

2400.25 G



U.S. DEPARTMENT OF HOUSING AND URBAN DEVELOPMENT

INFORMATION TECHNOLOGY SECURITY PROCEDURES

Version 2.0

April 30, 2007

Document Change History

Version Number	Date	Description
2.0	November 2006	Revised to match latest draft of NIST framework and incorporate new HUD requirements

Table of Contents

1.0	Introduction.....	1
1.1	Applicable Regulations and Standards	1
1.2	Document Organization	1
2.0	Roles and Responsibilities	4
2.1	Secretary of the Department of Housing and Urban Development	4
2.2	Chief Information Officer	4
2.3	Chief Information Security Officer.....	4
2.4	Office of Information Technology Security	4
2.5	Deputy Chief Information Officer for IT Operations	5
2.6	HUD Computer Security Incident Response Center	5
2.7	HUD Privacy Officer	5
2.8	Office of Security and Emergency Planning	5
2.9	Systems Engineering Oversight and Performance Management Division	5
2.10	Office of the Chief Procurement Officer (OCPO).....	5
2.11	Contracting Officer	5
2.12	Office of Human Resources.....	6
2.13	Office of the Inspector General.....	6
2.14	HUD General Counsel	6
2.15	Investment Review Board.....	6
2.16	Configuration Control Board	6
2.17	Program Office/System Owner.....	6
2.18	Information System Security Officer.....	7
2.19	System Administrator	7
2.20	Certification Agent.....	7
2.21	Authorizing Official.....	7
2.22	Supervisor	7
2.23	Users	8
2.24	Individuals with Key Contingency Roles	8
2.25	Service Provider.....	8
2.26	Developers	8
3.0	Management Procedures.....	9
3.1	Risk Assessment	9
3.1.1	Risk Assessment Policy and Procedures.....	9
3.1.2	Security Categorization.....	10
3.1.3	Risk Assessment	10
3.1.4	Risk Assessment Update.....	11
3.1.5	Vulnerability Scanning	11
3.1.6	E-Authentication Risk Assessment.....	12
3.2	Planning	13
3.2.1	Security Planning Policy and Procedures	14
3.2.2	System Security Plan	14

3.2.3	System Security Plan Update.....	14
3.2.4	Rules of Behavior	15
3.2.5	Privacy Impact Assessments.....	15
3.2.6	Security-Related Activity Planning	16
3.2.7	HUD Inventory	16
3.2.8	ISSO.....	17
3.3	System and Services Acquisition.....	17
3.3.1	System and Services Acquisition Policy and Procedures	17
3.3.2	Allocation of Resources	18
3.3.3	Life Cycle Support.....	18
3.3.4	Acquisitions	19
3.3.5	Information System Documentation	20
3.3.6	Software Usage Restrictions	20
3.3.7	User Installed Software.....	21
3.3.8	Security Engineering Principles.....	21
3.3.9	Outsourced Information System Services.....	22
3.3.10	Developer Configuration Management.....	22
3.3.11	Developer Security Testing.....	23
3.4	Certification, Accreditation, and Security Assessments	23
3.4.1	Certification, Accreditation, and Security Assessment Policy and Procedures..	24
3.4.2	Security Assessment	24
3.4.3	Information System Connections.....	25
3.4.4	Security Certification.....	25
3.4.5	Plan of Action and Milestones.....	26
3.4.6	Security Accreditation	27
3.4.7	Continuous Monitoring.....	27
4.0	Operational Procedures.....	29
4.1	Personnel Security	29
4.1.1	Personnel Security Policy and Procedures.....	29
4.1.2	Position Categorization.....	30
4.1.3	Personnel Screening.....	30
4.1.4	Personnel Termination.....	31
4.1.5	Personnel Transfer	31
4.1.6	Access Agreements.....	32
4.1.7	Third-Party Personnel Security.....	32
4.1.8	Personnel Sanctions	32
4.2	Physical and Environmental Protection.....	33
4.2.1	Physical and Environmental Protection Policy and Procedures	33
4.2.2	Physical Access Authorizations.....	34
4.2.3	Physical Access Control	34
4.2.4	Access Control for Transmission Medium	35
4.2.5	Access Control for Display Medium	35
4.2.6	Monitoring Physical Access	35
4.2.7	Visitor Control	36
4.2.8	Access Records	36

4.2.9	Power Equipment and Power Cabling	37
4.2.10	Emergency Shutoff	37
4.2.11	Emergency Power	38
4.2.12	Emergency Lighting.....	39
4.2.13	Fire Protection.....	39
4.2.14	Temperature and Humidity Controls	40
4.2.15	Water Damage Protection	40
4.2.16	Delivery and Removal	40
4.2.17	Alternate Work Site	41
4.2.18	Location of Information System Components.....	41
4.2.19	Information Leakage.....	42
4.2.20	Facilities Housing HUD Information Systems	42
4.2.21	Redundant Air-Cooling Systems	42
4.3	Contingency Planning.....	43
4.3.1	Contingency Planning Policy and Procedures	43
4.3.2	Contingency Plan.....	43
4.3.3	Contingency Training	44
4.3.4	Contingency Plan Testing and Exercises.....	45
4.3.5	Contingency Plan Update	46
4.3.6	Alternate Storage Site	46
4.3.7	Alternate Processing Site	47
4.3.8	Telecommunications Services	48
4.3.9	Information System Backup	49
4.3.10	Information System Recovery and Reconstitution	50
4.4	Configuration Management	50
4.4.1	Configuration Management Policy and Procedures	51
4.4.2	Baseline Configuration	51
4.4.3	Configuration Change Control.....	52
4.4.4	Monitor Configuration Changes	53
4.4.5	Access Restrictions for Change	53
4.4.6	Configuration Settings	54
4.4.7	Least Functionality.....	54
4.4.8	Information System Component Inventory	55
4.5	Maintenance.....	55
4.5.1	System Maintenance Policy and Procedures	55
4.5.2	Controlled Maintenance.....	56
4.5.3	Maintenance Tools.....	57
4.5.4	Remote Maintenance	57
4.5.5	Maintenance Personnel	59
4.5.6	Timely Maintenance	59
4.6	System and Information Integrity	59
4.6.1	System and Information Integrity Policy and Procedures	60
4.6.2	Flaw Remediation	60
4.6.3	Malicious Code Protection.....	61
4.6.4	Information System Monitoring Tools and Techniques	62
4.6.5	Security Alerts and Advisories	63

4.6.6	Security Functionality Verification.....	63
4.6.7	Software and Information Integrity	64
4.6.8	Spam Protection.....	64
4.6.9	Information Input Restrictions.....	65
4.6.10	Information Accuracy, Completeness, Validity, and Authenticity.....	65
4.6.11	Error Handling	66
4.6.12	Information Output Handling and Retention.....	66
4.7	Media Protection.....	66
4.7.1	Media Protection Policy and Procedures	67
4.7.2	Media Access.....	67
4.7.3	Media Labeling	67
4.7.4	Media Storage	68
4.7.5	Media Transport.....	68
4.7.6	Media Sanitization and Disposal	69
4.8	Incident Response	70
4.8.1	Incident Response Policy and Procedures	70
4.8.2	Incident Response Training	70
4.8.3	Incident Response Testing and Exercises	71
4.8.4	Incident Handling.....	71
4.8.5	Incident Monitoring	72
4.8.6	Incident Reporting	72
4.8.7	Incident Response Assistance.....	73
4.9	Awareness and Training	73
4.9.1	Security Awareness and Training Policy and Procedures	74
4.9.2	Security Awareness.....	74
4.9.3	Security Training	75
4.9.4	Security Training Records	76
4.9.5	Contacts with Security Groups and Associations	76
5.0	Technical Procedures.....	77
5.1	Identification and Authentication	77
5.1.1	Identification and Authentication Policy and Procedures.....	77
5.1.2	User Identification and Authentication.....	77
5.1.3	Device Identification and Authentication	78
5.1.4	Identifier Management.....	79
5.1.5	Authentication Management.....	79
5.1.6	Authentication Feedback	80
5.1.7	Cryptographic Module Authentication	81
5.2	Access Control.....	81
5.2.1	Access Control Policy and Procedures	82
5.2.2	Account Management	82
5.2.3	Access Enforcement.....	83
5.2.4	Information Flow Enforcement.....	84
5.2.5	Separation of Duties.....	84
5.2.6	Least Privilege	85
5.2.7	Unsuccessful Login Attempts	85

5.2.8	System Use Notification	86
5.2.9	Previous Logon Notification.....	86
5.2.10	Concurrent Session Control	86
5.2.11	Session Lock	87
5.2.12	Session Termination.....	87
5.2.13	Supervision and Review—Access Control.....	87
5.2.14	Permitted Actions without Identification or Authentication.....	88
5.2.15	Automated Marking	88
5.2.16	Automated Labeling.....	89
5.2.17	Remote Access.....	89
5.2.18	Wireless Access Restrictions	90
5.2.19	Access Control for Portable and Mobile Devices.....	91
5.2.20	Use of External Information Systems	91
5.2.21	Personal Use of Government Equipment.....	92
5.3	Audit and Accountability	92
5.3.1	Audit and Accountability Policy and Procedures	93
5.3.2	Auditable Events.....	93
5.3.3	Content of Audit Records	94
5.3.4	Audit Storage Capacity	95
5.3.5	Response to Audit Processing Failures.....	95
5.3.6	Audit Monitoring, Analysis, and Reporting	96
5.3.7	Audit Reduction and Report Generation.....	96
5.3.8	Time Stamps	97
5.3.9	Protection of Audit Information.....	97
5.3.10	Non-Repudiation.....	98
5.3.11	Audit Record Retention	98
5.4	System and Communications Protection	98
5.4.1	System and Communications Policy and Procedures.....	99
5.4.2	Application Partitioning.....	99
5.4.3	Security Function Isolation	99
5.4.4	Information Remnants	100
5.4.5	Denial of Service Protection	100
5.4.6	Resource Priority	101
5.4.7	Boundary Protection	101
5.4.8	Transmission Integrity	102
5.4.9	Transmission Confidentiality.....	103
5.4.10	Network Disconnect.....	103
5.4.11	Trusted Path	104
5.4.12	Cryptographic Key Establishment and Management	104
5.4.13	Use of Cryptography.....	105
5.4.14	Public Access Protections	105
5.4.15	Collaborative Computing.....	105
5.4.16	Transmission of Security Parameters.....	106
5.4.17	Public Key Infrastructure Certificates	106
5.4.18	Mobile Code.....	106
5.4.19	Voice Over Internet Protocol	107

5.4.20 Secure Name/Address Resolution Service (Authoritative Source)	107
5.4.21 Secure Name/Address Resolution Service (Recursive or Caching Resolver) ..	108
5.4.22 Architecture and Provisioning for Name/Address Resolution Service.....	108
5.4.23 Secure Name/Address Resolution Service (Recursive or Caching Resolver) ..	108
Acronyms	110
Definitions.....	113

1.0 Introduction

The Housing and Urban Development (HUD) *Information Technology Security Policy Handbook 2400.25, Rev. 1* (policy) states that 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 information system assets with due diligence and take the necessary steps to safeguard them while complying with federal mandates and the dictates of good stewardship.”

The HUD *Information Technology Security Procedures Handbook* provides guidance for implementing HUD security policies, which are in place to assure the protection of HUD’s information system assets. Together, the two documents provide HUD with a security foundation to preserve the confidentiality, integrity, and availability of HUD information and the value of information technology assets, as well as ensure the continued delivery of HUD services enabled by information systems. These procedures are to be used by all HUD employees and contractors who either use or are responsible for any system component.

The procedures document will be updated, as necessary, to reflect any changes in HUD policies or federal laws, regulations, or policies. At a minimum, it will be reviewed annually to coincide with the annual security policy review.

1.1 Applicable Regulations and Standards

The procedures in this handbook align with existing HUD and National Institute of Standards and Technology (NIST) documentation, as well as with Office of Management and Budget (OMB) regulations. The procedures provide a plan for the implementation of and compliance with required security controls. Other guidance documents are referenced, when possible, to streamline procedures, eliminate document duplication, and ease the burden of updating the procedures document as guidance documents change.

This handbook integrates security requirements from the Federal Information Processing Standard (FIPS) 200, *Minimum Security Requirements for Federal Information and Information Systems*, and controls that are documented in NIST Special Publication (SP) 800-53, *Recommended Security Controls for Federal Information Systems*, with procedures for compliance with HUD’s security policy.

1.2 Document Organization

The *Information Technology Security Procedures Handbook* is divided into three main sections:

- Chapter 1 covers the introduction and document organization.
- Chapter 2 provides a high-level outline of HUD’s organizational entities and their corresponding roles and responsibilities.
- Chapters 3, 4, and 5 describe procedures by class, family, control, security categorization, and supporting procedures.

To simplify compliance with FIPS 200 and NIST SP 800-53, the procedures are organized by class and family. This format facilitates preparing security documentation, as required in the HUD System Development Methodology (SDM), and establishing the security assessment criteria used during the certification and accreditation process.

As each new class begins, there is an overview and description of the class, associated controls, and associated procedures. At the beginning of each family, the associated FIPS 200 requirement is documented to set the framework for each family. A table aligns the NIST SP 800-53 control number with associated HUD security policy numbers. When a HUD-specific policy is not addressed in NIST SP 800-53 controls, a control was established for the HUD-specific policy requirement and placed within a class and control family. These additional controls are inserted at the end of the control family.

The numbering scheme relates to the order of controls within NIST SP 800-53. To illustrate the breakdown of the control numbering scheme, Section Number 3.1.1 represents the *Management* class, *Risk Assessment* family, and *Risk Assessment Policy and Procedures* control. The first number always represents the class associated with the specific control. The second number represents the family associated with the specific control; the third number represents the specific control in the family. Additional enhancements within a control are denoted with an “E” and a sequential number. Enhancements are used when greater protection is required (see Figure 1).

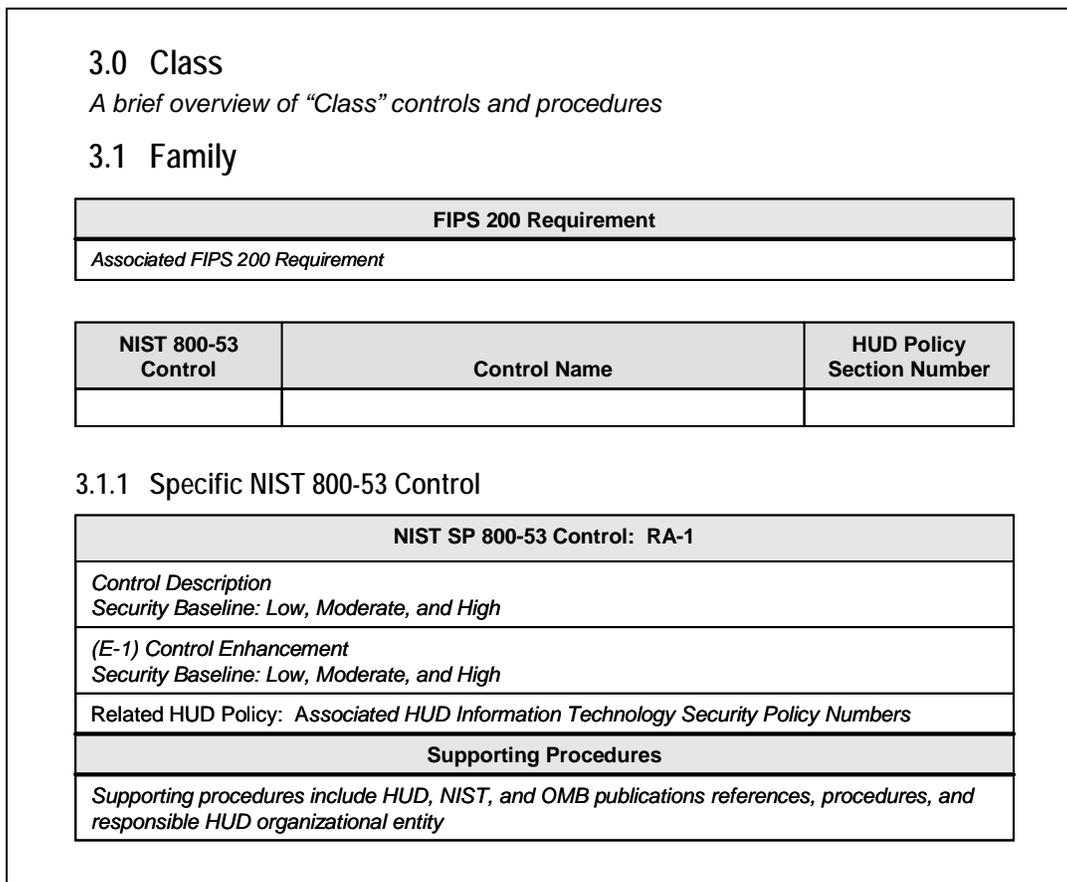


Figure 1. Procedures Organization

The supporting procedures for each control outline the steps to achieve the control, reference supporting guidance and documents, and identify the associated organizational entity or individual's role within HUD responsible for each step outlined in the procedure. Within supporting procedures, steps to achieve security baselines of moderate- and high-impact systems are highlighted.

The first control within each family is a requirement to develop policies and procedures for that family. These controls are satisfied by the HUD *Information Technology Security Policy Handbook 2400.25, Rev. 1* and this procedures handbook; therefore, the "Supporting Procedures" section is replaced with an "Implementation" section.

2.0 Roles and Responsibilities

The responsibility for HUD information and information systems must be integrated into all aspects of HUD's business operations and use of technology; therefore, these procedures apply to all HUD employees 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 responsibilities. The roles and responsibilities in this section focus only on the information security roles and responsibilities for the individuals and organizations that are involved in HUD's information security program. These individuals and organizations often have additional responsibilities.

2.1 Secretary of the Department of Housing and Urban Development

The Secretary of HUD is responsible for ensuring that HUD information and information systems are protected in accordance with congressional and presidential directives. To that end, the Secretary will ensure the Chief Information Officer (CIO), Chief Information Security Officer (CISO), and Program Offices or System Owners have the support and resources they need to effectively implement information security throughout HUD.

2.2 Chief Information Officer

The Chief Information Officer (CIO) is responsible for establishing and overseeing the department-wide Information Security Program and provides information security consulting assistance to all HUD program offices for their individual program. The CIO appoints, in writing, the CISO and reviews and evaluates the HUD information security program at least annually.

2.3 Chief Information Security Officer

The Chief Information Security Officer (CISO) directs the management of HUD's information security program. The CISO and the OITS security staff establish a strong foundation for HUD security by maintaining the HUD information security program. The CISO interacts with internal and external resources, and coordinates security compliance across HUD organizational elements.

2.4 Office of Information Technology Security

OITS issues department-wide information security policy, guidance, and architecture requirements for all HUD systems and provides oversight to ensure the policies are implemented. The office develops and maintains the HUD information security program serving as the agency-wide principal advisor on information system security matters. OITS reviews and approves the processes, techniques, and methodologies planned for securing information system assets.

2.5 Deputy Chief Information Officer for IT Operations

The Deputy CIO for IT Operations is responsible for the IT infrastructure (e.g., general support systems) that provides shared services across HUD. Following HUD information security program policy and guidance, the Deputy CIO for IT Operations ensures the implementation of security components to secure HUD's information system assets. Additional security responsibilities include addressing security technology issues and directing contingency planning.

2.6 HUD Computer Security Incident Response Center

The HUD Computer Security Incident Response Center (CSIRC) combats the disruptive short- and long-term effects of security threats, flaws, vulnerabilities, and incidents directed at HUD. The CSIRC also maintains a security incident reporting and handling capability and is responsible for operational and technical controls.

2.7 HUD Privacy Officer

The HUD Privacy Officer assures that service and service arrangement meet privacy policies regarding the protection, dissemination, and disclosure of information.

2.8 Office of Security and Emergency Planning

The Office of Security and Emergency Planning (OSEP) is responsible for the physical and environmental security controls that protect HUD's information system assets. Facility security and access are maintained by this office. These controls include ensuring the continuity of operations plans development and continuity of government programs, security clearance management, and physical access control mechanisms.

2.9 Systems Engineering Oversight and Performance Management Division

The Systems Engineering Oversight and Performance Management Division (SEO&PMD) maintains the Inventory of Automated Systems (IAS) that contains information on all HUD IT systems.

2.10 Office of the Chief Procurement Officer (OCPO)

OCPO ensures that HUD contracts, for IT systems and services include appropriate information security requirements. OCPO, in concert with OITS, other interested stakeholders (e.g., program office sponsoring the acquisition) and as appropriate, legal counsel within the Office of General Counsel, develops IT Security contract clauses, and other contract terms and conditions, as appropriate, based on current policies, regulations, and guidance for HUD information systems and services.

2.11 Contracting Officer

The contracting Officer (CO) has the authority to enter into, administer, and terminate contracts.

2.12 Office of Human Resources

The Office of Human Resources (OHR) is responsible for defining position sensitivity levels for government positions and risk levels for contractor positions, for performing security background investigations when necessary and for providing security-related exit procedures when employees leave HUD.

2.13 Office of the Inspector General

The Office of the Inspector General (OIG) is responsible for performing independent evaluations of internal and external security.

2.14 HUD General Counsel

HUD General Counsel develops security clauses, as appropriate, based on current policies, regulations, and guidance for HUD information systems and services in conjunction with OITS and OCPO.

2.15 Investment Review Board

The Investment Review Board is responsible for planning and for managing the capital planning and investment control process for HUD.

2.16 Configuration Control Board

The Configuration Control Board (CCB) serves as the decision-making body for system changes, approving information system changes in accordance with HUD policies and procedures.

2.17 Program Office/System Owner

Program Offices or System Owners are dependent on information systems to fulfill the business requirements necessary to achieve their program area's mission. They are responsible for the successful operation of those systems and ultimately accountable for the security of their information systems. They are also responsible for executing crucial steps to achieve management and operational controls and to ensure that the appropriate technical controls are effective in protecting the information and information systems under their purview. The Program Offices and System Owners are responsible for ensuring that certification and accreditation activities are completed and the Plan of Action & Milestones (POA&M) are maintained and reported.

2.18 Information System Security Officer

The Information System Security Officer (ISSO) is responsible for ensuring that the management, operational, and technical controls for securing the system(s) belonging to the program office are in place and effective. They are the principal points of contact for information systems security. They are responsible for all security aspects of their assigned systems from inception until disposal, as well as for ensuring system availability.

2.19 System Administrator

The system administrator is responsible for implementing and maintaining technical controls that enforce operational and managerial controls through mechanisms contained in the hardware, software, or firmware components of the information system. The security components they support may span across multiple systems and security controls. They must maintain an environment that creates a strong technical foundation for enforcement of information system security.

2.20 Certification Agent

The Certification Agent provides an impartial and unbiased assessment of HUD systems independently from the individuals directly responsible for information systems development and day-to-day system operations. The Certification Agent assesses all security documentation for the system, validates that the security requirements are implemented effectively, and documents the results in a Security Assessment Report.

2.21 Authorizing Official

The Authorizing Official is a senior government management official with the authority to formally assume responsibility for operating an information system at an acceptable level of risk. Authorizing Officials control personnel, operations, maintenance, and budgets for their systems or field sites; therefore, controlling the resources necessary to mitigate risks to their information systems. An Authorizing Official must be a Program Assistant Secretary, Deputy Assistant Secretary, or equivalent Program Head. Authorizing Officials may designate a representative to act on their behalf and they may be empowered to make certain decisions regarding the planning and resources for security activities, acceptability of SDM and certification and accreditation documentation, and the determination of risk to agency operations, agency assets, and individuals. The Authorizing Official cannot delegate the security accreditation decision and signing of the associated accreditation decision letter.

2.22 Supervisor

Supervisors authorize issuance of information system access for their staff and are directly responsible for notifying System Owners when staff members are terminated, transferred, or no longer need access to a system.

2.23 Users

Users is a broad term used for all personnel that interact with HUD information system resources either in a support function, by working directly with an information system resource (i.e., system user), or as a recipient of HUD information (i.e., information user). For the purposes of this document, users include all HUD employees and contractors, including vendors and agents, who provide services and resources to HUD. Users must understand and comply with HUD information security policies, standards, and procedures regarding the protection of HUD information system assets.

2.24 Individuals with Key Contingency Roles

Individuals with key contingency roles, as defined in systems' contingency plans, must receive training and be prepared to perform the required functions as defined in those plans.

2.25 Service Provider

Service providers include vendors, contractors and entities that provide IT services, information systems, and facilities housing HUD information systems. Service providers are responsible for maintaining security controls that are compliant with HUD security policy and procedures.

2.26 Developers

Developers, under HUD Program Office/System Owner direction and specifications, are responsible for developing, maintaining, and implementing information systems that are in compliance with HUD security policies and procedures, NIST guidance, and federal regulations.

3.0 Management Procedures

Management controls are the security controls (i.e., safeguards or countermeasures) for an information system that focus on the management of risk and the management of information system security. The procedures in this section provide guidance on how to implement management controls and HUD security requirements.

3.1 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 information systems and data that support their organization’s missions.

The following procedures ensure that there are mechanisms in place to address the identification, assessment, and mitigation of risks to information assets.

FIPS 200 Requirement
Organizations must periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational information systems and the associated processing, storage, or transmission of organizational information.

