9.5.3	15.1.1 15.2.2 16.1.5 15.1.8	AC-2.1 AC-3.2 SP-4.1	——
		IA-2 IA-2 (1)	9.5.3	15.1	——	——
		IA-1	——	11.2.3	——	——
5.1b	Identification and Authentication	IA-4	9.5.3	15.1.1 15.2.2 16.1.5 15.1.8	AC-2.1 AC-3.2 SP-4.1	——
		IA-5	——	15.1.7 15.1.10 15.1.11 15.1.12 15.1.13	AC-3.2	——
5.1c	Identification and Authentication	——	——	——	——	Best Practice

HUD Policy Section Number	Control Name	NIST 800-53 Control #	ISO/IEC 17799	NIST 800-26	GAO FISCAM	Other
5.1d	Identification and Authentication	AC-2 (1) AC-2 (3) AC-2 (4)	9.2.1 9.2.2	6.1.8 15.1.1 15.1.4 15.1.8 15.2.2 16.1.3 16.1.5 16.2.12	AC-2.1 AC-2.2 AC-3.2 SP-4.1	——
5.1e	Identification and Authentication	AC-2 (1) AC-2 (3) AC-2 (4)	9.2.1 9.2.2	6.1.8 15.1.1 15.1.4 15.1.8 15.2.2 16.1.3 16.1.5 16.2.12	AC-2.1 AC-2.2 AC-3.2 SP-4.1	——
5.1.1a	E-Authentication	IA-2	9.5.3	15.1	——	OMB-04-04
		IA-7	——	16.1.7	——	——
5.1.1b	E-Authentication	IA-5	——	——	——	OMB-04-04
5.1.2a	Device and Application Authentication	IA-3	9.4.4 9.5.1 9.8.1	16.2.7	——	——
5.1.3a	Passwords	IA-5	——	15.1.7 15.1.10 15.1.11 15.1.12 15.1.13	AC-3.2	——
5.1.3b	Passwords	IA-5	——	15.1.7 15.1.10 15.1.11 15.1.12 15.1.13	AC-3.2	——
5.1.3c	Passwords	IA-5	——	15.1.7 15.1.10 15.1.11 15.1.12 15.1.13	AC-3.2	——
5.1.3d	Passwords	IA-5	——	15.1.7 15.1.10 15.1.11 15.1.12 15.1.13	AC-3.2	——
5.1.3e	Passwords	IA-5	——	15.1.7 15.1.10 15.1.11 15.1.12 15.1.13	AC-3.2	Best Practice

HUD Policy Section Number	Control Name	NIST 800-53 Control #	ISO/IEC 17799	NIST 800-26	GAO FISCAM	Other
5.1.3f	Passwords	IA-5	——	15.1.7 15.1.10 15.1.11 15.1.12 15.1.13	AC-3.2	——
5.1.3g	Passwords	IA-5	——	15.1.7 15.1.10 15.1.11 15.1.12 15.1.13	AC-3.2	——
		IA-6	——	——	——	——
5.1.3h	Passwords	IA-5	——	15.1.7 15.1.10 15.1.11 15.1.12 15.1.13	AC-3.2	——
		SC-11	——	16.2.7	——	——
5.1.3i	Passwords	IA-5	——	15.1.7 15.1.10 15.1.11 15.1.12 15.1.13	AC-3.2	——
5.1.3j	Passwords	IA-5	——	15.1.7 15.1.10 15.1.11 15.1.12 15.1.13	AC-3.2	——
5.2a	Access Control	AC-1	9.1.1 9.4.1	15 16	——	——
		AC-2 (1) AC-2 (3) AC-2 (4)	9.2.1 9.2.2	6.1.8 15.1.1 15.1.4 15.1.8 15.2.2 16.1.3 16.1.5 16.2.12	AC-2.1 AC-2.2 AC-3.2 SP-4.1	——
5.2b	Access Control	AC-2 (1) AC-2 (3) AC-2 (4)	9.2.1 9.2.2	6.1.8 15.1.1 15.1.4 15.1.8 15.2.2 16.1.3 16.1.5 16.2.12	AC-2.1 AC-2.2 AC-3.2 SP-4.1	——