3.1.1 Risk Assessment Policy and Procedures

NIST SP 800-53 Control: RA-1
RA-1: The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented risk assessment policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the risk assessment policy and associated risk assessment controls.
Security Baseline: Low, Moderate, and High
Related HUD Policy: <i>Information Technology Security Policy, Handbook 2400.25, Rev. 1</i>
Implementation
This control is implemented by the <i>Information Technology Security Policy, Handbook 2400.25, Rev. 1</i> , which defines HUD’s security policies. The procedures related to the HUD policies are in this document, <i>HUD Information Technology Security Procedures</i> .

3.1.2 Security Categorization

NIST SP 800-53 Control: RA-2
<p>RA-2: The organization categorizes the information system and the information processed, stored, or transmitted by the system in accordance with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance and documents the results (including supporting rationale) in the system security plan. Designated senior-level officials within the organization review and approve the security categorizations.</p>
<p>Security Baseline: Low, Moderate, and High</p>
<p>Related HUD Policy: 3.1.2</p>
Supporting Procedures
<ol style="list-style-type: none"> 1. Identify the types of information contained in each HUD information system, including systems operated and maintained by third-party service providers, using the guidance in NIST SP 800-60, <i>Guide for Mapping Types of Information and Information Systems to Security Categories</i>. (Program Office/System Owner, ISSO) 2. Categorize the information as Low, Moderate, or High based on the guidance in NIST SP 800-60. (Program Office/System Owner, ISSO) 3. Determine the high-water mark for the system based on the categorization for confidentiality, integrity, and availability. (Program Office/System Owner, ISSO) 4. Submit the categorization to OITS for review and approval. (Program Office/System Owner) 5. Evaluate the categorization and approve or provide guidance to the submitting organization on how to correct the categorization. The CISO is responsible for approving the categorization for each HUD system. (CISO) 6. Enter the system categorization into the Inventory of Automated Systems (IAS). (Program Office/System Owner, ISSO) 7. Incorporate the system categorization into the security plan. (Project Office/System Owner, ISSO)

3.1.3 Risk Assessment

NIST SP 800-53 Control RA-3
<p>RA-3: The organization conducts assessments of the risk and magnitude of harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems that support the operations and assets of the agency (including information and information systems managed/operated by external parties).</p>
<p>Security Baseline: Low, Moderate, and High</p>
<p>Related HUD Policy: 3.1.3</p>

NIST SP 800-53 Control RA-3
Supporting Procedures
<ol style="list-style-type: none"> 1. Assess the risk on HUD systems at least every three years or when a significant change is planned and as defined in the HUD SDM. (Program Office/System Owner, ISSO) 2. Conduct and document the risk assessment following the guidance in NIST SP 800-30, <i>Risk Management Guide for Information Technology Systems</i> and the tools provided by GSA. (Program Office/System Owner, ISSO) 3. Document the risk assessment following the guidance in NIST SP 800-30 and the HUD risk assessment templates. Use the <i>Information Technology Security Risk Assessment Evaluation Checklist</i> to ensure it is complete. (Program Office/System Owner, ISSO) 4. Update the security plan with the results of the risk assessment. (Program Office/System Owner, ISSO) 5. Complete the risk assessment in accordance to the guidance in the HUD SDM. (Program Office/System Owner, ISSO) 6. Submit the risk assessment with the certification and accreditation documentation. (Program Office/System Owner) 7. Review and approve the risk assessment as part of the certification and accreditation process. (Certification Agent, Authorizing Official)

3.1.4 Risk Assessment Update

NIST SP 800-53 Control: RA-4
<p>RA-4: The organization updates the risk assessment at least every three years or whenever there are significant changes to the information system, the facilities where the system resides, or other conditions that may impact the security or accreditation status of the system.</p>
<p>Security Baseline: Low, Moderate, and High</p>
<p>Related HUD Policy: 3.1.4</p>
Supporting Procedures
<ol style="list-style-type: none"> 1. Update the risk assessment at least every three years or when a significant change is planned for the system following the guidance in NIST SP 800-30, <i>Risk Management Guide for Information Technology Systems</i>, and the HUD <i>Information Technology Security Risk Assessment Evaluation Checklist</i>. (Program Office/System Owner, ISSO) 2. Review and approve the risk assessment update as part of the certification and accreditation process if the risk assessment update is done in conjunction with a system reaccreditation. (Certification Agent, Authorizing Official)

3.1.5 Vulnerability Scanning

NIST SP 800-53 Control: RA-5
<p>RA-5: The organization scans for vulnerabilities in the information system monthly or when significant new vulnerabilities affecting the system are identified and reported.</p>
<p>Security Baseline: Moderate and High</p>

NIST SP 800-53 Control: RA-5
<p>E-1: The organization employs vulnerability scanning tools that include the capability to readily update the list of vulnerabilities scanned.</p> <p>Security Baseline: High</p>
<p>E-2: The organization updates the list of information system vulnerabilities every six months or when significant new vulnerabilities are identified and reported.</p> <p>Security Baseline: High</p>
<p>E-3: The organization employs vulnerability scanning procedures that can demonstrate the breadth and depth of scan coverage, including vulnerabilities checked and information system components scanned.</p> <p>Security Baseline: N/A</p>
<p>Related HUD Policy: 3.1.5</p>
Supporting Procedures
<ol style="list-style-type: none"> 1. Select HUD approved tools and techniques to scan for vulnerabilities in the information system. (OITS) 2. Train HUD personnel on how to appropriately use the vulnerability scanning tools and techniques and maintain the training as scanning tools and techniques change. (OITS) 3. Scan the HUD systems at least monthly, weekly for high-impact systems, or when significant new vulnerabilities are identified. NIST SP 800-42, <i>Guideline on Network Security Testing</i>, provides helpful guidance. (ISSO, System Administrator) 4. Share the vulnerability scanning results with others in the organization to ensure that all HUD systems are adequately protected. (CSIRC, Program Office/System Owner, ISSO) 5. Patch or reconfigure systems, as required, based on the results of the vulnerability scans and the guidance in the system configuration management plan. NIST 800-40, <i>Procedures for Handling Security Patches</i>, also provides helpful guidance. (ISSO, System Administrator) 6. Update the POA&M with the results of the vulnerability scanning. (Program Office/Systems Owner, ISSO)

3.1.6 E-Authentication Risk Assessment

HUD Policy: HUD RA-1
<p>HUD Policy: 3.1.6</p> <ol style="list-style-type: none"> a. Program Offices/System Owners shall conduct an e-authentication risk assessment (E-RA) of the transactional systems under their purview that use the Internet and/or the Intranet. The risk assessment shall be conducted in accordance with OMB guidance under OMB-04-04, <i>E-Authentication Guidance for Federal Agencies</i> and E-Authentication Program Management Office guidance, <i>E-Authentication e-RA Tool Activity Guide and HUD specific guidance (see HUD IT security website)</i>. b. Program Offices/System Owners shall submit the E-RA to the CISO for review and concurrence. c. Subsequent to the concurrence by the CISO, the authorizing official (same as the approving official for accreditation) for each organization shall give their written approval of the E-RA. d. Following E-RA approval, Program Offices/System Owners shall select the technology appropriate for the assurance level that's been identified in the E-RA using NIST 800-63, <i>Electronic Authentication Guideline</i>, version 1.0.2 and implement and test the controls. e. Update the E-RA whenever there are significant changes to the information system, the facilities

HUD Policy: HUD RA-1
<p>where the system resides, or other conditions that may impact the authentication requirements of the system if necessary.</p>
<p>Security Baseline: Low, Moderate, and High</p>
Supporting Procedures
<ol style="list-style-type: none"> 1. Identify all HUD transactional systems that operate over the Internet and/or Intranet that require authentication. (Program Office/System Owner, ISSO, Application Support Personnel) 2. Conduct and document the E-RA following the HUD specific guidance (<i>see HUD IT security website</i>). (Program Office/System Owner, ISSO, Application Support Personnel.) 3. Submit the E-RA to the CISO for review and concurrence. (Program Office/System Owner) 4. Review and approve or deny the e-authentication risk assessment. (OITS, CISO) 5. Subsequent to the concurrence by the CISO, the authorizing official (same as the approving official for accreditation) for each organization shall give their written approval of the E-RA. (Authorizing Official) 6. Following E-RA approval, use NIST 800-63, Electronic Authentication Guideline, version 1.0.2, to select the technology appropriate for assurance level identified in the E-RA and implement it. (Program Office/System Owner, ISSO, Application Support Personnel) 7. After authentication controls have been implemented, validate that the implemented system authentication has achieved the required assurance level. (Program Office/System Owner, ISSO) 8. Update the E-RA whenever there are significant changes to the information system, the facilities where the system resides, or other conditions that may impact the authentication requirements of the system if necessary. (Program Office/System Owner, ISSO, Application Support Personnel)

3.2 Planning

Security planning controls are designed to ensure that each organization plans for security to support their business activities and develops, implements and maintains security plans for its information systems.

The following procedures ensure that there are mechanisms in place to address planning for the protection of information assets to include policies, procedures and rules of behavior.

FIPS 200 Requirement
<p>Organizations must develop, document, periodically update, and implement security plans for organizational information systems that describe the security controls in place or planned for the information systems and the rules of behavior for individuals accessing the information systems.</p>

3.2.1 Security Planning Policy and Procedures

NIST SP 800-53 Control: PL-1
<p>PL-1: The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, security planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the security planning policy and associated security planning controls.</p> <p>Security Baseline: Low, Moderate, and High</p> <p>Related HUD Policy: <i>Information Technology Security Policy, Handbook 2400.25, Rev. 1</i></p>
Implementation
<p>This control is implemented by the <i>Information Technology Security Policy, Handbook 2400.25, Rev. 1</i>, which defines HUD’s security policies. The procedures related to the HUD policies are in this document, <i>HUD Information Technology Security Procedures</i>.</p>

3.2.2 System Security Plan

NIST SP 800-53 Control: PL-2
<p>PL-2: The organization develops and implements a security plan for the information system that provides an overview of the security requirements for the system and a description of the security controls in place or planned for meeting those requirements. Designated officials within the organization review and approve the plan.</p> <p>Security Baseline: Low, Moderate, and High</p> <p>Related HUD Policy: 3.2.2</p>
Supporting Procedures
<ol style="list-style-type: none"> 1. Prepare a security plan for each HUD information system following the guidance in NIST SP 800-18, Rev. 1, <i>Guide for Developing Security Plans for Information Technology Systems</i> and HUD <i>Certification and Accreditation Methodology</i>. Use the <i>HUD Information Technology Security Plan Evaluation Checklist</i> to ensure it is complete. (Program Office/System Owner, ISSO) 2. Complete and approve the security plan in writing prior to starting the certification and accreditation process. (Program Office/System Owner, ISSO) 3. Submit the security plan to the Certification Agent for assessment as part of the certification process. (Program Office/System Owner, ISSO) 4. Review the security plan during the certification process. (Certification Agent) 5. Approve the security plan during the accreditation process. (Authorizing Official)

3.2.3 System Security Plan Update

NIST SP 800-53 Control: PL-3
<p>PL-3: The organization reviews the security plan for the information system annually and revises the plan to address system/organizational changes or problems identified during plan implementation or security control assessments.</p> <p>Security Baseline: Low, Moderate, and High</p>

NIST SP 800-53 Control: PL-3
Related HUD Policy: 3.2.3
Supporting Procedures
<ol style="list-style-type: none"> 1. Update the security plan annually, when a significant change is planned for the system, or vulnerability has been identified. (Program Office/System Owner, ISSO) 2. Review and approve the security plan update as part of the certification process if the security plan update is done in conjunction with a system reaccreditation. (Certification Agent, Authorizing Official)

3.2.4 Rules of Behavior

NIST SP 800-53 Control: PL-4
<p>PL-4: The organization establishes and makes readily available to all information system users a set of rules that describes their responsibilities and expected behavior with regard to information and information system usage. The organization receives signed acknowledgement from users indicating that they have read, understand, and agree to abide by the rules of behavior prior to authorizing access to the information systems and its resident information.</p>
Security Baseline: Low, Moderate, and High
Related HUD Policy: 3.2.4
Supporting Procedures
<ol style="list-style-type: none"> 1. Develop rules of behavior applicable to all HUD systems. (OITS, CISO) 2. Determine if HUD enterprise rules of behavior are sufficient for the system, if not update as necessary with rules of behavior applicable to the information system. (Program Office/System Owner, ISSO) 3. Distribute rules of behavior to each system user and provide training on the consequences that may result if the rules of behavior are violated. (ISSO) 4. Sign the rules of behavior and return them to the appropriate ISSO. (Users) 5. Maintain copies of the signed rules of behavior. (ISSO)

3.2.5 Privacy Impact Assessments

NIST SP 800-53 Control: PL-5
<p>PL-5: The organization conducts a privacy impact assessment on the information system in accordance with OMB policy.</p>
Security Baseline: Low, Moderate, and High
Related HUD Policy: 3.2.5

NIST SP 800-53 Control: PL-5
Supporting Procedures
<ol style="list-style-type: none"> 1. Evaluate each HUD information system to determine if they contain personally identifiable information following guidance in OMB Memorandum 03-22. (Program Office/System Owner, ISSO) 2. Prepare a privacy impact assessment (PIA) for all systems that contain personally identifiable information following the guidance in OMB Memorandum 03-22. (Program Office/System Owner, ISSO) 3. Submit the PIA to the HUD Privacy Officer. (Program Office/System Owner, ISSO) 4. Review and approve the PIA. (HUD Privacy Officer)

3.2.6 Security-Related Activity Planning

NIST SP 800-53 Control: PL-6
<p>PL-6: The organization plans and coordinates security-related activities affecting the information system before conducting such activities in order to reduce the impact on organizational operations (i.e., mission, function, image, and reputation) organizational assets, and individuals.</p>
<p>Security Baseline: Moderate and High</p>
<p>Related HUD Policy: 3.2.6</p>
Supporting Procedures
<ol style="list-style-type: none"> 1. Plan and coordinate security-related activities (e.g., security assessments, audits, system hardware and software maintenance, security certification, and testing/exercises) to minimize impact on organizational operations and assets and individuals. (Program Office/System Owner, ISSO, System Administrators) 2. Coordinate all changes with the Configuration Control Board. (Program Office/System Owner, ISSO, System Administrators).

3.2.7 HUD Inventory

HUD Policy: HUD PL-1
<p>HUD Policy: 3.2.7</p> <p>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 semi-annually.</p>
<p>Security Baseline: Low, Moderate, and High</p>
Supporting Procedures
<ol style="list-style-type: none"> 1. Enter and update, semi-annually or when major changes occur, required information on each HUD application, including HUD systems operated by third-party providers in IAS at hudatwork.hud.gov/po/i/it/wklines/ias.cfm. (Program Office/System Owner, ISSO) 2. Validate the information annually in IAS to ensure it is accurate and up-to-date. (Systems Engineering, Oversight & Performance Management Division [SEO&PMD], OITS)

3.2.8 ISSO

HUD Policy: HUD PL-2
<p>HUD Policy: 3.2.8 Program Offices shall designate an ISSO as well as an alternate ISSO for every HUD information system under their purview.</p> <p>Security Baseline: Low, Moderate, and High</p>
Supporting Procedures
<ol style="list-style-type: none"> 1. Appoint an ISSO as well as an alternate ISSO for each HUD information system and submit the official appointment letter to the authorizing official and the CISO. (Program Office/System Owner) 2. Update the ISSO information in the security plan. (Program Office/System Owner)

3.3 System and Services Acquisition

System and services acquisition controls ensure that appropriate technical, administrative, physical, and personnel security requirements will be included in all specifications for the acquisition, operation or maintenance of HUD facilities, equipment, software, and related services or those operated by external providers of information system services on behalf of HUD.

The following procedures ensure that there are mechanisms in place for all acquisitions efforts.

FIPS 200 Requirement
<p>Organizations must: (i) allocate sufficient resources to adequately protect organizational information systems; (ii) employ system development life cycle processes that incorporate information security considerations; (iii) employ software usage and installation restrictions; and (iv) ensure that third-party providers employ adequate security measures to protect outsourced organizational information, applications, and/or services.</p>

3.3.1 System and Services Acquisition Policy and Procedures

NIST SP 800-53 Control: SA-1
<p>SA-1: The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, system and services acquisition policy that includes information security considerations and that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the system and services acquisition policy and associated system and services acquisition controls.</p> <p>Security Baseline: Low, Moderate, and High</p>
<p>Related HUD Policy: <i>Information Technology Security Policy, Handbook 2400.25, Rev. 1, HUD Acquisition Regulation, HUD System Development Methodology</i></p>

NIST SP 800-53 Control: SA-1
Implementation
This control is implemented by the <i>Information Technology Security Policy, Handbook 2400.25, Rev. 1</i> , which defines HUD’s security policies. The procedures related to the HUD policies are in this document, <i>HUD Information Technology Security Procedures</i> . Additional policies and procedures to be used as guidance for system and services acquisition can be found in the <i>HUD Acquisition Regulation</i> and the <i>HUD System Development Methodology</i> .

3.3.2 Allocation of Resources

NIST SP 800-53 Control: SA-2
SA-2: The organization determines, documents, and allocates as part of its capital planning and investment control process, the resources required to adequately protect the information system.
Security Baseline: Low, Moderate, and High
Related HUD Policy: 3.3.2
Supporting Procedures
<ol style="list-style-type: none"> 1. Determine and document security requirements for the information system in mission/business case planning, following guidance in HUD <i>CPIC Guidance</i> and NIST SP 800-65, <i>Integrating Security into the Capital Planning and Investment Control Process</i>. Requirements must be in compliance with HUD’s Enterprise Architecture requirements and the HUD security policy, <i>Information Technology Security Policy Handbook 2400.25, Rev. 1</i>. (Program Office/System Owner) 2. Calculate all security costs associated with the system life cycle as outlined in the <i>HUD System Development Methodology</i> and incorporate them in the capital planning and investment control process. (Program Office/System Owner) 3. Establish a discrete line item for information system security in the organization’s program and budget documentation (e.g., OMB Exhibit 300). (Program Office/System Owner) 4. Evaluate the information system security costs and certify that adequate security funding is included in the mission/business case throughout the system life cycle. (OITS, Investment Review Board)

3.3.3 Life Cycle Support

NIST SP 800-53 Control: SA-3
SA-3: The organization manages the information system using a system development life cycle methodology that includes information security considerations.
Security Baseline: Low, Moderate, and High
Related HUD Policy: 3.3.3
Supporting Procedures
<ol style="list-style-type: none"> 1. Validate that security activities take place as defined in the <i>HUD System Development Methodology</i> and in NIST SP 800-64, <i>Security Considerations in the Information System Development Life Cycle</i>. (Program Office/System Owner, ISSO, OCIO)

3.3.4 Acquisitions

NIST SP 800-53 Control: SA-4
<p>SA-4: The organization includes security requirements and/or security specifications, either explicitly or by reference, in information system acquisition contracts based on an assessment of risk and in accordance with applicable laws, Executive Orders, directives, policies, regulations, and standards.</p> <p>Security Baseline: Low, Moderate, and High</p>
<p>E-1: The organization requires in solicitation document that appropriate documentation be provided describing the functional properties of the security controls employed within the information system with sufficient detail to permit analysis and testing of the controls.</p> <p>Security Baseline: Moderate and High</p>
<p>E-2: The organization requires in solicitation documents that appropriate documentation be provided describing 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).</p> <p>Security Baseline: N/A</p>
<p>Related HUD Policy: 3.3.4</p>
Supporting Procedures
<ol style="list-style-type: none"> 1. Include, either explicitly or by reference, security requirements in solicitation documents (e.g., Requests for Proposal) that describe required security capabilities, required design and development processes, required test and evaluation procedures, and required documentation. (Program Office/System Owner, OCPO) 2. Include a request for documentation describing functional properties of the security controls for moderate- and high-impact systems. 3. Include a request for documentation describing the design and implementation details of the security controls for high-impact systems. 4. Require all contractors to adhere to the HUD security policy, <i>Information Technology Security Policy Handbook 2400.25, Rev. 1</i>, the HUD enterprise architecture, and the security controls in NIST 800-53, <i>Recommended Security Controls for Federal Information Systems</i>, including annual updates. (Program Office/System Owner, OCPO) 5. Require contract vehicles to include handling of sensitive information, information storage, processing, or transmitting using the contractor's computer systems, background investigations, clearances, and facility security. (Program Office/System Owner, OCPO) 6. Require contract vehicles to include a requirement to submit the names of contractor personnel assigned to the task and update the information when contractor personnel are reassigned or terminated. (Program Office/System Owner, OCPO) 7. Track contractor personnel assigned to the contract that have met all personnel requirements and are authorized to work on the HUD systems and programs throughout the life of the contract. (Program Office/System Owner, Government Technical Monitor [GTM]) 8. Require contractors to return all information and resources provided during the life of the contract and certify that all HUD information has been purged from any contractor-owned systems used to process HUD information. (Program Office/System Owner, OCPO)

3.3.5 Information System Documentation

NIST SP 800-53 Control: SA-5
<p>SA-5: The organization obtains, protects as required, and makes available to authorized personnel, adequate documentation for the information system.</p> <p>Security Baseline: Low, Moderate, and High</p>
<p>E-1: The organization includes documentation, if available from the vendor/manufacturer, describing the functional properties of the security controls employed within the information system with sufficient detail to permit analysis and testing of the controls.</p> <p>Security Baseline: Moderate and High</p>
<p>E-2: The organization includes documentation, if available from the vendor/manufacturer, describing 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).</p> <p>Security Baseline: High</p>
<p>Related HUD Policy: 3.3.5</p>
Supporting Procedures
<ol style="list-style-type: none"> 1. Ensure that adequate documentation for the information system and its constituent components is available and distributed to authorized personnel. Documentation includes, but is not limited to: security plans, contingency plans, documentation as required by the HUD SDM, certification and accreditation documentation, vendor-supplied documentation of purchased software and hardware, network diagrams, application documentation for in-house applications, system build and configuration documentation with optimization of system security settings, administrator and user manuals, and standard operating procedures. (Program Office/System Owner) 2. Label and protect all documentation as required. (Users, ISSO) 3. Require documentation, if available from the vendor/manufacturer, describing the functional properties of the security controls employed within moderate-or high-impact information systems have sufficient detail to permit analysis and testing of the controls. High impact systems should have sufficient detail to permit testing of the functional interfaces among control components. (Program Office/System Owner)

3.3.6 Software Usage Restrictions

NIST SP 800-53 Control: SA-6
<p>SA-6: The organization complies with software usage restrictions.</p> <p>Security Baseline: Low, Moderate, and High</p>
<p>Related HUD Policy: 3.3.6</p>

NIST SP 800-53 Control: SA-6
Supporting Procedures
<ol style="list-style-type: none"> 1. Use software and associated documentation in accordance with contract agreements and copyright laws. (Users) 2. Implement tracking systems to control copying and distribution of software and documentation protected by quantity licenses. (Program Office/System Owner) 3. Restrict the use of publicly accessible peer-to-peer file sharing technology to ensure that this capability is not used for the unauthorized distribution, display, performance, or reproduction of copyrighted work. (Program Office/System Owner)

3.3.7 User Installed Software

NIST SP 800-53 Control: SA-7
SA-7: The organization enforces explicit rules governing the installation of software by users.
Security Baseline: Low, Moderate, and High
Related HUD Policy: 3.3.7
Supporting Procedures
<ol style="list-style-type: none"> 1. Determine and document personnel who are authorized to download and install software on HUD systems. (Program Office/System Owner) 2. Identify and document the types of software downloads and installations that are permitted (e.g., updates and security patches to existing software) and what types of downloads and installations are prohibited (e.g., software that is free only for personal, not government, use) and restrict the use of install-on-demand software. (OITS, Program Office/System Owner) 3. Install non-standard software on HUD-owned or leased equipment only after obtaining written approval from the CISO. (Program Office/System Owner, CISO)

3.3.8 Security Engineering Principles

NIST SP 800-53 Control: SA-8
SA-8: The organization designs and implements the information system using security engineering principles.
Security Baseline: Moderate and High
Related HUD Policy: 3.3.8
Supporting Procedures
<ol style="list-style-type: none"> 1. Design and implement moderate-and high-impact systems using security engineering principles as defined in NIST SP 800-27, <i>Engineering Principles for Information Technology Security</i>, and the <i>HUD System Development Methodology</i>. (Program Office/System Owner, Developers, ISSO) 2. Develop and implement information systems in accordance with the HUD enterprise architecture. (Program Office/System Owner, Developers)

3.3.9 Outsourced Information System Services

NIST SP 800-53 Control: SA-9
SA-9: The organization: (i) requires that providers of external information system services employ adequate security controls in accordance with applicable laws, Executive Orders, directives, policies, regulations, standards, guidance, and established service-level agreements; and (ii) monitors security control compliance.
Security Baseline: Low, Moderate, and High
Related HUD Policy: 3.3.9
Supporting Procedures
<ol style="list-style-type: none"> 1. Submit all contracts for external information systems provided by third-party providers (e.g., commercial telecommunications services, network services, manned security services, or application services) to the CISO. (Program Office/System Owner, OCPO, CO) 2. Validate that the contract conforms to HUD's security policies and procedures, security controls, documentation and required chain of trust requirements. The CISO will also approve or deny the planned contract. (CISO) 3. Include the expectations of performance for each required security control, describing measurable outcomes, and identifying remedies and response requirements for any identified instance of non-compliance in contracts and service level agreements. NIST 800-35, <i>Guide to Information Technology Security Services</i>, provides guidance on security services. (OCPO, CO) 4. Conduct independent annual reviews in accordance with NIST standards and guidance to ensure that HUD security requirements are implemented and enforced. (Program Office/System Owner, ISSO, OCPO, CO, GTM)

3.3.10 Developer Configuration Management

NIST SP 800-53 Control: SA-10
SA-10: The organization requires that information system developers create and implement 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.
Security Baseline: High
Related HUD Policy: 3.3.10
Supporting Procedures
<ol style="list-style-type: none"> 1. Prepare a configuration management plan following the guidance in the HUD <i>System Development Methodology</i> to address the methods for controlling change during development and tracking security flaws for all high-impact systems. (Program Office/System Owner, ISSO) 2. Track and address all security flaws during development of high-impact systems. (Program Office/System Owner, ISSO, Developer) 3. Authorize changes to systems during development of high-impact systems. (Program Office/System Owner)

3.3.11 Developer Security Testing

NIST SP 800-53 Control: SA-11
SA-11: The organization requires that information system developers create a security test and evaluation plan, implement the plan, and document the results.
Security Baseline: Moderate and High
Related HUD Policy: 3.3.11
Supporting Procedures
<ol style="list-style-type: none"> 1. Create a security assessment plan for all information systems during development following the guidance in the HUD <i>Security Assessment Guidelines</i> and NIST SP 800-53A, <i>Guide for Assessing the Security Control in Federal Information Systems</i>, for all moderate- or high-impact systems. (Program Office/System Owner, ISSO) 2. Implement the plan and review the security based on the plan and document the results of the security assessment. Take corrective actions. (Program Office/System Owner, ISSO) 3. Use the results of the developmental security assessments for the certification and accreditation of the system only when there have been no subsequent changes to the security since the developer tested security and the developer test results have been verified. (Program Office/System Owner, ISSO, Certification Agent)

3.4 Certification, Accreditation, and Security Assessments

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.

The following procedures ensure that there are mechanisms in place to validate that every information system connected to the network has met at least a minimal set of security requirements for configuration and access.

FIPS 200 Requirement
Organizations must: (i) periodically assess the security controls in organizational information systems to determine if the controls are effective in their application; (ii) develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational information systems; (iii) authorize the operation of organizational information systems and any associated information system connections; and (iv) monitor information system security controls on an ongoing basis to ensure the continued effectiveness of the controls.

3.4.1 Certification, Accreditation, and Security Assessment Policy and Procedures

NIST SP 800-53 Control: CA-1
<p>CA-1: The organization develops, disseminates, and periodically reviews/updates: (i) formal, documented, security assessment and certification and accreditation policies that address purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the security assessment and certification and accreditation policies and associated assessment, certification, and accreditation controls.</p>
<p>Security Baseline: Low, Moderate and High</p>
<p>Related HUD Policy: <i>Information Technology Security Policy, Handbook 2400.25, Rev. 1</i></p>
Implementation
<p>This control is implemented by the <i>Information Technology Security Policy, Handbook 2400.25, Rev. 1</i>, which defines HUD's security policies. The procedures related to the HUD policies are in this document, <i>HUD Information Technology Security Procedures</i>, and the <i>HUD Certification and Accreditation Methodology: A Best Practices Guide for Information Security</i>.</p>

3.4.2 Security Assessment

NIST SP 800-53 Control: CA-2
<p>CA-2: The organization conducts an assessment of the security controls in the information system annually to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.</p>
<p>Security Baseline: Low, Moderate, and High</p>
<p>Related HUD Policy: 3.4.2</p>
Supporting Procedures
<ol style="list-style-type: none"> 1. Conduct and document a security assessment of each HUD information system following the guidance in NIST SP 800-53, <i>Recommended Security Controls for Federal Information Systems</i>, NIST SP 800-53A, <i>Guide for Assessing the Security Controls in Federal Information Systems</i>, and <i>HUD Security Assessment Guidelines</i>. (Program Office/System Owner, ISSO) 2. Develop a POA&M for all vulnerabilities found during the assessment, incorporating any additional vulnerabilities found during other assessment or review processes. (Program Office/System Owner, ISSO) 3. Submit the assessment reports and POA&M as specified in the <i>HUD IT Security Plans of Action and Milestones Process Guide</i>. (Program Office/System Owner, ISSO) 4. Update POA&Ms quarterly and submit them to OITS. (Program Office/System Owner)

3.4.3 Information System Connections

NIST SP 800-53 Control: CA-3
<p>CA-3: The organization authorizes all connections from the information system to other information systems outside of the accreditation boundary through the use of system connection agreements and monitors/controls the system interconnection on an ongoing basis.</p>
<p>Security Baseline: Low, Moderate, and High</p>
<p>Related HUD Policy: 3.4.3</p>
Supporting Procedures
<ol style="list-style-type: none"> 1. Define the need to connect to other systems outside the accreditation boundary. (Program Office/System Owner, ISSO) 2. Obtain the certification and accreditation documentation for the connecting system from the organization and provide them with certification and accreditation documentation on your system. (ISSO) 3. Analyze the certification and accreditation documentation to determine if the risk is acceptable for connection or if additional controls, in either system, need to be implemented prior to connection. (Program Office/System Owner, ISSO) 4. Document the interconnection agreement through an MOA/U for the business requirements and an Interconnection System Agreement for the technical and security requirements following the guidance in NIST SP 800-47, <i>Security Guide for Interconnection Information Technology Systems</i>. (Program Office/System Owner, ISSO)

3.4.4 Security Certification

NIST SP 800-53 Control: CA-4
<p>CA-4: The organization conducts an assessment of the security controls in the information system to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.</p>
<p>Security Baseline: Low, Moderate, and High</p>
<p>E-1: The organization employs an independent certification agent or certification team to conduct an assessment of the security controls in the information system.</p>
<p>Security Baseline: Moderate and High</p>
<p>Related HUD Policy: 3.4.4</p>

NIST SP 800-53 Control: CA-4
Supporting Procedures
<ol style="list-style-type: none"> 1. Conduct the security certification for each information system following the guidance in NIST SP 800-37, <i>Guide for the Security Certification and Accreditation of Federal Information Systems</i>, and the HUD <i>Certification and Accreditation Methodology</i>. (Program Office/System Owner, Certification Agent) 2. Ensure that individuals conducting the certification activities for all moderate- and high-impact systems are organizationally independent from those who designed and developed the system, who operate the system on a daily basis, who prepared the security documentation, and who are responsible for correcting deficiencies in the system. (Program Office/System Owner) 3. Assess the security controls following the guidance in NIST SP 800-53A, <i>Guide for Assessing the Security Controls in Federal Information Systems</i> and the HUD <i>Security Assessment Guidelines</i>. (Certification Agent) 4. Correct deficiencies identifying during the security assessment and retest to validate the security controls have been adequately implemented. (Program Office/System Owner, Certification Agent) 5. Update the security documentation (e.g., security plan). (Program Office/System Owner, ISSO) 6. Document the security assessment report and develop the POA&Ms. (Program Office/System Owner, ISSO) 7. Prepare the accreditation package with the documents required in NIST 800-37 and the HUD <i>Certification and Accreditation Methodology</i>. (Program Office/System Owner, ISSO) 8. Submit the accreditation package to the authorizing official for review and approval. (Program Office/System Owner)

3.4.5 Plan of Action and Milestones

NIST SP 800-53 Control: CA-5
<p>CA-5: The organization develops and updates quarterly, a plan of action and milestones for the information system that documents the organization’s planned, implemented, and evaluated remedial actions to correct deficiencies noted during the assessment of the security controls and to reduce or eliminate known vulnerabilities to the system.</p>
<p>Security Baseline: Low, Moderate, and High</p>
<p>Related HUD Policy: 3.4.5</p>
Supporting Procedures
<ol style="list-style-type: none"> 1. Compile the findings from security assessments, continuous monitoring activities, and any additional HUD assessments in a POA&M. (Program Office/System Owner, ISSO) 2. Prepare the POA&M following the annual HUD FISMA reporting guidance and the HUD <i>IT Security Plans of Action and Milestones Process Guide</i>. (Program Office/System Owner, ISSO) 3. Submit the POA&M to OITS as required for HUD FISMA reporting and as part of the accreditation package. (Program Office/System Owner, ISSO) 4. Evaluate and update the POA&M quarterly and monitor progress to improve the security status of all systems under their purview. (Program Office/System Owner, OITS) 5. Submit the HUD POA&M to OMB, as required. (OITS)

3.4.6 Security Accreditation

NIST SP 800-53 Control: CA-6
<p>CA-6: The organization authorizes (i.e., accredits) the information system for processing before operations and updates the authorization every three years or when there is a significant change to the system. A senior organizational official signs and approves the security accreditation.</p>
<p>Security Baseline: Low, Moderate, and High</p>
<p>Related HUD Policy: 3.4.6</p>
Supporting Procedures
<ol style="list-style-type: none"> 1. Review the accreditation package provided by the Program Office/System Owner. (Authorizing Official) 2. Evaluate the certification results to determine the risk to HUD's mission if the system becomes or remains operational. (Authorizing Official) 3. Make and document an accreditation decision based on the assessed risk of the information system to HUD's mission. The accrediting official can decide to accredit the system, deny accreditation, and not allow the system to be operational, or grant an interim accreditation allowing the system to operate for a limited time while the security posture of the system is improved to an acceptable level. Existing accreditation decisions made prior to the issue of HUD policies shall remain in effect if no significant changes to the system have been made and no deficiencies found. (Authorizing Official) 4. Notify the Program Office/System Owner, in writing, of the accreditation status of the system along with any expected actions and schedule for completion. (Authorizing Official) 5. Submit a copy of the accreditation decision letter to the CISO for FISMA reporting purposes. (Program Office/System Owner) 6. Review results from the continuous monitoring process and update the security documentation as necessary and share the results with the Authorizing Official. (Program Office/System Owner, ISSO)

3.4.7 Continuous Monitoring

NIST SP 800-53 Control: CA-7
<p>CA-7: The organization monitors the security controls in the information system on an ongoing basis.</p>
<p>Security Baseline: Low, Moderate, and High</p>
<p>E-1: The organization employs an independent certification agent or certification team to monitor the security controls in the information system on an ongoing basis.</p>
<p>Related HUD Policy: 3.4.7</p>

NIST SP 800-53 Control: CA-7

Supporting Procedures

1. Select a subset of the security controls for continuous monitoring based on the perceived risks to the information system and knowledge of the system and its potential vulnerabilities. (Program Office/System Owner, ISSO)
2. Assess the selected controls following the guidance in NIST SP 800-53A, *Guide for Assessing the Security Controls in Federal Information Systems* and HUD *Security Assessment Guidelines*. (ISSO, System Administrator)
3. Implement changes to the information system based on the results of the control assessment. (Program Office/System Owner, ISSO)
4. Update the security documentation as necessary to reflect any changes to the information system (e.g., security plans, POA&Ms). (Program Office/System Owner, ISSO)
5. Continue following the continuous monitoring process, selecting a varied subset of controls based on an assessment of risk, and validate that those controls remain effectively implemented. Implement and document any needed changes to the system. (Program Office/System Owner, ISSO)
6. Conduct annual penetration testing on HUD network components. (Deputy CIO for IT Operations, CISO)

4.0 Operational Procedures

Operational controls are the security controls (i.e., safeguards or countermeasures) for an information system that are primarily implemented and executed by people (as opposed to systems). The procedures in this section provide guidance on how to implement operational controls and HUD security requirements.

4.1 Personnel Security

Information systems face threats from many sources, including the actions of people - employees, external users, and contractor personnel. The intentional and unintentional actions of these individuals can potentially harm or disrupt information systems and their facilities. These actions can result in the destruction or modification of the data being processed, denial of service to the end users, and unauthorized disclosure of data, potentially jeopardizing HUD’s mission.

The following procedures ensure that there are mechanisms in place to address user activities, responsibilities and consequences for inappropriate actions.

FIPS 200 Requirement
Organizations must: (i) ensure that individuals occupying positions of responsibility within organizations (including third-party service providers) are trustworthy and meet established security criteria for those positions; (ii) ensure that organizational information and information systems are protected during personnel actions, such as terminations and transfers; and (iii) employ formal sanctions for personnel failing to comply with organizational security policies and procedures.

4.1.1 Personnel Security Policy and Procedures

NIST SP 800-53 Control: PS-1
PS-1. The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, personnel security policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the personnel security policy and associated personnel security controls.
Security Baseline: Low, Moderate, and High
Related HUD Policy: <i>Information Technology Security Policy, Handbook 2400.25, Rev. 1</i>
Implementation
This control is implemented by the <i>Information Technology Security Policy, Handbook 2400.25, Rev. 1</i> , which defines HUD’s security policies. The procedures related to the HUD policies are in this document, <i>HUD Information Technology Security Procedures</i> .

4.1.2 Position Categorization

NIST SP 800-53 Control: PS-2
PS-2: The organization assigns a risk designation to all positions and establishes screening criteria for individuals filling those positions. The organization reviews and revises position risk designations periodically in accordance with Office of Personnel Management guidance.
Security Baseline: Low, Moderate, and High
Related HUD Policy: 4.1.2
Supporting Procedures
<ol style="list-style-type: none"> 1. Define position sensitivity levels for government positions and risk levels for contractor positions for standard HUD positions in accordance with 5 Code of Federal Regulations (CFR) 731.106(a) and Office of Personnel Management (OPM) policy and guidance. (OITS, Office of Human Resources [OHR]) 2. Define screening criteria for individuals filling HUD positions based on the sensitivity level or risk designation. (OITS, OHR) 3. Review position risk designations annually in accordance with OPM and HUD guidance. (OITS, Program Office/System Owner)

4.1.3 Personnel Screening

NIST SP 800-53 Control: PS-3
PS-3: The organization screens individuals requiring access to organizational information and information systems before authorizing access.
Security Baseline: Low, Moderate, and High
Related HUD Policy: 4.1.3
Supporting Procedures
<ol style="list-style-type: none"> 1. Assign a position sensitivity level or risk level designation for each position based on the established screening criteria. (Program Offices/System Owners) 2. Conduct an MBI of individuals (employees and contractors) based on criteria established for the sensitivity level or risk designation of the assigned position consistent with: (OHR, OSEP) <ul style="list-style-type: none"> • 5 CFR 731.106 • OPM policy, regulations, and guidance • HUD policy, regulations, and guidance • FIPS 201 and NIST SP 800-73, SP 800-76, and SP 800-78 • HUD Handbook 732.3, <i>Personnel Security/Suitability</i> (contractor specific) 3. Determine if government employees are U.S. citizens and if contractors are U.S. citizens, nationals of the United States, or aliens lawfully admitted to the United States for permanent residence. (OHR, OSEP) 4. Determine if a HUD employee or contractor is eligible for access to HUD systems and provide the information to the requesting office based on a favorably adjudicated background investigation and valid citizenship requirements. (OHR, OSEP) 5. Grant or deny access to HUD systems based on adjudication results. (Program Office/System Owner, ISSO)

4.1.4 Personnel Termination

NIST SP 800-53 Control: PS-4
<p>PS-4 The organization, upon termination of individual employment, terminates information system access, conducts exit interviews, retrieves all organizational information system-related property, and provides appropriate personnel with access to official records created by the terminated employee that are stored on organizational information systems.</p>
<p>Security Baseline: Low, Moderate, and High</p>
<p>Related HUD Policy: 4.1.4</p>
Supporting Procedures
<ol style="list-style-type: none"> 1. Notify the ISSO when an employee or contractor is no longer employed or associated with HUD. (Supervisor) 2. Revoke system accesses for those employees/contractors. (ISSO, System Administrator) 3. Obtain access to all official records stored on HUD information systems of terminated HUD employees or contractors. (Program Office/System Owner, ISSO) 4. Obtain all organizational information, media, or system-related property (e.g., keys, identification [ID] cards) from employees or contractors before they leave HUD. (Program Office/System Owner, ISSO) 5. Conduct exit interviews for employees or contractors who will no longer be associated with HUD. (Program Office/System Owner)

4.1.5 Personnel Transfer

NIST SP 800-53 Control: PS-5
<p>PS-5: The organization reviews information systems/facilities access authorizations when personnel are reassigned or transferred to other positions within the organization and initiates appropriate actions.</p>
<p>Security Baseline: Low, Moderate, and High</p>
<p>Related HUD Policy: 4.1.5</p>
Supporting Procedures
<ol style="list-style-type: none"> 1. Review system access authorizations when an employee or contractor is reassigned or transferred to another position. (Supervisor, Program Office/System Owner, ISSO) 2. Revoke or reassign system accesses as appropriate. (ISSO, System Administrator) 3. Obtain all organizational information and system-related property (e.g., keys, ID cards, building passes) from employees or contractors as appropriate. (Program Office/System Owner, ISSO) 4. Transfer all official records stored on HUD information systems from the reassigned or transferred employee or contractor to an appropriate person. (Users, Program Office/System Owner, ISSO)

4.1.6 Access Agreements

NIST SP 800-53 Control: PS-6
PS-6: The organization completes appropriate signed access agreements for individuals requiring access to organizational information and information systems before authorizing access and reviews/updates the agreements every three years or when a transfer occurs.
Security Baseline: Low, Moderate, and High
Related HUD Policy: 4.1.6
Supporting Procedures
<ol style="list-style-type: none"> 1. Determine appropriate access agreements (e.g., rules of behavior, non-disclosure agreement, conflict-of-interest agreement) for each individual approved for access to HUD information systems. (Program Office/System Owner) 2. Provide all HUD-required access agreements to individuals who have requested and obtained approval to use HUD information systems. (ISSO, System Administrator) 3. Sign all required access agreements. (Users) 4. Maintain records of all access agreements. (Program Office/System Owner, ISSO) 5. Update the access agreements and have users re-sign them every three years or if a transfer occurs. (Program Offices/System Owners, ISSO)

4.1.7 Third-Party Personnel Security

NIST SP 800-53 Control: PS-7
PS-7: The organization establishes personnel security requirements including security roles and responsibilities for third-party providers and monitors provider compliance.
Security Baseline: Low, Moderate, and High
Related HUD Policy: 4.1.7
Supporting Procedures
<ol style="list-style-type: none"> 1. Ensure that personnel security requirements for third-party providers are included in acquisition-related documents. (Program Office/System Owner, Contracting Officer) 2. Review existing contracts to identify any contracts that do not include personnel security requirements. Modify the contracts to include personnel security requirements in a reasonable timeframe. (Program Office/System Owner) 3. Monitor the third-party providers to ensure they comply with personnel security requirements during the life of the contract. (Program Office/System Owner)

4.1.8 Personnel Sanctions

NIST SP 800-53 Control: PS-8
PS-8. The organization employs a formal sanctions process for personnel failing to comply with established information security policies and procedures.
Security Baseline: Low, Moderate, and High
Related HUD Policy: 4.1.8

NIST SP 800-53 Control: PS-8
Supporting Procedures
<ol style="list-style-type: none"> 1. Monitor the use of HUD information systems to determine if employees or contractors have violated HUD policies and procedures. (Program Office/System Owner, ISSO, System Administrator) 2. Notify the appropriate person when a violation occurs and determine the severity and willfulness of the violation. (Program Office/System Owner, ISSO, User) 3. Determine the appropriate disciplinary action for the violation, including termination of access to HUD systems, if appropriate (Program Office/System Owner, HUD General Counsel) 4. Determine if criminal or civil prosecution is warranted based on the severity and willfulness of the violation. (Program Office/System Owner, HUD General Counsel)

4.2 Physical and Environmental Protection

Physical security represents the first line of defense against intruders and adversaries attempting to gain access to facilities and or information systems. 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 departmental facilities.

The following procedures ensure that there are mechanisms in place to protect against threats associated with the physical environment to include physical access control as well as the physical plant controls.

FIPS 200 Requirement
Organizations must: (i) limit physical access to information systems, equipment, and respective operating environments to authorized individuals; (ii) protect the physical plant and supporting infrastructure for information systems; (iii) provide supporting utilities for information systems; (iv) protect information systems against environmental hazards; and (v) provide appropriate environmental controls in facilities containing information systems.

4.2.1 Physical and Environmental Protection Policy and Procedures

NIST SP 800-53 Control: PE-1
PE-1. The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, physical, and environmental protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the physical and environmental protection policy and associated physical and environmental protection controls.
Security Baseline: Low, Moderate, and High
Related HUD Policy: <i>Information Technology Security Policy, Handbook 2400.25, Rev. 1</i>
Implementation
This control is implemented by the <i>Information Technology Security Policy, Handbook 2400.25, Rev. 1</i> , which defines HUD’s security policies. The procedures related to the HUD policies are in this document, <i>HUD Information Technology Security Procedure</i> .

4.2.2 Physical Access Authorizations

NIST SP 800-53 Control: PE-2
<p>PE-2: The organization develops and keeps current a list of personnel with authorized access to the facility where the information system resides (except for those areas within the facility officially designated as publicly accessible) and issues appropriate authorization credentials. Designated officials within the organization review and approve the access list and authorization credentials annually.</p>
<p>Security Baseline: Low, Moderate, and High</p>
<p>Related HUD Policy: 4.2.2</p>
Supporting Procedures
<ol style="list-style-type: none"> 1. Maintain a list of individuals authorized to access all HUD facilities (e.g., Headquarters, Field Offices, Regional Offices) and update the access list promptly, adding new individuals who have been approved for access and removing individuals who no longer require access. (OSEP) 2. Issue approved access credentials to all individuals approved for access to HUD facilities. (OSEP) 3. Review and approve the access lists annually. (OSEP)

4.2.3 Physical Access Control

NIST SP 800-53 Control: PE-3
<p>PE-3: The organization controls all physical access points (including designated entry/exit points) to the facility where the information system resides (except for those areas within the facility officially designated as publicly accessible) and verifies individual access authorizations before granting access to the facility. The organization controls access to areas officially designated as publicly accessible, as appropriate, in accordance with the organization's assessment of risk.</p>
<p>Security Baseline: Low, Moderate, and High</p>
<p>E-1: The organization controls access to the information system independent of the physical access controls of the facility.</p>
<p>Security Baseline: High</p>
<p>Related HUD Policy: 4.2.3</p>
Supporting Procedures
<ol style="list-style-type: none"> 1. Control all physical access points to HUD facilities housing concentrations of information systems with an appropriate device (e.g., keys, locks, combinations, card readers) or guards, except for those areas designated as publicly accessible. (OSEP) 2. Control access to all individuals entering controlled areas. Confirm authorization credentials prior to granting access even after an emergency-related event. (OSEP) 3. Maintain an inventory of all access control devices, validating and updating the inventory every six months. (OSEP) 4. Change combinations and keys periodically and when keys are lost, combinations are compromised, or individuals are transferred or terminated. (OSEP)

4.2.4 Access Control for Transmission Medium

NIST SP 800-53 Control: PE-4
PE-4: The organization controls physical access to information system distribution and transmission lines within organizational facilities.
Security Baseline: High
Related HUD Policy: 4.2.4
Supporting Procedures
1. Control access to information system transmission lines by selecting an appropriate access control device. (Deputy CIO for IT Operations, Service Provider)

4.2.5 Access Control for Display Medium

NIST SP 800-53 Control: PE-5
PE-5: The organization controls physical access to information system devices that display information to prevent unauthorized individuals from observing the display output.
Security Baseline: Moderate and High
Related HUD Policy: 4.2.5
Supporting Procedures
1. Control access to designated areas that contain HUD information system devices (e.g., monitors, printers, fax machines) that display information from moderate- or high-impact systems by selecting an appropriate access control device (e.g., keys, locks, combinations, card readers). (OSEP, Service Provider)

4.2.6 Monitoring Physical Access

NIST SP 800-53 Control: PE-6
PE-6: The organization monitors physical access to the information system to detect and respond to physical security incidents.
Security Baseline: Low, Moderate, and High
E-1: The organization monitors real-time intrusion alarms and surveillance equipment.
Security Baseline: Moderate and High
E-2: The organization employs automated mechanisms to recognize potential intrusions and initiate appropriate response actions.
Security Baseline: High
Related HUD Policy: 4.2.6

NIST SP 800-53 Control: PE-6
Supporting Procedures
<ol style="list-style-type: none"> 1. Review physical access logs for facilities housing HUD information systems daily. (OSEP) 2. Conduct real-time monitoring of physical access to facilities housing moderate- and high-impact HUD information systems. Use automated mechanisms to monitor physical access to high-impact systems. (OSEP, Service Provider) 3. Investigate apparent security violations or suspicious physical access activities in a timely manner for low-impact systems and immediately for moderate- and high-impact systems. (OSEP)

4.2.7 Visitor Control

NIST SP 800-53 Control: PE-7
<p>PE-7: The organization controls physical access to the information system by authenticating visitors before authorizing access to the facility where the information system resides, other than areas designated as publicly accessible.</p> <p>Security Baseline: Low, Moderate, and High</p>
<p>(E-1): The organization escorts visitors and monitors visitor activity, when required.</p> <p>Security Baseline: Moderate and High</p>
<p>Related HUD Policy: 4.2.7</p>
Supporting Procedures
<ol style="list-style-type: none"> 1. Verify the identity of all visitors by means of government issued identification (e.g., government ID, drivers license) to limit access to facilities housing HUD information systems. (OSEP, Service Provider) 2. Sign in and out all visitors when entering or leaving facilities housing HUD information systems. (OSEP, Service Provider) 3. Provide an escort for all visitors to areas housing moderate-or high-impact HUD information systems. (Users) 4. Ensure contractors' access to facilities housing HUD information systems is limited to those work areas necessary to complete their assigned duties. (Program Office/System Owner, Service Provider)