HUD Policy Section Number	Control Name	NIST 800-53 Control #	ISO/IEC 17799	NIST 800-26	GAO FISCAM	Other
5.2c	Access Control	AC-5	8.1.4	6.1.1 6.1.2 6.1.3 15.2.1 16.1.2 17.1.5	SD-1.2	——
		AC-6	9.2.2	16.1.2 16.1.3 17.1.5	AC-3.2	——
5.2d	Access Control	AC-2 AC-2 (2)	——	——	——	——
5.2e	Access Control	AC-2 (1) AC-2 (3) AC-2 (4)	9.2.1 9.2.2	6.1.8 15.1.1 15.1.4 15.1.8 15.2.2 16.1.3 16.1.5 16.2.12	AC-2.1 AC-2.2 AC-3.2 SP-4.1	——
5.2f	Access Control	AC-14	——	16.2.12	——	——
5.2.1a	Automatic Account Lockout	AC-7	9.5.2	15.1.14	AC-3.2	——
5.2.1b	Automatic Account Lockout	AC-7	9.5.2	15.1.14	AC-3.2	——
5.2.2a	Logon and Session Security	AC-12	9.5.7	16.1.4 16.2.6	AC-3.2	——
		SC-10	——	16.2.6	AC-3.2	——
5.2.2b	Logon and Session Security	AC-10	——	——	——	——
		SC-17	10.3.5	——	——	——
5.2.3a	Warning Banner	AC-8	9.5.2	16.2.13 17.1.9	AC-3.2	——
5.2.3b	Warning Banner	AC-8	9.5.2	16.2.13 17.1.9	AC-3.2	——
5.2.3c	Warning Banner	AC-8	9.5.2	16.2.13 17.1.9	AC-3.2	——
Audit and Accountability						
5.3a	Audit and Accountability	AU-1	——	17	——	——
		AU-2 AU-2 (1)	11.1.2	17.1.1 17.1.2 17.1.4	——	——
		AU-3 AU-3 (1) AU-3 (2)	9.7.2	17.1.1	——	——
5.3b	Audit and Accountability	AU-9	12.3.2	17.1.3 17.1.4	——	——
5.3c	Audit and Accountability	AU-11	10.7.1 12.1.3	17.1.4	——	——

HUD Policy Section Number	Control Name	NIST 800-53 Control #	ISO/IEC 17799	NIST 800-26	GAO FISCAM	Other
5.3d	Audit and Accountability	AC-13 AC-13 (1)	9.2.4	7.1.10 11.2.2 16.1.10 17.1.6 17.1.7	AC-4 AC-4.3 SS-2.2	——
		AU-6 AU-6 (1)	9.7.2	17.1.1	——	——
5.3e	Audit and Accountability	AU-4	9.7.2	——	——	——
5.3f	Audit and Accountability	AU-5 AU-5 (1)	9.7.2	——	——	——
5.3g	Audit and Accountability	AU-5	9.7.2	——	——	——
5.3h	Audit and Accountability	AU-7 AU-7 (1)	——	17.1.2 17.1.7	——	——
5.3i	Audit and Accountability	AU-2 AU-2 (1)	11.1.2	17.1.1 17.1.2 17.1.4	——	——
		AU-3 AU-3 (1) AU-3 (2)	9.7.2	17.1.1	——	——
5.3j	Audit and Accountability	AU-8	9.7.3	——	——	——
5.4.1a	Remote Access and Dial-In	AC-17 AC-17 (1) AC-17 (2) AC-17 (3)	9.4.3 9.4.4	16.2.12 16.2.4 16.2.8	AC-3.2	——
5.4.1b	Remote Access and Dial-In	AC-17 AC-17 (1) AC-17 (2) AC-17 (3)	9.4.3 9.4.4	16.2.12 16.2.4 16.2.8	AC-3.2	——
5.4.1c	Remote Access and Dial-In	AC-17 AC-17 (1) AC-17 (2) AC-17 (3)	9.4.3 9.4.4	16.2.12 16.2.4 16.2.8	AC-3.2	——
5.4.1d	Remote Access and Dial-In	AC-17 AC-17 (1) AC-17 (2) AC-17 (3)	9.4.3 9.4.4	16.2.12 16.2.4 16.2.8	AC-3.2	——
5.4.2a	Network Security Monitoring	SI-4 SI-4 (1) SI-4 (2)	9.7.2	11.2.5 11.2.6	——	——
5.4.2b	Network Security Monitoring	SI-4 SI-4 (1) SI-4 (2)	9.7.2	11.2.5 11.2.6	——	——
5.4.2c	Network Security Monitoring	RA-5	——	10.3.2 14.2.1	——	FISMA-2004 E.2.a
5.4.2.d	Network Security Monitoring	——	——	——	——	NIST SP 800-42