4.2.8 Access Records

NIST SP 800-53 Control: PE-8
<p>PE-8: The organization maintains visitor access records to the facility where the information system resides (except for those areas within the facility officially designated as publicly accessible) that includes: (i) name and organization of the person visiting; (ii) signature of the visitor; (iii) form of identification; (iv) date of access; (v) time of entry and departure; (vi) purpose of visit; and (vii) name and organization of person visited. Designated officials within the organization review the visitor access records monthly.</p> <p>Security Baseline: Low, Moderate, and High</p>

NIST SP 800-53 Control: PE-8
E-1: The organization employs automated mechanisms to facilitate the maintenance and review of access records. Security Baseline: High
E-2: The organization maintains a record of all physical access, both visitor and authorized individuals. Security Baseline: High
Related HUD Policy: 4.2.8
Supporting Procedures
<ol style="list-style-type: none"> 1. Maintain visitor records for at least one year. Use an automated mechanism at any facility housing high-impact systems. (OSEP) 2. Review the visitor records monthly. (OSEP) 3. Review the records at closeout and keep the records on file and available for at least one year. (OSEP)

4.2.9 Power Equipment and Power Cabling

NIST SP 800-53 Control: PE-9
PE-9: The organization protects power equipment and power cabling for the information system from damage and destruction. Security Baseline: Moderate and High
E-1: The organization employs redundant and parallel power cabling paths. Security Baseline: N/A
Related HUD Policy: 4.2.9
Supporting Procedures
<ol style="list-style-type: none"> 1. Place power equipment and cabling for moderate-and high-impact information systems in a protected environment. (OSEP, Deputy CIO for IT Operations, Service Provider)

4.2.10 Emergency Shutoff

NIST SP 800-53 Control: PE-10
PE-10: The organization provides, for specific locations within a facility containing concentrations of information system resources, the capability of shutting off power to any information technology system that may be malfunctioning or threatened without endangering personnel by requiring them to approach the equipment. Security Baseline: Moderate and High
E-1; The organization protects the emergency power-off capability from accidental or unauthorized activation. Security Baseline: High

NIST SP 800-53 Control: PE-10
Related HUD Policy: 4.2.10
Supporting Procedures
<ol style="list-style-type: none"> 1. Verify periodically that electrical shutoff capability exists, is operational, and can safely be used in the event of a threat to or a malfunction of any moderate-or high-impact information system. (OSEP, Service Provider) 2. Update facilities to provide compliant electrical shutoff capability if this capability does not exist, or move the equipment to a compliant location. For high-impact systems, ensure the power-off capability is protected from accidental or unauthorized activation. (OSEP) 3. Prepare written procedures on how to implement an emergency electrical shut-off and keep the procedures up-to-date. (OSEP) 4. Train all responsible personnel on the safe procedures for emergency electrical shut-off. (OSEP, Program Office/System Owner, Service Provider)

4.2.11 Emergency Power

NIST SP 800-53 Control: PE-11
PE-11: The organization provides a short-term uninterruptible power supply to facilitate an orderly shutdown of the information system in the event of a primary power source loss.
Security Baseline: Moderate and High
E-1: The organization provides a long-term alternate power supply for the information system that is capable of maintaining minimally required operational capability in the event of an extended loss of the primary power source.
Security Baseline: High
E-2: The organization provides a long-term alternate power supply for the information system that is self-contained and not reliant on external power generation.
Security Baseline: N/A
Related HUD Policy: 4.2.11
Supporting Procedures
<ol style="list-style-type: none"> 1. Obtain and implement an appropriate short-term uninterruptible power supply for all HUD information systems to allow an orderly shut down if power is lost. (OSEP, Program Office/System Owner, Service Provider, System Administrator) 2. Obtain an alternate long-term power source for moderate- and high-impact HUD systems to maintain minimal operational capability. (OSEP, Program Office/System Owner, Service Provider) 3. Prepare written procedures on how to transfer to an alternate power source and keep the procedures up-to-date. (OSEP)

4.2.12 Emergency Lighting

NIST SP 800-53 Control: PE-12
PE-12: The organization employs and maintains automatic emergency lighting that activates in the event of a power outage or disruption and that covers emergency exits and evacuation routes.
Security Baseline: Low, Moderate, and High
Related HUD Policy: 4.2.12
Supporting Procedures
1. Provide automatic emergency lighting systems that activate in the event of a power outage or disruption that covers emergency exits and evacuation routes. (OSEP, Service Provider)

4.2.13 Fire Protection

NIST SP 800-53 Control: PE-13
PE-13: The organization employs and maintains fire suppression and detection devices/systems that can be activated in the event of a fire.
Security Baseline: Low, Moderate, and High
E-1: The organization employs fire detection devices/systems that activate automatically and notify the organization and emergency responders in the event of a fire.
Security Baseline: Moderate and High
E-2: The organization employs fire suppression devices/systems that provide automatic notification of any activation to the organization and emergency responders.
Security Baseline: High
E-3: The organization employs an automatic fire suppression capability in facilities that are not staffed on a continuous basis.
Security Baseline: High
Related HUD Policy: 4.2.13
Supporting Procedures
<ol style="list-style-type: none"> 1. Provide fire suppression and detection devices/systems that can be activated in the event of a fire. For moderate- and high-impact systems, the fire suppression devices/systems must activate automatically. (OSEP, Service Provider) 2. Notify, automatically, HUD facilities office and emergency responders when the fire detection system is activated by an event. (OSEP, Service Provider)

4.2.14 Temperature and Humidity Controls

NIST SP 800-53 Control: PE-14
PE-14: The organization regularly maintains, within acceptable levels, and monitors the temperature and humidity within the facility where the information system resides.
Security Baseline: Low, Moderate, and High
Related HUD Policy: 4.2.14
Supporting Procedures
1. Monitor and maintain the temperature and humidity within acceptable levels in all facilities housing HUD information systems. (OSEP, Service Provider)

4.2.15 Water Damage Protection

NIST SP 800-53 Control: PE-15
PE-15: The organization protects the information system from water damage resulting from broken plumbing lines or other sources of water leakage by providing master shutoff valves that are accessible, working properly, and known to key personnel.
Security Baseline: Low, Moderate, and High
E-1: The organization employs mechanisms that, without the need for manual intervention, protect the information system from water damage in the event of a significant water leak.
Security Baseline: High
Related HUD Policy: 4.2.15
Supporting Procedures
<ol style="list-style-type: none"> 1. Determine the location of the master water shutoff valves and train key personnel on the location of the master shutoff valves. (OSEP, Service Provider) 2. Ensure the water shutoff valves are accessible and working properly. For high-impact systems, ensure the shutoff valves operate automatically if a significant water leak occurs. (OSEP, Service Provider)

4.2.16 Delivery and Removal

NIST SP 800-53 Control: PE-16
PE-16: The organization authorizes and controls information system-related items entering and exiting the facility and maintains appropriate records of those items.
Security Baseline: Low, Moderate, and High
Related HUD Policy: 4.2.16

NIST SP 800-53 Control: PE-16
Supporting Procedures
<ol style="list-style-type: none"> 1. Control access to delivery areas and, if possible, isolate delivery areas from the information system and media libraries. (OSEP, Program Office/System Owner, Service Provider) 2. Authorize the delivery or removal of information system-related items associated with HUD information systems. (OSEP, Program Office/System Owner, Service Provider) 3. Maintain records of all information system-related items and status of their location. (OSEP, Program Office/System Owner, Service Provider)

4.2.17 Alternate Work Site

NIST SP 800-53 Control: PE-17
<p>PE-17: The organization employs appropriate management, operational, and technical information system security controls at alternate work sites.</p> <p>Security Baseline: Moderate and High</p> <p>Related HUD Policy: 4.2.17</p>
Supporting Procedures
<ol style="list-style-type: none"> 1. Ensure that individuals working at alternate work sites follow HUD information security requirements. (Program Office/System Owner, Users) 2. Implement appropriate controls for broadband communications for accessing moderate- or high-impact systems following the guidance in NIST SP 800-46, <i>Security for Telecommuting and Broadband Communications</i>. (Program Office/System Owner, Users, System Administrator) 3. Report any security problems to the ISSO and the HUD CSIRC. (Users)

4.2.18 Location of Information System Components

NIST SP 800-53 Control: PE-18
<p>PE-18: The organization positions information system components within the facility to minimize potential damage from physical and environmental hazards and to minimize the opportunity for unauthorized access.</p> <p>Security Baseline: Moderate and High</p> <p>E-1: The organization plans the location or site of the facility where the information system resides with regard to physical and environmental hazards and for existing facilities, considers the physical and environmental hazards in the risk mitigation strategy.</p> <p>Security Baseline: High</p> <p>Related HUD Policy: 4.2.18</p>
Supporting Procedures
<ol style="list-style-type: none"> 1. Store information system components at HUD facilities as deemed practical by the Deputy CIO for IT Operations. (Program Office/System Owner, Deputy CIO for IT Operations)

4.2.19 Information Leakage

NIST SP 800-53 Control: PE-19
PE-19: The organization protects the information system from information leakage due to electromagnetic signals emanations.
Security Baseline: N/A
Related HUD Policy: None
Supporting Procedures
If selected: 1. Protect the information system from information leakage due to electromagnetic signals emanations.

4.2.20 Facilities Housing HUD Information Systems

HUD Policy: HUD PE-1
HUD Policy: 4.2.20 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 information systems, and in some cases, areas designated as publicly accessible inside HUD facilities.
Security Baseline: Low, Moderate, and High
Supporting Procedures
1. Control access to facilities (e.g., data centers, wiring closets, server rooms) processing, transmitting, or storing HUD sensitive information by selecting an appropriate access control device (e.g., keys, locks, combinations, card readers). (OSEP, Service Provider)

4.2.21 Redundant Air-Cooling Systems

HUD Policy: HUD PE-2
HUD Policy: 4.2.21 For specific locations within a facility containing concentrations of information system resources (e.g., data centers, server rooms, or mainframe rooms), the facilities group or security officer shall maintain a redundant air-cooling system.
Security Baseline: Low, Moderate, and High
Supporting Procedures
1. Provide and maintain redundant air-cooling systems for specific locations within facilities housing HUD information systems that contain concentrations of information system resources. (OSEP)

4.3 Contingency Planning

Contingency planning relates to the establishment, maintenance, and effective implementation of plans for emergency response, backup operations, and post-disaster recovery for organizational information systems to ensure the availability of critical information resources and continuity of operations in emergency situations.

The following procedures ensure that there are mechanisms in place to protect information assets and restore services with minimal disruption during an emergency.

FIPS 200 Requirement
Organizations must establish, maintain, and effectively implement plans for emergency response, backup operations, and post-disaster recovery for organizational information systems to ensure the availability of critical information resources and continuity of operations in emergency situations.

4.3.1 Contingency Planning Policy and Procedures

NIST SP 800-53 Control: CP-1
CP-1: The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, contingency planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the contingency planning policy and associated contingency planning controls.
Security Baseline: Low, Moderate, and High
Related HUD Policy: <i>Information Technology Security Policy, Handbook 2400.25, Rev. 1</i>
Implementation
This control is implemented by the <i>Information Technology Security Policy, Handbook 2400.25, Rev. 1</i> , which defines HUD's security policies. The procedures related to the HUD policies are in this document, <i>HUD Information Technology Security Procedures</i> .

4.3.2 Contingency Plan

NIST SP 800-53 Control: CP-2
CP-2: The organization develops and implements a contingency plan for the information system addressing contingency roles, responsibilities, assigned individuals with contact information, and activities associated with restoring the system after a disruption or failure. Designated officials within the organization review and approve the contingency plan and distribute copies of the plan to key contingency personnel.
Security Baseline: Low, Moderate, and High
E-1: The organization coordinates contingency plan development with organizational elements responsible for related plans.
Security Baseline: Moderate and High

NIST SP 800-53 Control: CP-2
E-2: The organization conducts capacity planning so that necessary capacity for information processing, telecommunications, and environmental support exists during crisis situations.
Security Baseline: High
Related HUD Policy: 4.3.2
Supporting Procedures
<ol style="list-style-type: none"> 1. Develop a contingency plan that includes a business impact assessment for HUD information systems following guidance provided in the HUD <i>Contingency Planning Guidance</i> and NIST SP 800-34, <i>Contingency Planning Guide for Information Technology Systems</i>. (Program Office/System Owner, ISSO) 2. Distribute the contingency plan to key individuals, CISO, and the Deputy CIO for IT Operations. (Program Office/System Owner, ISSO) 3. Coordinate contingency activities with HUD organizations responsible for CIP and business continuity planning for moderate- or high-impact systems. (Program Office/System Owner) 4. Conduct capacity planning and impact analyses for high-impact systems to ensure necessary capacity for information processing, telecommunications, and environmental support exists during crisis situations. (Program Office/System Owner, ISSO)

4.3.3 Contingency Training

NIST SP 800-53 Control: CP-3
CP-3: The organization trains personnel in their contingency roles and responsibilities with respect to the information system and provides refresher training annually.
Security Baseline: Moderate and High
E-1: The organization incorporates simulated events into contingency training to facilitate effective response by personnel in crisis situations.
Security Baseline: High
E-2: The organization employs automated mechanisms to provide a more thorough and realistic training environment.
Security Baseline: N/A
Related HUD Policy: 4.3.3
Supporting Procedures
<ol style="list-style-type: none"> 1. Train personnel on their contingency roles and responsibilities. (Program Office/System Owner, ISSO) 2. Provide annual refresher training, focusing on any changes implemented in the previous year. (Program Office/System Owner, ISSO) 3. Incorporate simulations when training is associated with a high-impact system. (Program Office/System Owner, ISSO) 4. Complete annual refresher training and maintain contingency planning training records. (Program Office/System Owner, ISSO, Individuals with key contingency roles)

4.3.4 Contingency Plan Testing and Exercises

NIST SP 800-53 Control: CP-4
<p>CP-4: The organization: (i) tests and/or exercises the contingency plan for the information system annually using appropriate methods to determine the plan’s effectiveness and the organization’s readiness to execute the plan; and (ii) reviews the contingency plan test/exercise results and initiates corrective actions.</p> <p>Security Baseline: Moderate and High</p>
<p>E-1: The organization coordinates contingency plan testing and/or exercises with organizational elements responsible for related plans.</p> <p>Security Baseline: Moderate and High</p>
<p>E-2: The organization tests/exercises the contingency plan at the alternate processing site to familiarize contingency personnel with the facility and available resources and to evaluate the site’s capabilities to support contingency operations.</p> <p>Security Baseline: High</p>
<p>E-3: The organization employs automated mechanisms to more thoroughly and effectively test/exercise the contingency plan by providing more complete coverage of contingency issues, selecting more realistic test/exercise scenarios and environments, and more effectively stressing the information system and supported missions..</p> <p>Security Baseline: N/A</p>
<p>Related HUD Policy: 4.3.4</p>
Supporting Procedures
<ol style="list-style-type: none"> 1. Conduct and document the results of the annual contingency plan testing for moderate- and high-impact systems using an appropriate testing methodology (e.g., functional/tabletop exercise, full-scale testing). Test all high-impact systems at the alternate processing site. (Program Office/System Owner, ISSO) 2. Coordinate annual testing with HUD organizations responsible for CIP and business continuity planning. (Program Office/System Owner, ISSO) 3. Document test results noting any issues or problems. (Program Office/System Owner, ISSO) 4. Forward a copy of the test results to the CISO and the Deputy CIO for IT Operations. (Program Office/System Owner, ISSO) 5. Track contingency plan test dates for each HUD information system to meet FISMA reporting requirements. (OITS) 6. Initiate corrective actions and modify the contingency plan to address issues and problems noted during the test. (Program Office/System Owner, ISSO) 7. Distribute the updated contingency plan to all key personnel. (Program Office/System Owner, ISSO)

4.3.5 Contingency Plan Update

NIST SP 800-53 Control: CP-5
<p>CP-5: The organization reviews the contingency plan for the information system annually and revises the plan to address system/organizational changes or problems encountered during plan implementation, execution, or testing.</p>
<p>Security Baseline: Low, Moderate, and High</p>
<p>Related HUD Policy: 4.3.5</p>
Supporting Procedures
<ol style="list-style-type: none"> 1. Review the contingency plan annually, addressing system/organizational changes or problems identified during the plan implementation, execution, or testing. (Program Office/System Owner, ISSO) 2. Revise the contingency plan based on information collected during the review process. (Program Office/System Owner, ISSO) 3. Forward a copy of the revised contingency plan to key individuals and the Authorizing Official. (Program Office/System Owner, ISSO)

4.3.6 Alternate Storage Site

NIST SP 800-53 Control: CP-6
<p>CP-6: The organization identifies an alternate storage site and initiates necessary agreements to permit the storage of information system backup information.</p>
<p>Security Baseline: Moderate and High</p>
<p>E-1: The organization identifies an alternate storage site that is geographically separated from the primary storage site so as not to be susceptible to the same hazards.</p>
<p>Security Baseline: Moderate and High</p>
<p>E-2: The organization configures the alternate storage site to facilitate timely and effective recovery operations.</p>
<p>Security Baseline: High</p>
<p>E-3: The organization identifies potential accessibility problems to the alternate storage site in the event of an area-wide disruption or disaster and outlines explicit mitigation actions.</p>
<p>Security Baseline: High</p>
<p>Related HUD Policy: 4.3.6</p>

NIST SP 800-53 Control: CP-6
Supporting Procedures
<ol style="list-style-type: none"> 1. Procure alternate storage sites for all moderate- and high-impact systems, including obtaining alternate storage site agreements. Alternate sites for high-impact systems must be geographically separate from the primary storage site. (Deputy CIO for IT Operations) 2. Ensure the alternate site for high-impact systems is configured to facilitate timely and effective recovery procedures. (Deputy CIO for IT Operations) 3. Identify potential accessibility problems to the alternate storage site in the event of an area-wide disruption or disaster (e.g., massive power outage, bomb) and outline explicit mitigation instructions for high-impact systems. (Deputy CIO for IT Operations, Program Office/System Owner)

4.3.7 Alternate Processing Site

NIST SP 800-53 Control: CP-7
<p>CP-7: The organization identifies an alternate processing site and initiates necessary agreements to permit the resumption of information system operations for critical mission/business functions within 24 hours when the primary processing capabilities are unavailable.</p> <p>Security Baseline: Moderate and High</p>
<p>E-1: The organization identifies an alternate processing site that is geographically separated from the primary processing site so as not to be susceptible to the same hazards.</p> <p>Security Baseline: Moderate and High</p>
<p>E-2: The organization identifies potential accessibility problems to the alternate processing site in the event of an area-wide disruption or disaster and outlines explicit mitigation actions.</p> <p>Security Baseline: Moderate and High</p>
<p>E-3: The organization develops alternate processing site agreements that contain priority-of-service provisions in accordance with the organization's availability requirements.</p> <p>Security Baseline: Moderate and High</p>
<p>E-4: The organization fully configures the alternate processing site so that it is ready to be used as the operational site supporting a minimum required operational capability.</p> <p>Security Baseline: High</p>
<p>Related HUD Policy: 4.3.7</p>

NIST SP 800-53 Control: CP-7
Supporting Procedures
<ol style="list-style-type: none"> 1. Procure alternate processing sites for moderate- and high-impact systems, including obtaining alternate processing site agreements. Alternate sites must be geographically separate from the primary processing site. (Deputy CIO for IT Operations) 2. Provide equipment and supplies at the alternate site required to resume operations within the recovery time defined in the security plan or ensure contracts are in place to support delivery of the required equipment to the site in the specified timeframe. For high-impact systems, the site must be fully configured to support minimum required operational capabilities and ready to use as an operational site within the timeframe defined in the security plan. (Deputy CIO for IT Operations) 3. Define priority-of-service provisions based on availability requirements and include them in the processing site agreements. (Deputy CIO for IT Operations) 4. Identify potential accessibility problems to the alternate processing site in the event of an area-wide disruption or disaster and outline explicit mitigation instructions. (Deputy CIO for IT Operations, Program Office/System Owner)

4.3.8 Telecommunications Services

NIST SP 800-53 Control: CP-8
<p>CP-8: The organization identifies primary and alternate telecommunications services to support the information system and initiates necessary agreements to permit the resumption of system operations for critical mission/business functions within 24 hours when the primary telecommunications capabilities are unavailable.</p> <p>Security Baseline: Moderate and High</p>
<p>E-1: The organization develops primary and alternate telecommunications service agreements that contain priority-of-service provisions in accordance with the organization's availability requirements.</p> <p>Security Baseline: Moderate and High</p>
<p>E-2: The organization obtains alternate telecommunications services that do not share a single point of failure with primary telecommunications services.</p> <p>Security Baseline: Moderate and High</p>
<p>E-3: The organization obtains alternate telecommunications service providers that are sufficiently separated from primary service providers so as not to be susceptible to the same hazards.</p> <p>Security Baseline: High</p>
<p>E-4: The organization requires primary and alternate telecommunications service providers to have adequate contingency plans.</p> <p>Security Baseline: High</p>
<p>Related HUD Policy: 4.3.8</p>

NIST SP 800-53 Control: CP-8
Supporting Procedures
<ol style="list-style-type: none"> 1. Procure alternate telecommunications services to support moderate- and high-impact systems, including obtaining alternate telecommunications service agreements. Ensure the alternate service does not share a single point of failure with the primary service, is sufficiently separated from the primary service provider so as not to be susceptible to the same hazards, and available within 24 hours. (Deputy CIO for IT Operations) 2. Request Telecommunications Service Priority (TSP) for all telecommunications services used for national security emergency preparedness (see http://tsp.ncs.gov), if the primary or alternate telecommunications services are provided by a wireline carrier. (Deputy CIO for IT Operations) 3. Define priority-of-service provisions based on availability requirements and include in the telecommunications service agreement. (Deputy CIO for IT Operations) 4. Review telecommunications services provider's contingency plans for high-impact systems to determine if they are adequate. (Deputy CIO for IT Operations)

4.3.9 Information System Backup

NIST SP 800-53 Control: CP-9
<p>CP-9: The organization conducts backups of user-level and system-level information (including system state information) contained in the information system as specified in the information system contingency plan and protects backup information at the storage location.</p> <p>Security Baseline: Low, Moderate, and High</p>
<p>E-1: The organization tests backup information quarterly to verify media reliability and information integrity.</p> <p>Security Baseline: Moderate and High</p>
<p>E-2: The organization selectively uses backup information in the restoration of information system functions as part of contingency plan testing.</p> <p>Security Baseline: High</p>
<p>E-3: The organization stores backup copies of the operating system and other critical information system software in a separate facility or in a fire-rated container that is not collocated with the operational software.</p> <p>Security Baseline: High</p>
<p>E-4: The organization protects system backup information from unauthorized modification.</p> <p>Security Baseline: N/A</p>
<p>Related HUD Policy: 4.3.9</p>

NIST SP 800-53 Control: CP-9
Supporting Procedures
<ol style="list-style-type: none"> 1. Back-up user-level and system-level information, including system state information as defined in the security plan. (Deputy CIO for IT Operations, Program Office/System Owner, ISSO, System Administrator) 2. Store backup information at a secure offsite location as stated in the contingency plan. (Deputy CIO for IT Operations, Program Office/System Owner, ISSO, System Administrator) 3. Protect system backup information on high-impact systems from unauthorized modification whenever it is removed from a HUD facility. (Deputy CIO for IT Operations, Program Office/System Owner, ISSO, System Administrator). 4. Test the backup information quarterly to determine media usability and data integrity for moderate- and high-impact systems. (Deputy CIO for IT Operations, Program Office/System Owner, ISSO, System Administrator) 5. Test backup information and media with the contingency plan test for high-impact systems. (Deputy CIO for IT Operations, Program Office/System Owner, ISSO, System Administrator) 6. Store backup copies of the operating system and other critical information systems in a fire-rated container that is not collocated with the operating system, or in a separate facility. (Deputy CIO for IT Operations, Program Office/System Owner, ISSO, System Administrator)

4.3.10 Information System Recovery and Reconstitution

NIST SP 800-53 Control: CP-10
<p>CP-10: The organization employs mechanisms with supporting procedures to allow the information system to be recovered and reconstituted to a known secure state after a disruption or failure.</p> <p>Security Baseline: Low, Moderate, and High</p>
<p>E-1: The organization includes a full recovery and reconstitution of the information system as part of contingency plan testing.</p> <p>Security Baseline: High</p>
<p>Related HUD Policy: 4.3.10</p>
Supporting Procedures
<ol style="list-style-type: none"> 1. Provide mechanisms and supporting procedures to ensure recovery and reconstitution of the system's original state, including resetting all system parameters (either default or organization-established), reinstalling all patches, reestablishing all configuration settings, verifying the availability of all system documentation and operating procedures, reinstalling all application and system software, and reinstalling the information from the most recent backup. (Deputy CIO for IT Operations, Program Office/System Owner, ISSO, System Administrator) 2. Test the recovered system. (Program Office/System Owner, ISSO) 3. Test a full recovery and reconstitution of the information system as part of the annual contingency plan testing for high-impact systems. (Deputy CIO for IT Operations, Program Office/System Owner, ISSO, System Administrator)

4.4 Configuration Management

Configuration management manages the configuration of all hardware and software elements of information 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 configuration management process.

The following procedures ensure that there are mechanisms in place to track the configuration baseline and the changes to that configuration, address user activities and responsibilities, and consequences for inappropriate actions.

FIPS 200 Requirement
Organizations must: (i) establish and maintain baseline configurations and inventories of organizational information systems; (ii) establish and enforce security configuration settings for information technology products employed in organizational information systems; and (iii) monitor and control changes to the baseline configurations and to the constituent components of organizational information systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles.

4.4.1 Configuration Management Policy and Procedures

NIST SP 800-53 Control: CM-1
CM-1: The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, configuration management policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the configuration management policy and associated configuration management controls.
Security Baseline: Low, Moderate, and High
Related HUD Policy: <i>Information Technology Security Policy, Handbook 2400.25, Rev. 1</i>
Implementation
This control is implemented by the <i>Information Technology Security Policy, Handbook 2400.25, Rev. 1</i> , which defines HUD's security policies. The procedures related to the HUD policies are in this document, <i>HUD Information Technology Security Procedures</i> .

4.4.2 Baseline Configuration

NIST SP 800-53 Control: CM-2
CM-2: The organization develops, documents, and maintains a current-baseline configuration of the information system.
Security Baseline: Low, Moderate, and High
E-1: The organization updates the baseline configuration of the information system as an integral part of information system component installations.
Security Baseline: Moderate and High
E-2: The organization employs automated mechanisms to maintain an up-to-date, complete, accurate, and readily available baseline configuration of the information system.
Security Baseline: High

NIST SP 800-53 Control: CM-2
Related HUD Policy: 4.4.2
Supporting Procedures
<ol style="list-style-type: none"> 1. Document baseline configurations for all HUD systems. (Program Office/System Owner, ISSO, System Administrator) 2. Validate that the system configuration is consistent with HUD's Enterprise Architecture Technical Reference Model (TRM) and enterprise security architecture. (Program Office/System Owner, ISSO) 3. Update the baseline configuration during installation of information system components (e.g., upgrades, patches, new software) for moderate-and high-impact systems. (Program Office/System Owner, ISSO) 4. Use automated mechanisms to maintain an up-to-date, complete, accurate, and readily available baseline configuration for high-impact systems and components. (Program Office/System Owner)

4.4.3 Configuration Change Control

NIST SP 800-53 Control: CM-3
CM-3: The organization authorizes, documents, and controls changes to the information system.
Security Baseline: Moderate and High
E-1: The organization employs automated mechanisms to: (i) document proposed changes to the information system; (ii) notify appropriate approval authorities; (iii) highlight approvals that have not been received in a timely manner; (iv) inhibit change until necessary approvals are received; and (v) document completed changes to the information system.
Security Baseline: High
Related HUD Policy: 4.4.3
Supporting Procedures
<ol style="list-style-type: none"> 1. Prepare a Configuration Management Plan for each information system under their purview. (Program Office/System Owner, ISSO) 2. Establish a Configuration Control Board (CCB) for moderate- and high-impact systems and define their operating procedures in a configuration management plan, including procedures for emergency changes including critical patches. (Program Office/System Owner, ISSO) 3. Request changes to HUD systems justifying the need for the change and submit them to the CCB. (Program Office/System Owner, ISSO) 4. Test all proposed changes to determine the security impact and document and resolve any issues. (CCB, Program Office/System Owner, ISSO) 5. Approve or deny change request balancing functional needs with adequate security. (CCB) 6. Update all system documentation to reflect changes implemented in the system. (Program Office/System Owner, ISSO) 7. Use automated mechanisms to monitor configuration changes for high-impact systems that document proposed changes; notify appropriate approval authorities; highlight approvals that have not been received in a timely manner; and document completed changes to the information system. (Program Office/System Owner, ISSO) 8. Audit all activities associated with configuration changes in moderate- or high-impact systems. (Program Office/System Owner, IT Operations)

4.4.4 Monitor Configuration Changes

NIST SP 800-53 Control: CM-4
CM-4: The organization monitors changes to the information system and conducts security impact analyses to determine the effects of the changes.
Security Baseline: Moderate and High
Related HUD Policy: 4.4.4
Supporting Procedures
<ol style="list-style-type: none"> 1. Document system component changes as defined in the system configuration management plan. (Program Office/System Owner, ISSO) 2. Conduct a security impact analysis prior to the implementation of the change as required by NIST SP 800-37, <i>Guide to the Security Certification and Accreditation of Federal Information Systems</i>. (Program Office/System Owner, ISSO) 3. Initiate recertification activities, if a proposed change has a significant impact on the security of the system. (Program Office/System Owner, ISSO) 4. Verify that all security features are still functioning after a change has been implemented. (ISSO, System Administrator) 5. Audit all activities associated with configuration changes to the information systems. (ISSO, System Administrator)

4.4.5 Access Restrictions for Change

NIST SP 800-53 Control: CM-5
CM-5: The organization: (i) approves individual access privileges and enforces physical and logical access restrictions associated with changes to the information system; and (ii) generates, retains, and reviews records reflecting all such changes.
Security Baseline: Moderate and High
E-1: The organization employs automated mechanisms to enforce access restrictions and support auditing of the enforcement actions.
Security Baseline: High
Related HUD Policy: 4.4.5
Supporting Procedures
<ol style="list-style-type: none"> 1. Limit the personnel authorized to make changes to the information system based on their job responsibilities and approve individuals in writing that are authorized to make changes to the information system. (Program Office/System Owner, ISSO) 2. Review and update access restrictions based on changes in staff responsibilities, transfers, and terminations. (Program Office/System Owner, ISSO) 3. Use automated mechanisms to enforce access restrictions and support auditing for high-impact systems. (Program Office/System Owner, ISSO)

4.4.6 Configuration Settings

NIST SP 800-53 Control: CM-6
<p>CM-6: The organization: (i) establishes mandatory configuration settings for information technology products employed within the information system; (ii) configures the security settings of information technology products to the most restrictive mode consistent with operational requirements; (iii) documents the configuration settings; and (iv) enforces the configuration settings in all components of the information systems.</p>
<p>Security Baseline: Low, Moderate, and High</p>
<p>E-1: The organization employs automated mechanisms to centrally manage, apply, and verify configuration settings.</p>
<p>Security Baseline: High</p>
<p>Related HUD Policy: 4.4.6</p>
Supporting Procedures
<ol style="list-style-type: none"> 1. Configure the security settings for information technology products to meet the mandatory HUD configuration settings and to the most restrictive mode consistent with the system's operational requirements. (Program Offices/System Owners, ISSO, System Administrator) 2. Use automated mechanisms to manage, apply, and verify configuration settings for high-impact systems. (Program Office/System Owner, ISSO, System Administrator) 3. Document any deviations from the recommended configurations in the security plan. (Program Office/System Owner, ISSO)

4.4.7 Least Functionality

NIST SP 800-53 Control: CM-7
<p>CM-7: The organization configures the information system to provide only essential capabilities and specifically prohibits and/or restricts the use of the functions, ports, protocols, and/or services as identified by the Deputy CIO for IT Operations.</p>
<p>Security Baseline: Moderate and High</p>
<p>E-1: The organization reviews the information system to annually identify and eliminate unnecessary functions, ports, protocols, and/or services.</p>
<p>Security Baseline: High</p>
<p>Related HUD Policy: 4.4.7</p>
Supporting Procedures
<ol style="list-style-type: none"> 1. Configure the information system to provide only essential capabilities and prohibit any protocol or service not explicitly permitted at HUD. (System Administrator) 2. Review high-impact systems annually to identify and eliminate any unnecessary ports, protocols, or services. (Program Office/System Owner, ISSO)

4.4.8 Information System Component Inventory

NIST SP 800-53 Control: CM-8
<p>CM-8: The organization develops, documents, and maintains a current inventory of the components of the information system and relevant ownership information.</p> <p>Security Baseline: Low, Moderate, and High</p>
<p>E-1: The organization updates the inventory of information system components as an integral part of component installations.</p> <p>Security Baseline: Moderate and High</p>
<p>E-2: The organization employs automated mechanisms to maintain an up-to-date, complete, accurate, and readily available inventory of information system components.</p> <p>Security Baseline: High</p>
<p>Related HUD Policy: 4.4.8</p>
Supporting Procedures
<ol style="list-style-type: none"> 1. Inventory and document the information system components. (Program Office/System Owner, ISSO, OSEP, 2. Update the inventory during component installations for moderate- and high-impact systems. (Program Office/System Owner, ISSO, OSEP)

4.5 Maintenance

Regular maintenance of information systems mitigates some of the threats to the system. The maintenance control addresses policies and procedures to ensure that regular system maintenance and repairs occur.

FIPS 200 Requirement
<p>Organizations must: (i) perform periodic and timely maintenance on organizational information systems; and (ii) provide effective controls on the tools, techniques, mechanisms, and personnel used to conduct information system maintenance.</p>

4.5.1 System Maintenance Policy and Procedures

NIST SP 800-53 Control: MA-1
<p>MA-1: The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, information system maintenance policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the information system maintenance policy and associated system maintenance controls.</p> <p>Security Baseline: Low, Moderate, and High</p>
<p>Related HUD Policy: <i>Information Technology Security Policy, Handbook 2400.25, Rev. 1</i></p>

NIST SP 800-53 Control: MA-1
Implementation
This control is implemented by the <i>Information Technology Security Policy, Handbook 2400.25, Rev. 1</i> , which defines HUD's security policies. The procedures related to the HUD policies are in this document, <i>HUD Information Technology Security Procedures</i> .

4.5.2 Controlled Maintenance

NIST SP 800-53 Control: MA-2
MA-2: The organization schedules, performs, documents, and reviews records of routine preventative and regular maintenance (including repairs) on the components of the information system in accordance with manufacturer or vendor specifications and/or organizational requirements.
Security Baseline: Low, Moderate, and High
E-1: The organization maintains maintenance records for the information system that include: (i) the date and time of maintenance; (ii) name of the individual performing the maintenance; (iii) name of escort, if necessary; (iv) a description of the maintenance performed; and (v) a list of equipment removed or replaced (including identification numbers, if applicable).
Security Baseline: Moderate and High
E-2: The organization employs automated mechanisms to schedule and conduct maintenance as required, and to create up-to-date, accurate, complete, and available records of all maintenance actions, both needed and completed.
Security Baseline: High
Related HUD Policy: 4.5.2
Supporting Procedures
<ol style="list-style-type: none"> 1. Schedule, perform, and document routine preventative and regular maintenance on the components of the information system in accordance with manufacturer or vendor specifications and/or organizational requirements. (System Administrator) 2. Approve the removal of the information system or information system components from the facility when offsite repairs are necessary. (Program Office/System Owner, System Administrator) 3. Remove all information from associated media using approved procedures, if the information system or components requires offsite repair. (Program Office/System Owner, System Administrator) 4. Maintain maintenance records for moderate-and high-impact systems that includes the date and time of maintenance, name of the individual performing the maintenance, name of escort, if necessary, a description of the maintenance performed, and a list of equipment removed or replaced (including identification numbers, if applicable). For high-impact systems, use automated mechanisms to schedule, conduct, and document maintenance actions. (Program Office/System Owner, System Administrator) 5. Enable maintenance ports only during maintenance. (Program Office/System Owner, ISSO, System Administrator) 6. Check the security features to ensure the features are still functioning properly after maintenance is performed on the information system. (ISSO, System Administrator)

4.5.3 Maintenance Tools

NIST SP 800-53 Control: MA-3
<p>MA-3: The organization approves, controls, and monitors the use of information system maintenance tools and maintains the tools on an ongoing basis.</p> <p>Security Baseline: Moderate and High</p>
<p>E-1: The organization inspects all maintenance tools carried into a facility by maintenance personnel for obvious improper modifications.</p> <p>Security Baseline: High</p>
<p>E-2: The organization checks all media containing diagnostic and test programs for malicious code before the media are used in the information system.</p> <p>Security Baseline: High</p>
<p>E-3: The organization checks all maintenance equipment with the capability of retaining information so that no organizational information is written on the equipment or the equipment is appropriately sanitized before release; if the equipment cannot be sanitized, the equipment remains within the facility or is destroyed, unless an appropriate organization official explicitly authorizes an exception.</p> <p>Security Baseline: High</p>
<p>E-4: The organization employs automated mechanisms to restrict the use of maintenance tools to authorized personnel only.</p> <p>Security Baseline: N/A</p>
<p>Related HUD Policy: 4.5.3</p>
Supporting Procedures
<ol style="list-style-type: none"> 1. Approve all maintenance tools prior to using them on HUD systems. (Deputy CIO for IT Operations, Program Office/System Owner, System Administrator) 2. Inspect the maintenance tools for obvious improper modifications when the tools are used on high-impact systems. (Program Office/System Owner, System Administrator) 3. Maintain the maintenance tools regularly. (System Administrator) 4. Check all media containing diagnostic and test programs (e.g., software or firmware used for system maintenance or diagnostics) for malicious code before the media are used on high-impact systems. (System Administrator) 5. Verify all external maintenance equipment contains no HUD data and that it is properly sanitized prior to being removed from facilities housing HUD information systems when used on high-impact systems. Confiscate equipment used for testing if HUD data cannot be removed, unless the CISO authorizes an exception. (Program Office/System Owner, System Administrator)

4.5.4 Remote Maintenance

NIST SP 800-53 Control: MA-4
<p>MA-4: The organization authorizes, monitors, and controls remotely executed maintenance and diagnostic activities, if employed.</p> <p>Security Baseline: Low, Moderate, and High</p>

NIST SP 800-53 Control: MA-4
<p>E-1: The organization audits all remote maintenance and diagnostic sessions, and appropriate organizational personnel review the maintenance records of the remote sessions.</p> <p>Security Baseline: High</p>
<p>E-2: The organization addresses the installation and use of remote maintenance and diagnostic links in the security plan for the information system.</p> <p>Security Baseline: High</p>
<p>E-3: The organization does not allow remote maintenance or diagnostic services to be performed by a provider that does not implement for its own information system, a level of security at least as high as that implemented on the system being serviced, unless the component being serviced is removed from the information system and sanitized (with regard to organizational information) before the service begins and also sanitized (with regard to potentially malicious software) after the service is performed and before being reconnected to the information system.</p> <p>Security Baseline: High</p>
<p>Related HUD Policy: 4.5.4</p>
Supporting Procedures
<ol style="list-style-type: none"> 1. Document the use of remote diagnostic tools in the security plan for the information system. For high-impact systems, include information on the installation and use of remote diagnostic links in the security plan. (Program Office/System Owner, ISSO) 2. Maintain maintenance records for all remote maintenance, diagnostic, and service activities and review the logs periodically. (ISSO) 3. Implement techniques to improve security of remote maintenance based on an assessment of risk. These techniques can include encryption and decryption of diagnostic communications, strong identification and authentication techniques, such as Level 3 or 4 tokens as described in NIST SP 800-63, or remote disconnect verification. (Program Office/System Owner, ISSO) 4. Terminate all sessions and remote connections when remote maintenance is completed. Change passwords if used for authentication following each remote maintenance service session. (System Administrator) 5. Audit all remote maintenance sessions and review the records periodically. (Program Office/System Owner, ISSO) 6. Ensure diagnostic or maintenance services or organizations performing remote diagnostic or maintenance services on high-impact information systems, implement 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 an approved level of security, sanitize and physically separate the system from other information systems before connecting the remote access line. Deny remote maintenance if the information system cannot be sanitized due to a system failure. (Deputy CIO for IT Operations, Program Office/System Owner)

4.5.5 Maintenance Personnel

NIST SP 800-53 Control: MA-5
MA-5: The organization allows only authorized personnel to perform maintenance on the information system.
Security Baseline: Low, Moderate, and High
Related HUD Policy: 4.5.5
Supporting Procedures
<ol style="list-style-type: none"> 1. Permit only authorized personnel to perform maintenance on the information system. (Program Office/System Owner, System Administrator) 2. Document all individuals authorized to perform maintenance on high-impact information systems. (Deputy CIO for IT Operations, Program Office/System Owner, System Administrator) 3. Supervise maintenance personnel during the performance of maintenance activities on the information system when maintenance personnel do not have access to organizational information. The assigned supervisor must have access to organizational information. (Deputy CIO for IT Operations, Program Office/System Owner, System Administrator)

4.5.6 Timely Maintenance

NIST SP 800-53 Control: MA-6
MA-6: The organization obtains maintenance support and spare parts for critical components within 48 hours of failure.
Security Baseline: Moderate and High
Related HUD Policy: 4.5.6
Supporting Procedures
<ol style="list-style-type: none"> 1. Obtain maintenance support and spare parts within 48 hours of failure for critical components in moderate- and high-impact systems. (Deputy CIO for IT Operations, Program Office/System Owner, System Administrator)

4.6 System and Information Integrity

System and information integrity controls ensure that policies and procedures are implemented to protect information assets from malicious code as well as enable rapid identification, reporting and correction of information system flaws.

FIPS 200 Requirement
Organizations must: (i) identify, report, and correct information and information system flaws in a timely manner; (ii) provide protection from malicious code at appropriate locations within organizational information systems; and (iii) monitor information system security alerts and advisories and take appropriate actions in response.

4.6.1 System and Information Integrity Policy and Procedures

NIST SP 800-53 Control: SI-1
<p>SI-1: The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, system and information integrity policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the system and information integrity policy and associated system and information integrity controls.</p>
<p>Security Baseline: Low, Moderate, and High</p>
<p>Related HUD Policy: <i>Information Technology Security Policy, Handbook 2400.25, Rev. 1</i></p>
Implementation
<p>This control is implemented by the <i>Information Technology Security Policy, Handbook 2400.25, Rev. 1</i>, which defines HUD's security policies. The procedures related to the HUD policies are in this document, <i>HUD Information Technology Security Procedures</i>.</p>

4.6.2 Flaw Remediation

NIST SP 800-53 Control: SI-2
<p>SI-2: The organization identifies, reports, and corrects information system flaws.</p>
<p>Security Baseline: Low, Moderate, and High</p>
<p>E-1: The organization centrally manages the flaw remediation process and installs updates automatically.</p>
<p>Security Baseline: High</p>
<p>E-2: The organization employs automated mechanisms to periodically and upon demand determine the state of information system components with regard to flaw remediation.</p>
<p>Security Baseline: Moderate and High</p>
<p>Related HUD Policy: 4.6.2</p>

NIST SP 800-53 Control: SI-2
Supporting Procedures
<ol style="list-style-type: none"> 1. Review available published sources and alerts identifying software flaws. (IT Operations) 2. Test newly released security relevant patches, service packs, and hot fixes in a test environment following guidance in NIST SP 800-40, <i>Procedures for Handling Security Patches</i> and the <i>HUD Patch Management Policy and Network Security</i>. (IT Operations) 3. Determine if the new security release provides adequate protection to the HUD systems without introducing destructive side effects. (IT Operations) 4. Approve security relevant patches, service packs, or hot fixes for implementation in the HUD environment within the timeframe defined by the <i>HUD Patch Management Policy and Network Security</i> unless an exception has been requested. (IT Operations) 5. Install all updates that can be applied using automated mechanisms for moderate- and high-impact systems. (IT Operations) 6. Monitor HUD systems to valid that security releases have been installed effectively throughout HUD. (IT Operations) 7. Report flaws discovered during security assessments, continuous monitoring, or incident response activities to IT Operations. (Program Office/System Owner, ISSO, System Administrator) 8. Determine if the flaws identified during security assessments or monitoring impact the HUD enterprise and, if necessary, determine an appropriate solution, test the planned fix, and implement it throughout HUD using an automated mechanism in accordance with the <i>HUD Patch Management Policy and Network Security</i>. (IT Operations)

4.6.3 Malicious Code Protection

NIST SP 800-53 Control: SI-3
SI-3: The information system implements malicious code protection.
Security Baseline: Low, Moderate, and High
E-1: The organization centrally manages malicious code protection mechanisms.
Security Baseline: Moderate and High
E-2: The information system automatically updates malicious code protection mechanisms.
Security Baseline: Moderate and High
Related HUD Policy: 4.6.3

NIST SP 800-53 Control: SI-3
Supporting Procedures
<ol style="list-style-type: none"> 1. Use virus protection mechanisms at critical information system entry and exit points (e.g., electronic mail servers, web servers, proxy servers) and at workstations, servers, or mobile computing devices on the network. (OSEP, System Administrators) 2. Configure virus protection software to prevent users from disabling it or modifying configuration settings. (OSEP, System Administrators) 3. Configure the virus protection software to automatically check all files on access, download, and when emailing attachments. (OSEP, System Administrators) 4. Configure software to automatically forward antivirus generated alerts to HUD's intrusion detection system. (OSEP, System Administrators) 5. Update antivirus software and signature files automatically whenever new releases are available in accordance with HUD's configuration management policy and procedures. (CSIRC) 6. Eradicate any malicious code discovered. (System Administrator, Users)

4.6.4 Information System Monitoring Tools and Techniques

NIST SP 800-53 Control: SI-4
<p>SI-4: The organization employs tools and techniques to monitor events on the information system, detect attacks, and provide identification of unauthorized use of the system.</p> <p>Security Baseline: Moderate and High</p>
<p>E-1: The organization interconnects and configures individual intrusion detection tools into a system-wide intrusion detection system using common protocols.</p> <p>Security Baseline: N/A</p>
<p>E-2: The organization employs automated tools to support near real-time analysis of events.</p> <p>Security Baseline: High</p>
<p>E-3: The organization employs automated tools to integrate intrusion detection tools into access control and flow control mechanisms for rapid response to attacks by enabling reconfiguration of these mechanisms in support of attack isolation and elimination.</p> <p>Security Baseline: N/A</p>
<p>E-4: The information system monitors inbound and outbound communications for unusual or unauthorized activities or conditions.</p> <p>Security Baseline: Moderate and High</p>
<p>E-5: The information system provides a real time alert when the following indications of compromise or potential compromise occur:</p> <ul style="list-style-type: none"> • Access to selected privileged files of applications • Activities inconsistent with the typical user's profile or pattern of use <p>Security Baseline: High</p>
<p>Related HUD Policy: 4.6.4</p>

NIST SP 800-53 Control: SI-4
Supporting Procedures
<ol style="list-style-type: none"> 1. Use automated tools and techniques to monitor moderate- and high-impact HUD information systems to detect attacks and provide identification of unauthorized use of the system. Monitor inbound and outbound communications for unusual or unauthorized activities or conditions. (CSIRC, System Administrator) 2. Provide a real time alert when the following events occur: (CSIRC, System Administrator) <ul style="list-style-type: none"> • Access to selected privileged files of applications • Activities inconsistent with the typical user's profile or pattern of use

4.6.5 Security Alerts and Advisories

NIST SP 800-53 Control: SI-5
<p>SI-5: The organization receives information system security alerts/advisories on a regular basis, issues alerts/advisories to appropriate personnel, and takes appropriate actions in response.</p> <p>Security Baseline: Low, Moderate, and High</p>
<p>E-1: The organization employs automated mechanisms to make security alerts and advisory information available throughout the organization as needed.</p> <p>Security Baseline: N/A</p>
<p>Related HUD Policy: 4.6.5</p>
Supporting Procedures
<ol style="list-style-type: none"> 1. Receive and review daily information system security alerts/advisories from reliable sources. (CSIRC) 2. Analyze the alert and document the appropriate action to take for the security alert. (CSIRC) 3. Forward appropriate alerts to all HUD employees and contractors using HUD resources. (CSIRC)

4.6.6 Security Functionality Verification

NIST SP 800-53 Control: SI-6
<p>SI-6. The information system verifies the correct operation of security functions upon system startup and restart and restarts the system when anomalies are discovered.</p> <p>Security Baseline: High</p>
<p>E-1: The organization employs automated mechanisms to provide notification of failed automated security tests.</p> <p>Security Baseline: N/A</p>
<p>E-2: The organization employs automated mechanisms to support management of distributed security testing.</p> <p>Security Baseline: N/A</p>
<p>Related HUD Policy: 4.6.6</p>

NIST SP 800-53 Control: SI-6
Supporting Procedures
<ol style="list-style-type: none"> 1. Configure the information system to verify the correct operation of security features at system startup and restart. (System Administrator) 2. Restart high-impact systems when anomalies are discovered. (System Administrator)

4.6.7 Software and Information Integrity

NIST SP 800-53 Control: SI-7
<p>SI-7: The information system detects and protects against unauthorized changes to software and information.</p> <p>Security Baseline: High</p>
<p>E-1: The organization reassesses the integrity of software and information by performing monthly integrity scans of the system.</p> <p>Security Baseline: High</p>
<p>E-2: The organization employs automated tools that provide notification to appropriate individuals upon discovering discrepancies during integrity verification.</p> <p>Security Baseline: High</p>
<p>E-3: The organization employs centrally managed integrity verification tools</p> <p>Security Baseline: N/A</p>
<p>Related HUD Policy: 4.6.7</p>
Supporting Procedures
<ol style="list-style-type: none"> 1. Implement integrity verification applications on high-impact information systems to look for evidence of information tampering, errors, and omissions. (Developers) 2. Implement good software engineering practices (e.g., parity checks, cyclical redundancy checks, cryptographic hashes) and use tools to automatically monitor the integrity of high-impact systems. (Developers)