HUD Policy Section Number	Control Name	NIST 800-53 Control #	ISO/IEC 17799	NIST 800-26	GAO FISCAM	Other
5.4.3a	Network Connectivity	AC-3 AC-3 (1)	9.2.4 9.4.6 9.4.8	15.1.1 16.1.1 16.1.2 16.1.3 16.1.7 16.1.9 16.2.7 16.2.10 16.2.11 16.2.15	AC-2 AC-3.2	——
		AC-1	9.1.1 9.4.1	15 16	——	——
5.4.3b	Network Connectivity	SC-7 SC-7 (1)	9.4.6	16.2.2 16.2.7 16.2.8 16.2.9 16.2.10 16.2.11 16.2.14	AC-3.2	——
		AC-4	9.4.6 9.4.8	——	——	——
5.4.3c	Network Connectivity	CM-7 CM-7 (1)	9.4.2	10.3.1	——	——
5.4.3d	Network Connectivity	SC-7 SC-7 (1)	9.4.6	16.2.2 16.2.7 16.2.8 16.2.9 16.2.10 16.2.11 16.2.14	AC-3.2	——
5.4.3e	Network Connectivity	SC-7 SC-7 (1)	9.4.6	16.2.2 16.2.7 16.2.8 16.2.9 16.2.10 16.2.11 16.2.14	AC-3.2	——
5.4.3f	Network Connectivity	SC-7 SC-7 (1)	9.4.6	16.2.2 16.2.7 16.2.8 16.2.9 16.2.10 16.2.11 16.2.14	AC-3.2	——
5.4.3g	Network Connectivity	AC-19	9.5.1 9.8.1	7.3.1 7.3.2	——	——
5.4.3h	Network Connectivity	AC-19	9.5.1 9.8.1	7.3.1 7.3.2	——	——

HUD Policy Section Number	Control Name	NIST 800-53 Control #	ISO/IEC 17799	NIST 800-26	GAO FISCAM	Other
5.4.4a	Internet Security	SC-18	——	——	——	——
		SC-7 SC-7 (1)	9.4.6	16.2.2 16.2.7 16.2.8 16.2.9 16.2.10 16.2.11 16.2.14	AC-3.2	——
5.4.4b	Internet Security	SC-7 SC-7 (1)	9.4.6	16.2.2 16.2.7 16.2.8 16.2.9 16.2.10 16.2.11 16.2.14	AC-3.2	——
5.4.4c	Internet Security	SC-18	——	——	——	——
5.4.4d	Internet Security	SC-5	8.1.3	——	——	——
5.4.4e	Internet Security	SC-14	8.7.6	16.3.1	——	——
5.4.5a	Personal Email Accounts	——	——	——	——	Best Practice
5.4.5b	Personal Email Accounts	——	——	——	——	HUD Policy
5.5.1a	Encryption	SC-13	——	16.1.7 16.1.8	——	FIPS 46-3 FIPS 140-2 FIPS 197
5.5.1b	Encryption	SC-12	10.3.5	16.1.7 16.1.8	——	——
5.5.1c	Encryption	AC-17 AC-17 (1) AC-17 (2) AC-17 (3)	9.4.3 9.4.4	16.2.12 16.2.4 16.2.8	AC-3.2	——
		SC-9 SC-9 (1)	——	——	——	——
		SC-8 SC-8 (1)	8.7.3	11.2.1 11.2.4 11.2.9 16.2.14	AC-3.2	——
		IA-7	——	16.1.7	——	——
		AC-18 AC-18 (1)	——	——	——	——
5.5.1d	Encryption	AC-19 (1)	9.5.1 9.8.1	7.3.1 7.3.2	——	——
5.5.2a	Public Key Infrastructure	——	——	——	——	Best Practice
5.5.2b	Public Key Infrastructure	SC-17	——	——	——	——
5.5.2c	Public Key Infrastructure	SC-17	——	——	——	——
5.5.2d	Public Key Infrastructure	——	——	——	——	Best Practice
5.5.2e	Public Key Infrastructure	——	——	——	——	Best Practice
5.5.2f	Public Key Infrastructure	IA-7	——	16.1.7	——	OMB GPEA
5.5.2g	Public Key Infrastructure	IA-7	——	16.1.7	——	Homeland Security PDD-12

HUD Policy Section Number	Control Name	NIST 800-53 Control #	ISO/IEC 17799	NIST 800-26	GAO FISCAM	Other
5.5.3a	Public Key/Private Key	——	——	——	——	Best Practice
5.5.3b	Public Key/Private Key	——	——	——	——	FIPS 186-2
5.5.3c	Public Key/Private Key	——	——	——	——	FIPS 186-2
5.6a	Malicious Code Protection	SI-1	——	11	——	——
		SI-3 SI-3 (1) SI-3 (2)	8.3.1	11.1.1 11.1.2	——	——
		SI-4 SI-4 (1) SI-4 (2)	9.7.2	11.2.5 11.2.6	——	——
		SI-5	——	14.1.1 14.1.2 14.1.5	SP-3.4	——
5.6b	Malicious Code Protection	SI-1	——	11	——	——
5.6c	Malicious Code Protection	SI-8 SI-8 (1) SI-8 (2)	——	——	——	——
5.7a	Miscellaneous	SC-15	——	——	——	Best Practice
5.7b	Miscellaneous	SC-19	——	——	——	Best Practice