4.6.8 Spam Protection

NIST SP 800-53 Control: SI-8
<p>SI-8: The information system implements spam protection.</p> <p>Security Baseline: Moderate and High</p>
<p>E-1: The organization centrally manages spam protection mechanisms.</p> <p>Security Baseline: High</p>
<p>E-2: The information system automatically updates spam protection mechanisms.</p> <p>Security Baseline: N/A</p>

NIST SP 800-53 Control: SI-8
Related HUD Policy: 4.6.8
Supporting Procedures
<ol style="list-style-type: none"> 1. Use spam and spyware mechanisms at critical information system entry points (e.g., email servers, web servers, proxy servers) and at workstations, servers, or mobile computing devices on the network. (System Administrator, ISSO, Users) 2. Detect and take appropriate action on unsolicited messages and spyware/adware transported by email, email attachments, Internet accesses, removable media, or other common means. (System Administrator) 3. Report serious problems following the CSIRC guidance. (Users)

4.6.9 Information Input Restrictions

NIST SP 800-53 Control: SI-9
SI-9: The organization restricts the capability to input information to the information system to authorized personnel.
Security Baseline: Moderate and High
Related HUD Policy: 4.6.9
Supporting Procedures
<ol style="list-style-type: none"> 1. Determine if restrictions on personnel authorized to provide input to the information system extends beyond the typical access controls employed by moderate- and high-impact systems. (Program Office/System Owner, ISSO) 2. Implement, if appropriate, restrictions to the information system based on specific operational or project responsibilities. (Program Office/System Owner, ISSO)

4.6.10 Information Accuracy, Completeness, Validity, and Authenticity

NIST SP 800-53 Control: SI-10
SI-10: The information system checks information for accuracy, completeness, validity, and authenticity.
Security Baseline: Moderate and High
Related HUD Policy: 4.6.10
Supporting Procedures
<ol style="list-style-type: none"> 1. Check moderate- and high-impact systems for accuracy, completeness, and validity as close to the point of origin as possible. (Developer) 2. Check valid syntax of information system inputs of moderate- and high-impact systems to ensure that inputs match specific definitions for format and content (e.g., character set, length, numerical range, acceptable values). (Developer)

4.6.11 Error Handling

NIST SP 800-53 Control: SI-11
SI-11. The information system identifies and handles error conditions in an expeditious manner without providing information that could be exploited by adversaries.
Security Baseline: Moderate and High
Related HUD Policy: 4.6.11
Supporting Procedures
<ol style="list-style-type: none"> 1. Generate error messages in moderate- and high-impact systems that provide timely and useful information to users without revealing information that could be exploited by adversaries. (Developer) 2. Restrict error messages to authorized personnel only (e.g., system administrators, maintenance personnel). (Developer) 3. Ensure that sensitive information is not listed in error logs or associated administrative messages. (Developer)

4.6.12 Information Output Handling and Retention

NIST SP 800-53 Control: SI-12
SI-12: The organization handles and retains output from the information system in accordance with application laws, directives, policies, regulations, standards, and operational requirements.
Security Baseline: Moderate and High
Related HUD Policy: 4.6.12
Supporting Procedures
<ol style="list-style-type: none"> 1. Determine and document in the security plan requirements for output handling including retention time for moderate- and high-impact information systems. (Program Office/System Owner, ISSO) 2. Handle information system output according to the approved procedures in the security plan. (Program Office/System Owner, ISSO, User) 3. Retain and dispose of information system output according to the approved procedures in the security plan. (Program Office/System Owner, ISSO, Users)

4.7 Media Protection

Information resides in many forms and can be stored in different ways. Media controls are protective measures specifically designed to safeguard electronic data and hardcopy information. These procedures addresses the protection, marking, sanitization, production input/output, and disposal of media containing sensitive information.

FIPS 200 Requirement
Organizations must: (i) protect information contained in organizational information systems in printed form or on digital media; (ii) limit access to information in printed form or on digital media removed from organizational information systems to authorized users; and (iii) sanitize or destroy digital media before disposal or release for reuse.

4.7.1 Media Protection Policy and Procedures

NIST SP 800-53 Control: MP-1
<p>MP-1: The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, media protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the media protection policy and associated media protection controls.</p>
<p>Security Baseline: Low, Moderate, and High</p>
<p>Related HUD Policy: <i>Information Technology Security Policy, Handbook 2400.25, Rev. 1</i></p>
Implementation
<p>This control is implemented by the <i>Information Technology Security Policy, Handbook 2400.25, Rev. 1</i>, which defines HUD's security policies. The procedures related to the HUD policies are in this document, <i>HUD Information Technology Security Procedures, Handbook, Rev. 1</i>.</p>

4.7.2 Media Access

NIST SP 800-53 Control: MP-2
<p>MP-2: The organization restricts access to information system media to authorized individuals.</p>
<p>Security Baseline: Low, Moderate, and High</p>
<p>(E-1): The organization employs automated mechanisms to restrict access to media storage areas and to audit access attempts and access granted.</p>
<p>Security Baseline: High</p>
<p>Related HUD Policy: 4.7.2</p>
Supporting Procedures
<ol style="list-style-type: none"> 1. Protect, and eventually dispose of, documents and electronic media according to the sensitivity marking defined in HUD guidelines. (ISSO, System Administrator, Users) 2. Restrict access to media storage areas through automated mechanisms or a guard station for high-impact systems. (Program Office/System Owner, OSEP) 3. Audit all access and access attempts to gain entry to the media storage area for high-impact systems. (Program Office/System Owner, OSEP)

4.7.3 Media Labeling

NIST SP 800-53 Control: MP-3
<p>MP-3: The organization: (i) affixes external labels to removable information system media and information system output indicating the distribution limitations, handling caveats and applicable security markings (if any) of the information; and (ii) exempts the media types of hardware components designated by the Deputy CIO for IT Operations from labeling so long as they remain within an environment designated by the Deputy CIO for IT Operations.</p>
<p>Security Baseline: High</p>

NIST SP 800-53 Control: MP-3
Related HUD Policy: 4.7.3
Supporting Procedures
<ol style="list-style-type: none"> 1. Mark printed output containing sensitive information according to HUD guidelines. (Users) 2. Place a cover sheet on any printed output without a marking. (System Administrators, Users) 3. Label all removable information system media with external labels that identify distribution limitations, handling caveats, and applicable security markings, if any. (Users) 4. Implement an automated marking mechanism for high-impact systems. (Deputy CIO for IT Operations)

4.7.4 Media Storage

NIST SP 800-53 Control: MP-4
MP-4: The organization physically controls and securely stores information system media, within controlled areas.
Security Baseline: Moderate and High
Related HUD Policy: 4.7.4
Supporting Procedures
<ol style="list-style-type: none"> 1. Label media with the FIPS 199 security category for the information system. (Developers, Users) 2. Protect information system media, both printed output and digital, based on the FIPS 199 security category of the information system until the media are destroyed or sanitized. (Program Office/System Owner, ISSO, Users) 3. Protect any unmarked media until it is reviewed and appropriately labeled. (Program Office/System Owner, ISSO, Users) 4. Store in a locked canister or encrypt the media from high-impact systems prior to removal from the primary storage sites. (Program Office/System Owner, ISSO) 5. Secure unattended laptops in offices via a locking cable, locked office, or a locked cabinet or desk. (Program Office/System Owner, ISSO, User)

4.7.5 Media Transport

NIST SP 800-53 Control: MP-5
MP-5: The organization protects and controls information system media during transport outside of controlled areas and restricts the activities associated with transport of such media to authorized personnel.
Security Baseline: Moderate and High
E-1: The organization protects digital and non-digital media during transport outside of controlled areas using methods approved by the Deputy CIO for IT Operations.
Security Baseline: Moderate and High

NIST SP 800-53 Control: MP-5
E-2: The organization documents, where appropriate, activities associated with the transport of information system media using methods approved by the Deputy CIO for IT Operations.
Security Baseline: Moderate and High
E-3: The organization employs an identified custodian at all times to transport information system media.
Security Baseline: High
Related HUD Policy: 4.7.5
Supporting Procedures
<ol style="list-style-type: none"> 1. Protect the information on digital and non-digital media from moderate- or high-impact systems during transport. (Program Office/System Owner, System Administrator) 2. Restrict pickup, receipt, transfer, or delivery of media, both digital and non-digital, to authorized personnel based on the marking restrictions. (Users) 3. Assign a custodian to transport media from high-impact systems with a formal handoff of responsibilities between custodians. (Program Office/System Owner, ISSO) 4. Maintain records to document pickup, receipt, transfer, and delivery activities associated with the transport of the information system media. (Program Office/System Owner, ISSO)

4.7.6 Media Sanitization and Disposal

NIST SP 800-53 Control: MP-6
MP-6: The organization: (i) sanitizes information system media, both digital and non-digital, prior to disposal or release for reuse; (ii) tracks, documents, and verifies media sanitization actions; and (iii) periodically tests sanitization equipment and procedures to ensure correct performance.
Security Baseline: Low, Moderate, and High
E-1: The organization tracks, documents, and verifies media sanitation and disposal actions.
Security Baseline: High
E-2: The organization periodically tests sanitization equipment and procedures to verify correct performance.
Security Baseline: High
Related HUD Policy: 4.7.6
Supporting Procedures
<ol style="list-style-type: none"> 1. Sanitize information system digital media, including removing all labels, markings, and activity logs using approved equipment, techniques, and procedures in accordance with the guidance in NIST SP 800-88, <i>Guidelines for Media Sanitation</i>. (ISSO, System Administrator) 2. Maintain records that track, document, and verify that media sanitization has occurred. (ISSO, System Administrator) 3. Test the sanitization equipment and procedures periodically to ensure correct performance. (ISSO, System Administrator)

4.8 Incident Response

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. Incident response relates to action taken in reaction to an incident occurrence.

The following procedures ensure that there are mechanisms in place to address the ability to respond to events in the network environment.

FIPS 200 Requirement
Organizations must: (i) establish an operational incident handling capability for organizational information systems that includes adequate preparation, detection, analysis, containment, recovery, and user response activities; and (ii) track, document, and report incidents to appropriate organizational officials and/or authorities.

4.8.1 Incident Response Policy and Procedures

NIST SP 800-53 Control: IR-1
IR-1: The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, incident response policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the incident response policy and associated incident response controls.
Security Baseline: Low, Moderate, and High
Related HUD Policy: <i>Information Technology Security Policy, Handbook 2400.25, Rev. 1</i>
Implementation
This control is implemented by the <i>Information Technology Security Policy, Handbook 2400.25, Rev. 1</i> , which defines HUD's security policies. The procedures related to the HUD policies are in this document, <i>HUD Information Technology Security Procedures</i> .

4.8.2 Incident Response Training

NIST SP 800-53 Control: IR-2
IR-2. The organization trains personnel in their incident response roles and responsibilities with respect to the information system and provides refresher training annually.
Security Baseline: Moderate and High
E-1: The organization incorporates simulated events into incident response training to facilitate effective response by personnel in crisis situations.
Security Baseline: High
E-2: The organization employs automated mechanisms to provide a more thorough and realistic training environment.
Security Baseline: N/A

NIST SP 800-53 Control: IR-2
Related HUD Policy: 4.8.2
Supporting Procedures
<ol style="list-style-type: none"> 1. Prepare an incident response training program based on guidance in NIST SP 800-61, <i>Computer Security Incident Handling Guide</i>. (CSIRC) 2. Train personnel on the CSIRC policies and procedures at orientation, when changes in guidance occur, and annually by May 31 of each year. (Program Office/System Owner, CSIRC) 3. Simulate actual incidents/events using automated mechanisms during training of incident response technical personnel for high-impact systems. (Program Office/System Owner, CSIRC)

4.8.3 Incident Response Testing and Exercises

NIST SP 800-53 Control: IR-3
IR-3: The organization tests and/or exercises the incident response capability for the information system annually using OITS-defined tests or exercises to determine the incident response effectiveness and documents the results.
Security Baseline: Moderate and High
E-1: The organization employs automated mechanisms to more thoroughly and effectively test the incident response.
Security Baseline: High
Related HUD Policy: 4.8.3
Supporting Procedures
<ol style="list-style-type: none"> 1. Prepare tests and exercises based on guidance found in NIST SP 800-61, <i>Computer Security Incident Handling Guide</i>. (OITS) 2. Test the incident response capability for moderate- and high-impact systems annually using automated mechanisms for high-impact systems. (CSIRC, OITS) 3. Record the results of the test and exercises noting any positive actions taken, problems, issues, and corrective measures. (OITS) 4. Update the incident response plan with lessons learned during the tests. (CSIRC) 5. Correct issues and problems identified during the test and exercises. (CSIRC)

4.8.4 Incident Handling

NIST SP 800-53 Control: IR-4
IR-4: The organization implements an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery.
Security Baseline: Low, Moderate, and High
E-1: The organization employs automated mechanisms to support the incident handling process.
Security Baseline: Moderate and High
Related HUD Policy: 4.8.4

NIST SP 800-53 Control: IR-4
Supporting Procedures
<ol style="list-style-type: none"> 1. Prepare HUD CSIRC guidance following the guidance in NIST SP 800-61, <i>Computer Security Incident Handling Guide</i> (e.g., team structure and staffing, techniques for handling specific types of incidents, communication plan). (CSIRC) 2. Detect and analyze security incidents. Use automated mechanism to support incident handling for moderate- and high-impact systems. (CSIRC, ISSO, System Administrator) 3. Contain, eradicate, and recover from incidents following the processes outlined in the CSIRC guidance. (CSIRC, ISSO, System Administrator) 4. Update HUD incident response guidance based on lessons learned during incidents. (CSIRC)

4.8.5 Incident Monitoring

NIST SP 800-53 Control: IR-5
IR-5: The organization tracks and documents information system security incidents on an ongoing basis.
Security Baseline: Moderate and High
E-1: The organization employs automated mechanisms to assist in the tracking of security incidents and in the collection and analysis of incident information.
Security Baseline: High
Related HUD Policy: 4.8.5
Supporting Procedures
<ol style="list-style-type: none"> 1. Track and document all information security incidents for moderate- and high-impact systems using automated analysis mechanisms for high-impact systems. (CSIRC, ISSO, System Administrator)

4.8.6 Incident Reporting

NIST SP 800-53 Control: IR-6
IR-6: The organization promptly reports incident information to appropriate authorities.
Security Baseline: Low, Moderate, and High
E-1: The organization employs automated mechanisms to assist in the reporting of security incidents.
Security Baseline: Moderate and High
Related HUD Policy: 4.8.6

NIST SP 800-53 Control: IR-6
Supporting Procedures
<ol style="list-style-type: none"> 1. Report security incidents following HUD CSIRC guidance. (Users) 2. Report all security incidents in a Weekly Incident Report after the incidents have been validated. Include in the report the number of incidents following the categories required for FISMA reporting. The categories include unauthorized access, denial of service, malicious code, improper usage, and other types of high priority incidents as defined in the HUD CSIRC guidance. (CSIRC) 3. Report significant computer security incidents to appropriate authorities (e.g., USCERT, using automated mechanisms to assist in the reporting of security incidents for moderate- or high-impact systems after identification and validation of the incident occurrence. (CSIRC) 4. Prepare an annual report on security incidents to meet FISMA reporting requirements. (CSIRC, OITS)

4.8.7 Incident Response Assistance

NIST SP 800-53 Control: IR-7
<p>IR-7: The organization provides an incident support resource that offers advice and assistance to users of the information system for the handling and reporting of security incidents. The support resource is an integral part of the organization’s incident response capability.</p> <p>Security Baseline: Low, Moderate, and High</p>
<p>E-1: The organization employs automated mechanisms to increase the availability of incident response-related information and support.</p> <p>Security Baseline: Moderate and High</p>
<p>Related HUD Policy: 4.8.7</p>
Supporting Procedures
<ol style="list-style-type: none"> 1. Integrate incident reporting assistance into current help desk functions. (CSIRC) 2. Coordinate access to forensics services with the Office of the Inspector General (OIG), when required. (CSIRC, OIG) 3. Provide automated means for obtaining incident response-related information and support for moderate- and high-impact systems. (CSIRC) 4. Provide feedback to ISSOs on incidents to help prevent reoccurrence. (CSIRC)

4.9 Awareness and Training

Each organization is required to provide users and personnel with significant security responsibilities for a system to be made aware of the security risks associated with their use and management of that system.

This control ensures that mechanisms are in place to verify and track security awareness and training associated with the use and operation of HUD information systems.

FIPS 200 Requirement
Organizations must: (i) ensure that managers and users of organizational information systems are made aware of the security risks associated with their activities and of the applicable laws, Executive Orders, directives, policies, standards, instructions, regulations, or procedures related to the security of organizational information systems; and (ii) ensure that organizational personnel are adequately trained to carry out their assigned information security-related duties and responsibilities.

4.9.1 Security Awareness and Training Policy and Procedures

NIST SP 800-53 Control: AT-1
AT-1: The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, security awareness and training policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the security awareness and training policy and associated security awareness and training controls.
Security Baseline: Low, Moderate, and High
Related HUD Policy: <i>Information Technology Security Policy, Handbook 2400.25, Rev. 1</i>
Implementation
This control is implemented by the <i>Information Technology Security Policy, Handbook 2400.25, Rev. 1</i> , which defines HUD's security policies. The procedures related to the HUD policies are in this document, <i>HUD Information Technology Security Procedures</i> .

4.9.2 Security Awareness

NIST SP 800-53 Control: AT-2
AT-2: The organization provides basic security awareness training to all information system users (including managers and senior executives) before authorizing access to the system, when required by system changes, at new employees' orientation, and annually by May 31 of each year thereafter.
Security Baseline: Low, Moderate, and High
Related HUD Policy: 4.9.2

NIST SP 800-53 Control: AT-2
Supporting Procedures
<ol style="list-style-type: none"> 1. Maintain the HUD enterprise-level security awareness training program following the guidance in NIST SP 800-50, <i>Building an Information Technology Security Awareness and Training Program</i> and the requirements in 5 CFR. Part 930.301. (OITS) 2. Provide initial security awareness training to all HUD employees and contractors who have access to HUD information at the HUD orientation or prior to granting access to any HUD systems. (Program Office/System Owner) 3. Provide system-specific security awareness training annually, or when required by system changes. Update the training material annually or as required. (OITS, Program Office/System Owner, ISSO) 4. Provide annual security awareness refresher training, which includes enterprise and system-specific training, to all HUD employees and contractors prior to May 31 of each year. (Program Office/System Owner, ISSO) 5. Request a waiver to exempt a HUD employee or contractor from the annual security awareness training only in limited circumstances. (Program Office/System Owner) 6. Review the waiver request and approve or deny it, providing a written response to the requesting organization. (OITS) 7. Revoke user account and access privileges from HUD employees or contractors who have not received annual awareness training and have not received a waiver. (Program Office/System Owner, ISSO, System Administrator)

4.9.3 Security Training

NIST SP 800-53 Control: AT-3
<p>AT-3: The organization identifies personnel that have significant information system security roles and responsibilities during the system development life cycle, documents those roles and responsibilities, and provides appropriate information system security training: (i) before authorizing access to the system or performing assigned duties; (ii) when required by system changes; and (iii) annually thereafter.</p>
<p>Security Baseline: Low, Moderate, and High</p>
<p>Related HUD Policy: 4.9.3</p>
Supporting Procedures
<ol style="list-style-type: none"> 1. Document specific HUD roles with significant security responsibilities and define the security training required to fulfill those roles in accordance with the requirements contained in 5 CFR Part 930.301 and NIST SP 800-50, <i>Building an Information Technology Security Awareness and Training Program</i>. (OITS) 2. Identify HUD employees or contractors with significant system security roles and responsibilities. (Program Office/System Owner) 3. Prepare an Information Security Professional Training Plan following HUD guidance to address specific training needs of identified personnel. (Program Office/System Owner, Users with significant security responsibilities) 4. Submit the Training Plan to the CISO by September 1 of each year. (Program Office/System Owner)

4.9.4 Security Training Records

NIST SP 800-53 Control: AT-4
AT-4: The organization documents and monitors individual information system security training activities, including basic security awareness training and specific information system security training.
Security Baseline: Low, Moderate, and High
Related HUD Policy: 4.9.4
Supporting Procedures
<ol style="list-style-type: none"> 1. Provide a standard report format or tool to document and monitor the annual security awareness training and security role-based training. (OITS) 2. Maintain records of all employees/contractors receiving security awareness and role-based security training. Include the individual's name and position, types of training received, and the cost of the training. (Program Office/System Owner) 3. Report the training activity statistics semi-annually to the CISO on December 15 and June 15 of each year and as part of the annual FISMA reporting process. (Program Offices)

4.9.5 Contacts with Security Groups and Associations

NIST SP 800-53 Control: AT-5
AT-5: The organization establishes and maintains contacts with special interest groups, specialized forums, professional associations, news groups, and/or peer groups of security professionals in similar organizations to stay up-to-date with the latest recommended security practices, techniques, and technologies and to share the latest security-related information including threats, vulnerabilities, and incidents.
Security Baseline: N/A
Related HUD Policy: None
Supporting Procedures
<p>In selected:</p> <ol style="list-style-type: none"> 1. Join and maintain contacts with security special interest groups, forums, professional associations, news groups, and/or peer groups of security professionals in similar organizations. Select groups in keeping with the HUD's mission requirements. (OITS, IT Operations, ISSO)

5.0 Technical Procedures

Technical controls are the security controls (i.e., safeguards or countermeasures) for an information system that are primarily implemented and executed by the information system through mechanisms contained in the information system’s hardware, software, or firmware components. The procedures in this section provide guidance on how to implement technical controls and HUD security requirements.

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.

The following procedures ensures that there is a mechanism in place to associate user and system activity to the credentials used.

FIPS 200 Requirement
Organizations must identify information system users, processes acting on behalf of users, or devices and authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.

5.1.1 Identification and Authentication Policy and Procedures

NIST SP 800-53 Control: IA-1
IA-1: The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, identification and authentication policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the identification and authentication policy and associated identification and authentication controls.
Security Baseline: Low, Moderate, and High
Related HUD Policy: <i>Information Technology Security Policy, Handbook 2400.25, Rev. 1</i>
Implementation
This control is implemented by the <i>Information Technology Security Policy, Handbook 2400.25, Rev. 1</i> , which defines HUD’s security policies. The procedures related to the HUD policies are in this document, <i>HUD Information Technology Security Procedures</i> .

5.1.2 User Identification and Authentication

NIST SP 800-53 Control: IA-2
IA-2: The information system uniquely identifies and authenticates users (or processes acting on behalf of users).
Security Baseline: Low, Moderate, and High

NIST SP 800-53 Control: IA-2
<p>E-1: The information system employs multifactor authentication for remote system access that is NIST SP 800-63 level 3 compliant.</p> <p>Security Baseline: Moderate</p>
<p>E-2: The information system employs multifactor authentication for local system access that is NIST SP 800-63 level 3 compliant.</p> <p>Security Baseline: High</p>
<p>E-3: The information system employs multifactor authentication for remote system access that is NIST SP 800-63 level 4 compliant.</p> <p>Security Baseline: High</p>
<p>Related HUD Policy: 5.1.2</p>
Supporting Procedures
<ol style="list-style-type: none"> 1. Select an appropriate method to authenticate a user's identity prior to granting access to HUD systems. Appropriate methods include passwords, tokens, or biometrics. (Program Office/System Owner, Authorizing Official) 2. Select a combination of authentication techniques for high-impact systems. (Program Office/System Owner, Authorizing Official) 3. Ensure personal identity verification (PIV) credentials conform to the specifications in FIPS 201, <i>Personal Identity Verification for Federal Employees and Contractors</i>, NIST SP 800-73, <i>Interfaces for Personal Identity Verification</i>, and NIST SP 800-76, <i>Biometric Data Specifications for Personal Identity Verification</i> and NIST SP 800-78, <i>Cryptographic Standards and Key Sizes for Personal Identity Verification</i>. (Deputy CIO for IT Operations, OITS)

5.1.3 Device Identification and Authentication

NIST SP 800-53 Control: IA-3
<p>IA-3: The information system identifies and authenticates specific devices before establishing a connection.</p> <p>Security Baseline: Moderate and High</p>
<p>Related HUD Policy: 5.1.3</p>
Supporting Procedures
<ol style="list-style-type: none"> 1. Select an approved solution to identify and authenticate devices on local or wide area networks from the HUD Enterprise Architecture TRM. (OITS, Program Office/System Owner, ISSO)

5.1.4 Identifier Management

NIST SP 800-53 Control: IA-4
<p>IA-4: The organization manages user identifiers by: (i) uniquely identifying each user; (ii) verifying the identity of each user; (iii) receiving authorization to issue a user identifier from an appropriate organization official; (iv) issuing the user identifier to the intended party; (v) disabling the user identifier after no more than 90 days of inactivity; and (vi) archiving user identifiers.</p>
<p>Security Baseline: Low, Moderate, and High</p>
<p>Related HUD Policy: 5.1.4</p>
Supporting Procedures
<ol style="list-style-type: none"> 1. Approve a user's request for access to HUD systems. (Program Office/System Owner, Supervisor) 2. Assign a unique user identifier and password or authentication device to each approved user. (ISSO, System Administrator) 3. Validate that the appropriate person receives the identification and authentication information or device. (ISSO) 4. Protect any identification and authentication materials. Do not share these materials. (Users) 5. Disable user identification after 90 days of inactivity. (ISSO, System Administrator)

5.1.5 Authentication Management

NIST SP 800-53 Control: IA-5
<p>IA-5: The organization manages information system authenticators by: (i) defining initial authenticator content; (ii) establishing administrative procedures for initial authenticator distribution, for lost/compromised, or damaged authenticators, and for revoking authenticators; (iii) changing default authenticators upon information system installation; and (iv) changing/refreshing authenticators periodically.</p>
<p>Security Baseline: Low, Moderate, and High</p>
<p>Related HUD Policy: 5.1.5</p>

NIST SP 800-53 Control: IA-5
Supporting Procedures
<p>For password-based authentication:</p> <ol style="list-style-type: none"> 1. Develop administrative procedures for initial password distribution, for lost/compromised passwords, and for revoking passwords. (ISSO, System Administrator) 2. Configure the system to enforce the policies listed below. If the system cannot enforce the policies, develop administrative procedures to provide equivalent security. (Program Office/System Owner, ISSO, System Administrator) <ul style="list-style-type: none"> • Do not display passwords when entered • Protect passwords from unauthorized disclosure and modification when stored or transmitted • Disallow users from reusing a password for at least eight iterations • Require users to change their passwords at least every 90 days • Require strong passwords as defined in the HUD policy 3. Restrict the use of group passwords to circumstances where operational needs require them. Obtain approval from the appropriate authorizing official prior to implementing the group password. (Program Office/System Owner, ISSO) 4. Replace all default or factory-set administrator passwords provided by vendors. (System Administrator) <p>For PKI-based authentication:</p> <ol style="list-style-type: none"> 1. Develop administrative procedures for distributing PKI certificates, lost, or compromised certificates, and for revoking certificates based on the guidance in FIPS 201, <i>Personal Identity Verification for Federal Employees and Contractors</i>, NIST SP 800-73, <i>Interfaces for Personal Identity Verification</i>, NIST SP 800-76, <i>Biometric Data Specifications for Personal Identity Verification</i> and NIST SP 800-78, <i>Cryptographic Standards and Key Sizes for Personal Identity Verification</i>. (Program Office/System Owner, ISSO) 2. Include guidance from NIST SP 800-63, <i>Electronic Authentication Guideline</i>, if the application provides an e-government service. (Program Office/System Owner, ISSO)

5.1.6 Authentication Feedback

NIST SP 800-53 Control: IA-6
<p>IA-6: The information system obscures feedback of authentication information during the authentication process to protect the information from possible exploitation/use by unauthorized individuals .</p>
<p>Security Baseline: Low, Moderate, and High</p>
<p>Related HUD Policy: 5.1.6</p>
Supporting Procedures
<ol style="list-style-type: none"> 1. Provide feedback to a user on the success or failure of attempted authentication. (Developer, System Administrator) 2. Design the system to mask or obscure authentication information during the authentication process. (Developer, System Administrator)

5.1.7 Cryptographic Module Authentication

NIST SP 800-53 Control: IA-7
<p>IA-7: The information system employs authentication methods that meet the requirements of applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance for authentication to a cryptographic module.</p>
<p>Security Baseline: Low, Moderate, and High</p>
<p>Related HUD Policy: 5.1.7</p>
Supporting Procedures
<ol style="list-style-type: none"> 1. Assess the HUD moderate- and high-impact systems to determine if the services listed below are provided. Select an appropriate encryption method if these services are provided. (Program Office/System Owner, ISSO) <ul style="list-style-type: none"> • Remote access • Wireless access • Cryptographic module authentication • Transmission integrity and confidentiality 2. Select a HUD approved method to encrypt sensitive information. (Program Office/System Owner) HUD approved encryption methods include: <ul style="list-style-type: none"> • 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, <i>Security Requirements for Cryptographic Modules</i> (as amended). All new systems should use AES. • 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 3. Validate that the cryptographic key establishment and management is done in accordance with NIST SP 800-56, <i>Recommendation on Key Establishment Schemes</i>, and NIST SP 800-57, <i>Recommendation on Key Management</i>. (Program Office/System Owner/ISSO)

5.2 Access Control

Access control addresses user authorization to utilize an information system. It also addresses the processes and types of transactions that are allowed. The following procedures ensure that there are limitations on who can access a system and the mechanisms for verifying a users needs to access the system.

FIPS 200 Requirement
<p>Organizations must limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems) and to the types of transactions and functions that authorized users are permitted to exercise.</p>

5.2.1 Access Control Policy and Procedures

NIST SP 800-53 Control: AC-1
<p>AC-1: The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the access control policy and associated access controls.</p>
<p>Security Baseline: Low, Moderate, and High</p>
<p>Related HUD Policy: <i>Information Technology Security Policy, Handbook 2400.25, Rev. 1</i></p>
Implementation
<p>This control is implemented by the <i>Information Technology Security Policy, Handbook 2400.25, Rev. 1</i>, which defines HUD's security policies. The procedures related to the HUD policies are in this document, <i>HUD Information Technology Security Procedures</i>.</p>

5.2.2 Account Management

NIST SP 800-53 Control: AC-2
<p>AC-2: The organization manages information system accounts, including establishing, activating, modifying, reviewing, disabling, and removing accounts. The organization reviews information system accounts annually.</p>
<p>Security Baseline: Low, Moderate, and High</p>
<p>E-1: The organization employs automated mechanisms to support the management of information system accounts.</p>
<p>Security Baseline: Moderate and High</p>
<p>E-2: The information system automatically terminates temporary and emergency accounts after 48 hours.</p>
<p>Security Baseline: Moderate and High</p>
<p>E-3: The information system automatically disables inactive accounts after 90 days.</p>
<p>Security Baseline: Moderate and High</p>
<p>E-4: The organization employs automated mechanisms to audit account creation, modification, disabling, and termination actions and notify, as required, appropriate individuals.</p>
<p>Security Baseline: Moderate and High</p>
<p>Related HUD Policy: 5.2.2</p>

NIST SP 800-53 Control: AC-2	
Supporting Procedures	
<ol style="list-style-type: none"> 1. Review and approve or deny requests for access to HUD systems based on a valid need-to-know, intended system usage, and completion of all personnel security requirements using automated mechanisms for moderate- and high-impact systems. For moderate- and high-impact systems, track account creation, disabling, and termination and notify appropriate individuals of all changes. (Program Office/System Owner, ISSO) 2. Access Privileges that increase from greater than read only must be processed through HUD's account management system including the completion of background investigation forms. Background investigation forms must be submitted to the personnel security branch in OSEP. (Program Office/System Owner, System Security Administrator) 3. Assign system administrators separate accounts for administrator and non-administrator responsibilities. (Program Office/System Owner, ISSO, System Administrator) 4. Disable user IDs after 90 days of inactivity. For moderate- and high-impact systems, use an automated mechanism to disable inactive user accounts. (ISSO, System Administrator) 5. Disable guest/anonymous accounts and change default vendor or factory-set administrator passwords for all HUD system. (Deputy CIO for IT Operations, ISSO, System Administrator) 6. Authorize temporary and emergency accounts based on organizational requirements. Automatically terminate the temporary or emergency accounts 48 hours after the emergency is resolved for moderate- and high-impact systems. (Program Office/System Owner, ISSO) 7. Notify Program Office/System Owner when users are terminated, transferred, or no longer need access to a system. (Supervisor) 8. Remove or disable the associated accounts of terminated or transferred employees or contractors, immediately after notification. (ISSO, System Administrator) 9. Review and validate system accounts annually. (Program Office/System Owner) 	

5.2.3 Access Enforcement

NIST SP 800-53 Control: AC-3	
<p>AC-3: The information system enforces assigned authorizations for controlling access to the system in accordance with applicable policy.</p>	
<p>Security Baseline: Low, Moderate, and High</p>	
<p>E-1: The information system restricts access to privileged functions (deployed in hardware, software, and firmware) and security-relevant information to explicitly authorized personnel.</p>	
<p>Security Baseline: Moderate and High</p>	
<p>Related HUD Policy: 5.2.3</p>	
Supporting Procedures	
<ol style="list-style-type: none"> 1. Establish proper access controls (e.g., access control lists, capability lists). (Developer, System Administrator) 2. Enforce assigned authorization and access control implementation on every network component. (Program Office/System Owner, ISSO, System Administrator) 3. Employ access enforcement mechanisms at the application level, when necessary, based on an assessment of risk. (Program Office/System Owner, Developer) 4. Use FIPS 140-2 compliant cryptography if encryption of stored information is employed as an access control mechanism. (Program Office/System Owner, Developer, System Administrator) 	

5.2.4 Information Flow Enforcement

NIST SP 800-53 Control: AC-4
<p>AC-4: The information system enforces assigned authorizations for controlling the flow of information within the system and between interconnected systems in accordance with applicable policy.</p> <p>Security Baseline: Moderate and High</p>
<p>E-1: The information system implements information flow control enforcement using explicit labels on information, source, and destination objects as a basis for flow control decisions.</p> <p>Security Baseline: N/A</p>
<p>E-2: The information system implements information flow control enforcement using protected processing domains (e.g., domain type-enforcement) as a basis for flow control decisions.</p> <p>Security Baseline: N/A</p>
<p>E-3: The information system implements information flow control enforcement using dynamic security policy mechanisms as a basis for flow control decisions.</p> <p>Security Baseline: N/A</p>
<p>Related HUD Policy: 5.2.4</p>
Supporting Procedures
<ol style="list-style-type: none"> 1. Select appropriate methods/guidelines to control the flow of information within and between interconnected systems (e.g., firewall rules, application flow control) (Developer, System Administrator)

5.2.5 Separation of Duties

NIST SP 800-53 Control: AC-5
<p>AC-5: The information system enforces separation of duties through assigned access authorizations.</p> <p>Security Baseline: Moderate and High</p>
<p>Related HUD Policy: 5.2.5</p>
Supporting Procedures
<ol style="list-style-type: none"> 1. Establish appropriate division of responsibilities and separate duties, as needed, to eliminate conflicts of interest within each HUD division/office. (HUD Division Directors/Office Directors) 2. Enforce division and separation of duties and responsibilities for critical system functions among different individuals to minimize the possibility of fraudulent or criminal activity. (Program Office/System Owner) 3. Implement access control software that prevents users from having all the necessary authority or information access to perform fraudulent activity without collusion in moderate- and high-impact systems. (ISSO, Developer, System Administrator)

5.2.6 Least Privilege

NIST SP 800-53 Control: AC-6
<p>AC-6: The information system enforces the most restrictive set of rights/privileges or accesses needed by users (or processes acting on behalf of users) for the performance of specified tasks.</p>
<p>Security Baseline: Moderate and High</p>
<p>Related HUD Policy: 5.2.6</p>
Supporting Procedures
<ol style="list-style-type: none"> 1. Grant users the most restrictive set of privileges needed to perform authorized tasks. (Program Office/System Owner, ISSO) 2. Implement least privilege access on network devices (e.g., firewalls, routers, switches). (Developer, System Administrator) 3. Restrict the accesses needed by processes acting on behalf of users for the performance of specified tasks. (Developer, System Administrator)

5.2.7 Unsuccessful Login Attempts

NIST SP 800-53 Control: AC-7
<p>AC-7: The information system enforces a limit of three consecutive invalid access attempts by a user during a thirty-minute time period. The information system locks the account and requires manual intervention by an appropriate security administrator to unlock the account when the maximum number of unsuccessful attempts is exceeded.</p>
<p>Security Baseline: Low, Moderate, and High</p>
<p>E-1: The information system automatically locks the account/node until released by an administrator when the maximum number of unsuccessful attempts is exceeded.</p>
<p>Security Baseline: N/A</p>
<p>Related HUD Policy: 5.2.7</p>
Supporting Procedures
<ol style="list-style-type: none"> 1. Configure HUD information systems to enforce an account lockout that limits the number of consecutive failed logon attempts to three within a thirty-minute time period and deny logon of any kind while the account remains locked. (Program Office/System Owner) 2. Notify the appropriate HUD system administrator to manually unlock the account following a lockout due to consecutive failed attempts. (Users, System Administrator)

5.2.8 System Use Notification

NIST SP 800-53 Control: AC-8
<p>AC-8: The information system displays an approved, system use notification message before granting system access informing potential users: (i) that the user is accessing a U.S. Government information system; (ii) that system usage may be monitored, recorded, and subject to audit; (iii) that unauthorized use of the system is prohibited and subject to criminal and civil penalties; and (iv) that use of the system indicates consent to monitoring and recording. The system use notification message provides appropriate privacy and security notices (based on associated privacy and security policies or summaries) and remains on the screen until the user takes explicit actions to log on to the information system.</p>
<p>Security Baseline: Low, Moderate, and High</p>
<p>Related HUD Policy: 5.2.8</p>
Supporting Procedures
<ol style="list-style-type: none"> 1. Implement a HUD standard system warning banner that notifies users that they have accessed a U.S. Government system, they are subject to monitoring and recording for inappropriate use, they can be punished for inappropriate use, and that system use indicates consent. (ISSO, System Administrator) 2. Implement a security and privacy statement including a description of the authorized uses of the system for all HUD information systems accessible by the public. (Program Office/System Owner, ISSO)

5.2.9 Previous Logon Notification

NIST SP 800-53 Control: AC-9
<p>AC-9: The information system notifies the user, upon successful logon, of the date and time of the last logon, and the number of unsuccessful logon attempts since the last successful logon.</p>
<p>Security Baseline: N/A</p>
<p>Related HUD Policy: None</p>
Supporting Procedures
<p>If selected:</p> <ol style="list-style-type: none"> 1. Notify the user after successful logon, the date and time of the last logon and the number of unsuccessful logon attempts since the last successful logon. (Developer, System Administrator)

5.2.10 Concurrent Session Control

NIST SP 800-53 Control: AC-10
<p>AC-10: The information system limits the number of concurrent sessions for any user to none.</p>
<p>Security Baseline: High</p>
<p>Related HUD Policy: 5.2.10</p>
Supporting Procedures
<ol style="list-style-type: none"> 1. Disallow concurrent sessions for high-impact systems. (Developer, System Administrator)

5.2.11 Session Lock

NIST SP 800-53 Control: AC-11
AC-11: The information system prevents further access to the system by initiating a session lock after 15 minutes of inactivity, and the session lock remains in effect until the user reestablishes access using appropriate identification and authentication procedures.
Security Baseline: Moderate and High
Related HUD Policy: 5.2.11
Supporting Procedures
<ol style="list-style-type: none"> 1. Lock all workstations prior to leaving them unattended. (Users) 2. Provide an automated mechanism to lockout a session after fifteen minutes of inactivity. (Developer, System Administrator) 3. Implement password-protected screen savers on all workstations owned/leased by HUD and ensure the screen saver will automatically lock the workstation after fifteen minutes of inactivity and that users can directly initiate the screen locking mechanisms. (Program Office/System Owner)

5.2.12 Session Termination

NIST SP 800-53 Control: AC-12
AC-12: The information system automatically terminates a remote session after twenty minutes of inactivity.
Security Baseline: Moderate and High
E-1: Automatic session termination applies to local and remote sessions.
Security Baseline: High
Related HUD Policy: 5.2.12
Supporting Procedures
<ol style="list-style-type: none"> 1. Terminate a session by logging out of the system. (User) 2. Configure moderate- or high-impact systems to terminate user sessions after twenty minutes of inactivity. (Program Office/System Owner)

5.2.13 Supervision and Review—Access Control

NIST SP 800-53 Control: AC-13
AC-13: The organization supervises and reviews the activities of users with respect to the enforcement and usage of information system access controls.
Security Baseline: Low, Moderate, and High
E-1: The organization employs automated mechanisms to facilitate the review of user activities.
Security Baseline: High
Related HUD Policy: 5.2.13

NIST SP 800-53 Control: AC-13
Supporting Procedures
<ol style="list-style-type: none"> 1. Review audit records periodically for suspicious, unusual, or inappropriate activities and report findings to an appropriate official. Review audit records of users with significant access control responsibilities more frequently. (Program Office/System Owner, ISSO, System Administrator) 2. Implement an automated mechanism to facilitate the review of audit records for moderate- and high-impact systems. (ISSO, System Administrator)

5.2.14 Permitted Actions without Identification or Authentication

NIST SP 800-53 Control: AC-14
<p>AC-14: The organization identifies and documents specific user actions that can be performed on the information system without identification or authentication.</p> <p>Security Baseline: Low, Moderate, and High</p> <p>E-1: The organization permits actions to be performed without identification and authentication only to the extent necessary to accomplish mission objectives.</p> <p>Security Baseline: Moderate and High</p> <p>Related HUD Policy: 5.2.14</p>
Supporting Procedures
<ol style="list-style-type: none"> 1. Identify and document user actions that can be performed on public websites or other publicly accessible information systems without identification and authentication. (OITS, Program Office/System Owner) 2. Limit and document user actions that can be performed without identification and authentication on moderate- or high-impact systems to the extent necessary to accomplish mission objectives. (Program Office/System Owner)

5.2.15 Automated Marking

NIST SP 800-53 Control: AC-15
<p>AC-15: The information system marks output using standard naming conventions to identify any special dissemination, handling, or distribution instructions.</p> <p>Security Baseline: High</p> <p>Related HUD Policy: 5.2.15</p>
Supporting Procedures
<ol style="list-style-type: none"> 1. Mark printed output from high-impact systems according to HUD guidelines. (Users)

5.2.16 Automated Labeling

NIST SP 800-53 Control: AC-16
AC-16: The information system appropriately labels information in storage, in process, and in transmission.
Security Baseline: N/A
Related HUD Policy: None
Supporting Procedures
If selected: 1. Label information in storage, in process, and in transmission in accordance with access control requirements and special dissemination, handling, or distribution requirements based on an assessment of risk. (Developer)

5.2.17 Remote Access

NIST SP 800-53 Control: AC-17
AC-17: The organization authorizes, monitors, and controls all methods of remote access to the information system.
Security Baseline: Low, Moderate, and High
E-1: The organization employs automated mechanisms to facilitate the monitoring and control of remote access methods.
Security Baseline: Moderate and High
E-2: The organization uses cryptography to protect the confidentiality and integrity of remote access sessions.
Security Baseline: Moderate and High
E-3: The organization controls all remote accesses through a limited number of managed access control points.
Security Baseline: Moderate and High
E-4: The organization permits remote access for privileged functions only for compelling operational needs and documents the rationale for such access in the security plan for the information system.
Security Baseline: Moderate and High
Related HUD Policy: 5.2.17

NIST SP 800-53 Control: AC-17
Supporting Procedures
<ol style="list-style-type: none"> 1. Request authorization for remote access in writing, including remote access for privileged functions (e.g., maintenance ports and system and device administration). (Supervisor) 2. Approve or deny requests for remote access based on an adequate justification. (Program Office/System Owner, ISSO) 3. Permit remote access for privileged functions only for compelling operational needs and emergencies. (Program Office/System Owner, ISSO) 4. Provide written approval to the system administrator prior to implementing the remote access. (Program Office/System Owner, ISSO) 5. Use HUD centrally managed remote access mechanisms or a mechanism authorized by the Deputy CIO for IT Operations. Use automated mechanisms for moderate- and high-impact systems. (Program Office/System Owner) 6. Implement encryption to protect the confidentiality or remote access sessions for moderate- and high-impact systems. (Deputy CIO for IT Operations) 7. Use HUD's telecommuting web site (https://telework.hud.gov/login.asp or iNotes to telecommute. (Users) 8. Do not open a peer-to-peer session while logged into the HUD telecommuting web site. (Users)

5.2.18 Wireless Access Restrictions

NIST SP 800-53 Control: AC-18
<p>AC-18: The organization: (i) establishes usage restrictions and implementation guidance for wireless technologies; and (ii) authorizes, monitors, controls wireless access to the information system.</p>
<p>Security Baseline: Low, Moderate, and High</p>
<p>E-1: The organization uses authentication and encryption to protect wireless access to the information system.</p>
<p>Security Baseline: Moderate and High</p>
<p>E-2: The organization scans for unauthorized wireless points annually and takes appropriate action if such access points are discovered.</p>
<p>Security Baseline: High</p>
<p>Related HUD Policy: 5.2.18</p>
Supporting Procedures
<ol style="list-style-type: none"> 1. Configure all WLAN and wireless access points in accordance with NIST SP 800-48, <i>Wireless Network Security</i>. (Deputy CIO for IT Operations) 2. Implement Extensible Authentication Protocol with Wi-Fi Access Protection or IEEE 802.11i on WLANs or access points to provide encryption and strong identification and authentication for moderate- and high-impact systems. (Deputy CIO for IT Operations) 3. Request approval for use of wireless technologies with supporting justification. Submit the request to the CISO. (Program Office/System Owner) 4. Review requests and deny or approve use of wireless technologies at HUD. (CISO, OITS) 5. Monitor all use of wireless technologies at HUD including scanning for rogue access points. (Deputy CIO for IT Operations, System Administrator) 6. Disable all rogue access points. (Deputy CIO for IT Operations, System Administrator)

5.2.19 Access Control for Portable and Mobile Devices

NIST SP 800-53 Control: AC-19
AC-19: The organization: (i) establishes usage restrictions and implementation guidance for organization-controlled portable and mobile devices; and (ii) authorizes, monitors, and controls device access to organizational information systems.
Security Baseline: Moderate and High
Related HUD Policy: 5.2.19
Supporting Procedures
<ol style="list-style-type: none"> 1. Request approval in writing to connect mobile or portable systems to HUD’s network, providing verification that the device meets the HUD connection criteria. (Users) 2. Approve or deny requests to connect mobile or portable systems to HUD’s network. (Deputy CIO for IT Operations) 3. Use approved encryption algorithms to protect information residing on portable or mobile moderate- or high-impact systems. (Program Office/System Owner) 4. Monitor the use of mobile and portable systems on HUD’s networks. (Deputy CIO for IT Operations)

5.2.20 Use of External Information Systems

NIST SP 800-53 Control: AC-20
AC-20: The organization establishes terms and conditions for authorized individuals to: (i) access the information system from an external information system; and (ii) process, store, and/or transmit organization-controlled information using an external information system,
Security Baseline: Low, Moderate, and High
E-1: The organization prohibits authorized individuals from using an external information system to access the information system or to process, store, or transmit organization-controlled information except in situations where the organization: (i) can verify the employment of required security controls on the external system as specified in the organization’s information security policy and system security plan; or (ii) has approved information system connection or processing agreements with the organizational entity hosting the external information system.
Security Baseline: Moderate and High
Related HUD Policy: 5.2.20
Supporting Procedures
<ol style="list-style-type: none"> 1. Do not install personally owned equipment or software (e.g., laptop computers, personal digital devises) on HUD’s network without written approval. (Users) 2. Submit a written request to the HUD CISO to connect to HUD’s network that includes the terms and conditions defined in HUD policy. (Program Office/System Owner) 3. Approve or deny the ability to connect personally owned equipment or software to HUD’s network in writing. (OITS) 4. Do not transmit sensitive HUD information to any personal email account that is not authorized to receive it. (Users) 5. Do not copy or download HUD information or documents to any external media for use on any personally owned equipment. (Users)

5.2.21 Personal Use of Government Equipment

HUD Policy: HUD AC-1
<p>HUD Policy: 5.2.21</p> <ol style="list-style-type: none"> 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 MOA/U. c. HUD employees or contractors shall not access personal email accounts from internal HUD networks or with HUD-provided equipment. <p>Security Baseline: Low, Moderate, and High</p>
Supporting Procedures
<ol style="list-style-type: none"> 1. Permit HUD information systems/computers for limited personal use by government employees so long as the use does not interfere with official duties, cause degradation of network services, or violate the rules of behavior. (Program Office/System Owner) 2. Prohibit contractors and other non-HUD employees' limited personal use of HUD information systems/computers unless specifically permitted by the governing contract or MOA/U. (Program Office/System Owner) 3. Do not access personal or corporate email accounts from internal HUD networks or with HUD-provided equipment. (Program Office/System Owner)

5.3 Audit and Accountability

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

This control ensures that there is a mechanism in place to track and associate user and system activity to events.

FIPS 200 Requirement
<p>Organizations must: (i) create, protect, and retain information system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate information system activity; and (ii) ensure that the actions of individual information system users can be uniquely traced to those users so they can be held accountable for their actions.</p>

5.3.1 Audit and Accountability Policy and Procedures

NIST SP 800-53 Control: AU-1
AU-1: The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, audit and accountability policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the audit and accountability policy and associated audit and accountability controls.
Security Baseline: Low, Moderate, and High
Related HUD Policy: <i>Information Technology Security Policy, Handbook 2400.25, Rev. 1</i>
Implementation
This control is implemented by the <i>Information Technology Security Policy, Handbook 2400.25, Rev. 1</i> , which defines HUD's security policies. The procedures related to the HUD policies are in this document, <i>HUD Information Technology Security Procedures</i> .