APPENDIX B. ACRONYMS

3DES	Triple Data Encryption Standard
AES	Advanced Encryption Standard
AIS	Automated Information System
AO	Authorizing Official
AP	Access Point
BIA	Business Impact Analysis
C&A	Certification and Accreditation
CA	Certification Authority
CBA	Cost-Benefit Analysis
CD	Compact Disk
CFR	Code of Federal Regulations
CIO	Chief Information Officer
CIP	Critical Infrastructure Protection
CISO	Chief Information Security Officer
CM	Configuration Management
CO	Contracting Officer
COOP	Continuity of Operations
COTS	Commercial off-the Shelf
CPIC	Capital Planning & Investment Control
CSA	Computer Security Act
CSIRC	Computer Security Incident Response Center
CSO	Chief Security Officer
DHCP	Dynamic Host Configuration Protocol
DoS	Denial of Service
DVD	Digital Versatile Disk
EA	Enterprise Architecture
EAP	Extensible Authentication Protocol
EO	Executive Order
FAR	Federal Acquisition Regulation
FIPS	Federal Information Processing Standard

FISCAM	Federal Information System Controls Audit Manual
FISMA	Federal Information Security Management Act
GAO	General Accountability Office
GISRA	Government Information Security Reform Act
GSA	General Service s Administration
GTM	Government Technical Monitor
GTR	Government Technical Representative
HIPAA	Health Insurance Portability and Accountability Act
HSPD	Homeland Security Presidential Directive
HUD	Department of Housing and Urban Development
HUDAR	HUD Acquisition Regulation
IATO	Interim Authority to Operate
ID	Identification
IDS	Intrusion Detection System
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronic Engineers
IG	Inspector General
ISO	International Standards Organization
ISSB	Information Systems Security Branch
ISSO	Information System Security Officer
IT	Information Technology
ITMRA	Information Technology Management Reform Act
LAN	Local Area Network
MAC	Media Access Control
MBI	Minimum Background Investigation
MOA	Memorandum of Agreement
NIST	National Institute of Standards and Technology
NIST SP	National Institute of Standards and Technology Special Publication
NSA	National Security Agency
O&M	Operations & Maintenance
OAMS	Office of Administration and Management Services
OIG	Office of Inspector General

OMB	Office of Management and Budget
OPC	Office of Procurement and Contracts
OPM	Office of Personnel Management
PDA	Personal Digital Assistant
PDD	Presidential Decision Directive
PIV	Personal Identity Verification
PKI	Public Key Infrastructure
POA&M	Plans of Action and Milestones
POC	Point of Contact
QA	Quality Assurance
SDLC	System Development Life Cycle
SOW	Statement of Work
SP	Special Publication
SSL	Secure Sockets Layer
TBD	To Be Determined
TCP/IP	Transmission Control Protocol/Internet Protocol
TLS	Transport Layer Security
TSP	Telecommunications Service Priority
U.S.C.	United States Code
USB	Universal Serial Bus
USCERT	United States Computer Emergency Readiness Team
USERID	User ID
VoIP	Voice over Internet Protocol
VPN	Virtual Private Network
WAN	Wide Area Network
WAP	WiFi Access Protection
WG	Working Group
WLAN	Wireless Local Area Network

INFORMATION TECHNOLOGY SECURITY POLICY

2400.25

U.S. DEPARTMENT OF
HOUSING AND URBAN DEVELOPMENT

INFORMATION TECHNOLOGY
SECURITY POLICY

Handbook 2400.25, Rev. 1
(All previous versions are obsolete)

Table of Contents

Special Attention of:

Transmittal for Handbook No: 2400.25 REV-1

Issued: May 20, 2005

1. This Transmits: HUD Handbook 2400.25 REV-1, Information Technology Security Policy

2. Summary:

The purpose of this policy is to prescribe the authorities, minimal acceptable standards and responsibilities for managing a Computer Security Program focusing on management, technical and operational security controls. The objective is to provide security protection commensurate with the risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption or modification to an information technology asset.

The Federal Information Security Management Act 2002 mandates that agencies establish security programs to ensure the confidentiality, integrity and availability of its information technology (IT) assets. The Office of Management and Budget (OMB) Circular A-130 *Management of Federal Information Resources* directs all government agencies to implement and maintain a Computer Security Program.

3. Filing Instructions:

Remove:	Insert:
Table of Contents Handbook 2400.25, dated 9/2004	Table of Contents Handbook 2400.25, Rev. 1, dated 5/2005