5.3.2 Auditable Events

NIST SP 800-53 Control: AU-2
AU-2: The information system generates audit records for the events specified in the security plan.
Security Baseline: Low, Moderate, and High
E-1: The information system provides the capability to compile audit records from multiple components throughout the system into a system-wide (logical or physical), time-correlated audit trail.
Security Baseline: High
E-2: The information system provides the capability to manage the selection of events to be audited by individual components of the system.
Security Baseline: High
E-3: The organization periodically reviews and updates the list of organization-defined auditable events.
Security Baseline: Moderate and High
Related HUD Policy: 5.3.2

NIST SP 800-53 Control: AU-2	
Supporting Procedures	
<ol style="list-style-type: none"> 1. Specify which information system components carry out auditing activities and what type of events will be audited in the security plan (e.g., failed login attempts, patch installations, access control changes, software installations). The list of auditable events must be adequate to support after-the-fact investigations of security incidents. (Program Office/System Owner, Deputy CIO for IT Operations, ISSO) 2. Audit records shall be sufficient in detail to facilitate the reconstruction of events if compromise or malfunction occurs or is suspected. The audit record shall contain at least the following information: <ul style="list-style-type: none"> • Identity of each user and device accessing or attempting to access an information system • Time and date of the access and the logoff • Activities that might modify, bypass, or negate information security safeguards • Security-relevant actions associated with automated processing • All activities performed using an administrator's identity 3. Update the list of auditable events periodically for moderate- and high-impact systems. (Program Office/System Owner, Deputy CIO for IT Operations) 4. Compile audit records from multiple components into a system-wide (logical or physical), time-correlated audit trail for high-impact systems. (Deputy CIO for IT Operations) 	

5.3.3 Content of Audit Records

NIST SP 800-53 Control: AU-3	
<p>AU-3: The information system produces audit records that contain sufficient information to establish what events occurred, the sources of the events, and the outcomes of the events.</p>	
<p>Security Baseline: Low, Moderate, and High</p>	
<p>E-1: The information system provides the capability to include additional, more detailed information in the audit records for audit events identified by type, location, or subject.</p>	
<p>Security Baseline: Moderate and High</p>	
<p>E-2: The information system provides the capability to centrally manage the content of audit records generated by individual components throughout the system.</p>	
<p>Security Baseline: High</p>	
<p>Related HUD Policy: 5.3.3</p>	
Supporting Procedures	
<ol style="list-style-type: none"> 1. Record the following information for each auditable event and any additional information as specified in the system security plan: (Program Office/System Owner, ISSO) <ul style="list-style-type: none"> • Time and date of the event (using Greenwich Mean Time [GMT]) • Component of the information system where the event occurred (e.g., software or hardware component) • Type of event • User/subject identify • Outcome of the event (success or failure) 2. Provide more detail for audit events identified by type, location, or subject for moderate- and high-impact systems when possible. (Program Office/System Owner, ISSO) 	

5.3.4 Audit Storage Capacity

NIST SP 800-53 Control: AU-4
AU-4: The organization allocates sufficient audit record storage capacity and configures auditing to reduce the likelihood of such capacity being exceeded.
Security Baseline: Low, Moderate, and High
Related HUD Policy: 5.3.4
Supporting Procedures
<ol style="list-style-type: none"> 1. Allocate adequate system audit record storage capacity to configure auditing to reduce the likelihood of the auditing capability from being exceeded . (Program Office/System Owner, Deputy CIO for IT Operations, ISSO)

5.3.5 Response to Audit Processing Failures

NIST SP 800-53 Control: AU-5
AU-5: The information system alerts appropriate organizational officials in the event of an audit processing, and takes the following additional actions: shut down the system, overwrites the oldest audit records, or stops generating audit records.
Security Baseline: Low, Moderate, and High
E-1: The information system provides a warning when allocated audit record storage volume reaches 80%.
Security Baseline: High
(E-2): The information system provides a real-time alert when the following audit failure events occur: <ul style="list-style-type: none"> • Allocated audit record storage volume reaches 92%
Security Baseline: High
Related HUD Policy: 5.3.5
Supporting Procedures
<ol style="list-style-type: none"> 1. Notify the responsible officials in the event of an audit failure or when an audit storage capacity is near maximum, preferably with automated notification (e.g., pager, email). (Program Office/System Owner, ISSO) 2. Execute one or all of the following actions in the event of an audit failure or audit storage capacity being reached: (Program Office/System Owner, System Administrator) <ul style="list-style-type: none"> • Shut down the system • Overwrite the oldest audit records • Stop generating audit records

5.3.6 Audit Monitoring, Analysis, and Reporting

NIST SP 800-53 Control: AU-6
<p>AU-6: The organization regularly reviews/analyzes information system audit records for indications of inappropriate or unusual activity, investigates suspicious activity or suspected violations, reports findings to appropriate officials, and takes necessary actions.</p> <p>Security Baseline: Moderate and High</p>
<p>E-1: The organization employs automated mechanisms to integrate audit monitoring, analysis, and reporting into an overall process for investigation and response to suspicious activities.</p> <p>Security Baseline: High</p>
<p>E-2: The organization employs automated mechanisms to alert security personnel of the following inappropriate or unusual activities with security implications:</p> <ul style="list-style-type: none"> • Audit failure • Audit storage capacity near maximum • Items defined in the system security plan <p>Security Baseline: Moderate and High</p>
<p>Related HUD Policy: 5.3.6</p>
Supporting Procedures
<ol style="list-style-type: none"> 1. Analyze audit records periodically, as defined in the security plan, for evidence of suspicious, unusual, and inappropriate activity. Audit records of users with significant information system roles and responsibilities more frequently. (Program Office/System Owner, ISSO) 2. Notify appropriate officials of any suspected violations found in audit records. (Program Office/System Owner, ISSO) 3. Use automated mechanisms to facilitate audit review and response to suspicious event activity for moderate- and high-impact systems and integrate logs when possible for analysis (e.g., firewalls, routers, switches). Integrate the automated audit capability with the incident response capability. (Program Office/System Owner, ISSO, System Administrator)

5.3.7 Audit Reduction and Report Generation

NIST SP 800-53 Control: AU-7
<p>AU-7: The information system provides an audit reduction and report generation capability.</p> <p>Security Baseline: Moderate and High</p>
<p>E-1: The information system provides the capability to automatically process audit records for events of interest based upon selectable, event criteria.</p> <p>Security Baseline: Moderate and High</p>
<p>Related HUD Policy: 5.3.7</p>

NIST SP 800-53 Control: AU-7
Supporting Procedures
<ol style="list-style-type: none"> 1. Use audit reduction, review, and reporting techniques for moderate- or high-impact systems. Ensure these techniques will not alter the original audit record needed to support post-incident investigations. (Program Office/System Owner, ISSO) 2. Provide the ability to automatically process audit events based on selectable, event criteria for moderate- and high-impact systems. (Program Office/System Owner, ISSO)

5.3.8 Time Stamps

NIST SP 800-53 Control: AU-8
AU-8: The information system provides time stamps for use in audit record generation.
Security Baseline: Low, Moderate, and High
E-1: The organization synchronizes internal information system clocks monthly.
Security Baseline: Moderate and High
Related HUD Policy: 5.3.8
Supporting Procedures
<ol style="list-style-type: none"> 1. Provide time stamps for use with all audit record generation. (Program Office/System Owner, Deputy CIO for IT Operations) 2. Synchronize internal information system clocks monthly. (Deputy CIO for IT Operations)

5.3.9 Protection of Audit Information

NIST SP 800-53 Control: AU-9
AU-9: The information system protects audit information and audit tools from unauthorized access, modification, and deletion.
Security Baseline: Low, Moderate, and High
E-1: The information system produces audit records on hardware-enforced, write-once media.
Security Baseline: N/A
Related HUD Policy: 5.3.9
Supporting Procedures
<ol style="list-style-type: none"> 1. Restrict audit trails and logs to authorized personnel. (Program Office/System Owner, ISSO)

5.3.10 Non-Repudiation

NIST SP 800-53 Control: AU-10
AU-10: The information system provides the capability to determine whether a given individual took a particular action.
Security Baseline: N/A
Related HUD Policy: None
Supporting Procedures
If selected: 1. Provide the capability to determine whether an individual took a particular action. Examples of this capability include digital signatures, digital message receipts, or time stamps. (Program Office/System Owner)

5.3.11 Audit Record Retention

NIST SP 800-53 Control: AU-11
AU-11: The organization retains audit records for one year to provide support for after-the-fact investigations of security incidents and to meet regulatory and organizational information retention requirements.
Security Baseline: Low, Moderate, and High
Related HUD Policy: 5.3.11
Supporting Procedures
1. Retain recorded system audit records in accordance with HUD record retention policies, but for no less than one year. (Program Office/System Owner, ISSO)

5.4 System and Communications Protection

Systems and communications protection controls ensure that system and communications protection policies and procedures are implemented that address the protection of information transmitted or received by the organization’s information systems.

The following procedures address placing appropriate protection in place for systems and communications to include separation of functions, cryptographic key management, denial of service and boundary protection.

FIPS 200 Requirement
Organizations must: (i) monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information system; and (ii) employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational information systems.

5.4.1 System and Communications Policy and Procedures

NIST SP 800-53 Control: SC-1
<p>SC-1: The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, system and communications protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the system and communications protection policy and associated system and communications protection controls.</p>
<p>Security Baseline: Low, Moderate, and High</p>
<p>Related HUD Policy: <i>Information Technology Security Policy, Handbook 2400.25, Rev. 1</i></p>
Implementation
<p>This control is implemented by the <i>Information Technology Security Policy, Handbook 2400.25, Rev. 1</i>, which defines HUD’s security policies. The procedures related to the HUD policies are in this document, <i>HUD Information Technology Security Procedures</i>.</p>

5.4.2 Application Partitioning

NIST SP 800-53 Control: SC-2
<p>SC-2: The information system separates user functionality (including user interface services) from information system management functionality.</p>
<p>Security Baseline: Moderate and High</p>
<p>Related HUD Policy: 5.4.2</p>
Supporting Procedures
<ol style="list-style-type: none"> 1. Separate user interface services (e.g., public web pages) from information storage and management services (e.g., database management) for moderate- and high-impact systems. (Program Office/System Owner)

5.4.3 Security Function Isolation

NIST SP 800-53 Control: SC-3
<p>SC-3: The information system isolates security functions from non-security functions.</p>
<p>Security Baseline: High</p>
<p>E-1: The information system employs underlying hardware separation mechanisms to facilitate security function isolation.</p>
<p>Security Baseline: N/A</p>
<p>E-2: The information system isolates critical security functions (i.e., functions enforcing access and information flow control) from both non-security functions and from other security functions.</p>
<p>Security Baseline: N/A</p>

NIST SP 800-53 Control: SC-3
<p>E-3: The information system minimizes the number of non-security functions included within the isolation boundary containing security functions.</p> <p>Security Baseline: N/A</p>
<p>E-4: The information system security functions are implemented as largely independent modules that avoid unnecessary interactions between modules.</p> <p>Security Baseline: N/A</p>
<p>E-5: The information system security functions are implemented as a layered structure minimizing interactions between layers of the design and avoiding any dependence by lower layers on the functionality or correctness of higher layers.</p> <p>Security Baseline: N/A</p>
<p>Related HUD Policy: 5.4.3</p>
Supporting Procedures
<ol style="list-style-type: none"> 1. Isolate security functions on high-impact systems from non-security functions by means of partitions, domains, etc. and ensure the information system maintains a separate domain for each executing process.

5.4.4 Information Remnants

NIST SP 800-53 Control: SC-4
<p>SC-4: The information system prevents unauthorized and unintended information transfer via shared system resources.</p> <p>Security Baseline: Moderate and High</p>
<p>Related HUD Policy: 5.4.4</p>
Supporting Procedures
<ol style="list-style-type: none"> 1. Control information system remnants for moderate-and high-impact systems (e.g., prevent information produced by the actions of a prior user/role from being available to any current user/role that obtains access to a shared system resource after that resource has been released back to the information system). (Program Office/System Owner)

5.4.5 Denial of Service Protection

NIST SP 800-53 Control: SC-5
<p>SC-5: The information system protects against or limits the effects of the denial of service attacks identified at www.us-cert.gov.</p> <p>Security Baseline: Low, Moderate, and High</p>
<p>E-1: The information system restricts the ability of users to launch denial of service attacks against other information systems or networks.</p> <p>Security Baseline: N/A</p>

NIST SP 800-53 Control: SC-5
E-2: The information system manages excess capacity, bandwidth, or other redundancy to limit the effects of information flooding types of denial of service attacks.
Security Baseline: N/A
Related HUD Policy: 5.4.5
Supporting Procedures
<ol style="list-style-type: none"> 1. Configure interfaces protecting HUD's network perimeter to filter packet types specific to denial of service attacks. (System Administrator) 2. Protect publicly accessible information systems by employing increased capacity and bandwidth combined with service redundancy. (Deputy CIO for IT Operations, System Administrator)

5.4.6 Resource Priority

NIST SP 800-53 Control: SC-6
SC-6: The information system limits the use of resources by priority.
Security Baseline: N/A
Related HUD Policy: None
Supporting Procedures
<p>If selected:</p> <ol style="list-style-type: none"> 1. Ensure that a lower-priority process is not able to interfere with the information system servicing any higher-priority process. (Deputy CIO for IT Operations, System Administrator)

5.4.7 Boundary Protection

NIST SP 800-53 Control: SC-7
SC-7: The information system monitors and controls communications at the external boundary of the information system and at key internal boundaries within the system.
Security Baseline: Low, Moderate, and High
E-1: The organization physically allocates publicly accessible information system components to separate sub-networks with separate, physical network interfaces.
Security Baseline: Moderate and High
E-2: The organization prevents public access into the organization's internal networks except as appropriately mediated.
Security Baseline: Moderate and High
E-3: The organization limits the number of access points to the information system to allow for better monitoring of inbound and outbound network traffic.
Security Baseline: Moderate and High

NIST SP 800-53 Control: SC-7
<p>E-4: The organization implements a managed interface (boundary protection devices in an effective security architecture) with any external telecommunication service, implementing controls appropriate to the required protection of the confidentiality and integrity of the information being transmitted.</p> <p>Security Baseline: Moderate and High</p>
<p>E-5: The information system denies network traffic by default and allows network traffic by exception (i.e., deny all, permit by exception).</p> <p>Security Baseline: Moderate and High</p>
<p>E-6: The organization prevent the unauthorized release of information outside of the information system boundary or any unauthorized communication through the information system boundary when there is an operational failure of the boundary protection mechanisms.</p> <p>Security Baseline: High</p> <p>Related HUD Policy: 5.4.7</p>
Supporting Procedures
<ol style="list-style-type: none"> 1. Provide controlled interfaces (e.g., proxies, gateways, routers, firewalls, encrypted tunnels) for any connection to the Internet or other external networks or information systems. (Deputy CIO for IT Operations, System Administrator) 2. Prevent the unauthorized release of information outside the information system boundary if an operational failure of the boundary protection mechanism (e.g., firewall, failsafe mechanism, access control) occurs. (Deputy CIO for IT Operations, System Administrator) 3. Mediate public access to HUD's internal networks through a proxy service. (Deputy CIO for IT Operations, Program Office/System Owner, System Administrator) 4. Establish separate sub-networks with separate physical network interfaces (e.g., demilitarized zone [DMZ]) for publicly-accessible system components. (Deputy CIO for IT Operations, System Administrator) 5. Provide the same level of communication controls for alternate processing sites as the primary site. (Deputy CIO for IT Operations, Program Office/System Owner)

5.4.8 Transmission Integrity

NIST SP 800-53 Control: SC-8
<p>SC-8: The information system protects the integrity of transmitted information.</p> <p>Security Baseline: Moderate and High</p>
<p>E-1: The organization employs cryptographic mechanisms to recognize changes to information during transmission unless otherwise protected by alternative physical measures.</p> <p>Security Baseline: High</p> <p>Related HUD Policy: 5.4.8</p>

NIST SP 800-53 Control: SC-8
Supporting Procedures
<ol style="list-style-type: none"> 1. Choose a cryptographic mechanism that employs an integrity checking capability. (Program Office/System Owner, Deputy CIO for IT Operations) 2. Protect high-impact systems using cryptographic mechanisms to prevent unauthorized disclosure of information during transmission unless protected by alternative physical measures (e.g., PDS). National Security Telecommunications and Information Systems Security Instruction (NSTISSI) No. 7003 contains guidance on the use of PDS. NIST SP 800-52 provides guidance on protection transmission confidentiality using Transport Layer Security (TLS). NIST SP 800-77 provides guidance on protecting transmission confidentiality using IPsec. (Program Office/System Owner, Deputy CIO for IT Operations)

5.4.9 Transmission Confidentiality

NIST SP 800-53 Control: SC-9
<p>SC-9: The information system protects the confidentiality of transmitted information.</p> <p>Security Baseline: Moderate and High</p>
<p>E-1: The organization employs cryptographic mechanisms to prevent unauthorized disclosure of information during transmission unless otherwise protected by alternative physical measures.</p> <p>Security Baseline: High</p>
<p>Related HUD Policy: 5.4.9</p>
Supporting Procedures
<ol style="list-style-type: none"> 1. Protect the confidentiality of transmitted information by selecting an appropriate cryptographic mechanism. (Program Owner/System Owner) 2. Protect high-impact systems using cryptographic mechanisms to prevent unauthorized disclosure of information during transmission unless protected by alternative physical measures (e.g., PDS). NSTISSI No. 7003 contains guidance on the use of PDS. NIST SP 800-52 provides guidance on protection transmission confidentiality using Transport Layer Security (TLS). NIST SP 800-77 provides guidance on protecting transmission confidentiality using IPsec. (Program Owner/System Owner, Deputy CIO for IT Operations)

5.4.10 Network Disconnect

NIST SP 800-53 Control: SC-10
<p>SC-10: The information system terminates a network connection at the end of a session or after ten minutes of inactivity.</p> <p>Security Baseline: Moderate and High</p>
<p>Related HUD Policy: 5.4.10</p>

NIST SP 800-53 Control: SC-10
Supporting Procedures
<ol style="list-style-type: none"> 1. Configure moderate- or high-impact systems to terminate a network connection at the end of a session or after ten minutes of inactivity. (Program Office/System Owner, Developer, System Administrator) 2. Submit a request for a waiver and provide documented operation requirements with the justification. (Program Office/System Owner) 3. Review the request and approve or deny it, providing a written response. (OITS)

5.4.11 Trusted Path

NIST SP 800-53 Control: SC-11
<p>SC-11: The information system establishes a trusted communications path between the user and the following security functions of the system:</p> <ul style="list-style-type: none"> • Information system authentication and reauthentication (e.g., login)
Security Baseline: N/A
Related HUD Policy: None
Supporting Procedures
<p>If selected:</p> <ol style="list-style-type: none"> 1. Establish a trusted communications path between the user and the security functions of the system. (Program Office/System Owner, Developer)

5.4.12 Cryptographic Key Establishment and Management

NIST SP 800-53 Control: SC-12
<p>SC-12: When cryptography is required and employed within the information system, the organization establishes and manages cryptographic keys using automated mechanisms with supporting procedures or manual procedures.</p>
Security Baseline: Moderate and High
Related HUD Policy: 5.4.12
Supporting Procedures
<ol style="list-style-type: none"> 1. Employ automated mechanisms for cryptographic key establishment and key management following the guidance in NIST SP 800-56, <i>Recommendation on Key Establishment Schemes</i>, and NIST SP 800-57, <i>Recommendation on Key Management</i>. (Deputy CIO for IT Operations, Program Office/System Owner)

5.4.13 Use of Cryptography

NIST SP 800-53 Control: SC-13
<p>SC-13: For information requiring cryptographic protection, the information system implements cryptographic mechanisms that comply with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance.</p>
<p>Security Baseline: Low, Moderate, and High</p>
<p>Related HUD Policy: 5.4.13</p>
Supporting Procedures
<p>1. Select cryptography mechanisms that have been validated under FIPS 140-2 standards (as amended) or NSA Type 1 or Type 2 encryption (see http://csrc.nist.gov/cryptval/). (Deputy CIO for IT Operations, Program Office/System Owner)</p>

5.4.14 Public Access Protections

NIST SP 800-53 Control: SC-14
<p>SC-14: The information system protects the integrity and availability of publicly available information and applications.</p>
<p>Security Baseline: Low, Moderate, and High</p>
<p>Related HUD Policy: 5.4.14</p>
Supporting Procedures
<p>1. Design publicly-accessible information systems to protect the integrity and availability of the information and applications. (Developer)</p>

5.4.15 Collaborative Computing

NIST SP 800-53 Control: SC-15
<p>SC-15: The information system prohibits remote activation of collaborative computing mechanisms and provides an explicit indication of use to the local users.</p>
<p>Security Baseline: Moderate and High</p>
<p>E-1: The information system provides physical disconnect of camera and microphone in a manner that supports ease of use.</p>
<p>Security Baseline: N/A</p>
<p>Related HUD Policy: 5.4.15</p>
Supporting Procedures
<p>1. Configure information systems to prohibit remote activation of collaborative computing resources and to provide explicit indication of their use to local users for moderate- and high-impact systems. (System Administrator)</p>

5.4.16 Transmission of Security Parameters

NIST SP 800-53 Control: SC-16
<p>SC-16: The information system reliably associates security parameters with information exchanged between information systems.</p>
<p>Security Baseline: N/A</p>
<p>Related HUD Policy: None</p>
Supporting Procedures
<p>If selected:</p> <ol style="list-style-type: none"> Associate security parameters (e.g., security labels and markings) either explicitly or implicitly with the information contained within the information system. (Program Office/System Owner, Developer)

5.4.17 Public Key Infrastructure Certificates

NIST SP 800-53 Control: SC-17
<p>SC-17: The organization issues public key certificates under an appropriate certificate policy or obtains public key certificates under an appropriate certificate policy from an approved service provider.</p>
<p>Security Baseline: Moderate and High</p>
<p>Related HUD Policy: 5.4.17</p>
Supporting Procedures
<ol style="list-style-type: none"> Select and implement PKI for HUD in accordance with NIST SP 800-32, <i>Introduction to Public Key Technology and the Federal PKI Infrastructure</i>. (Deputy CIO for IT Operations, CISO) Establish root certificate authority (CA) and operate under an approved certificate policy and certificate practice statement. Any additional CA's within HUD must be subordinate to the root CA. (Deputy CIO for IT Operations) Cross-certify the HUD root CA with the Federal Bridge. (Deputy CIO for IT Operations, CISO) Issue the certificate to the individual using a security process after the recipient's identity has been verified in accordance with NIST SP 800-63, <i>Electronic Authentication Guidelines</i>. (Deputy CIO for IT Operations) Issue separate public/private key pairs for encryption and digital signature. (Deputy CIO for IT Operations, CISO) Conduct an annual compliance audit of the root CA and all subordinate CAs. (Deputy CIO for IT Operations, CISO) Do not disclose or share your private keys. (Users)

5.4.18 Mobile Code

NIST SP 800-53 Control: SC-18
<p>SC-18: The organization: (i) establishes usage restrictions and implementation guidance for mobile code technologies based on the potential to cause damage to the information system if used maliciously; and (ii) authorizes, monitors, and controls the use of mobile code within the information system.</p>
<p>Security Baseline: Moderate and High</p>

NIST SP 800-53 Control: SC-18
Related HUD Policy: 5.4.18
Supporting Procedures
<ol style="list-style-type: none"> 1. Submit a request to use mobile code to the CISO, including a justification for using mobile code. (Program Office/System Owner) 2. Review the request and approve or deny it, providing a written response. (OITS) 3. Prevent the development, acquisition, or introduction of unapproved mobile code (e.g., ActiveX, Java Script, PDF, Shockwave movies) within moderate- or high-impact information systems following the guidance in NIST SP 800-28, <i>Guidelines on Active Content and Mobile Code</i>. (Program Office/System Owner, ISSO, CISO)

5.4.19 Voice Over Internet Protocol

NIST SP 800-53 Control: SC-19
SC-19: The organization: (i) establishes usage restrictions and implementation guidance for Voice Over Internet Protocol (VoIP) technologies based on the potential to cause damage to the information system if used maliciously; and (ii) authorizes, monitors, and controls the use of VoIP within the information system.
Security Baseline: Moderate and High
Related HUD Policy: 5.4.19
Supporting Procedures
<ol style="list-style-type: none"> 1. Submit a request to use VOIP to the CISO and the Deputy CIO for IT Operations. (Program Office/System Owner) 2. Review the request and approve or deny it, providing a written response. (OITS) 3. Document, monitor, and control the use of VOIP in accordance with NIST SP 800-58, <i>Security Considerations for Voice over IP Systems</i>. (Deputy CIO for IT Operations)

5.4.20 Secure Name/Address Resolution Service (Authoritative Source)

NIST SP 800-53 Control: SC-20
SC-20: The information system that provides name/address resolution service provides additional data origin and integrity artifacts along with the authoritative data it returns in response to resolution queries.
Security Baseline: Moderate and High
E-1: The information system, when operating as part of a distributed, hierarchical namespace, provides the means to indicate the security status of child subspaces and (if the child supports secure resolution services) enable verification of a chain of trust among parent and child domains.
Security Baseline: N/A
Related HUD Policy: 5.4.20
Supporting Procedures
<ol style="list-style-type: none"> 1. Enable remote clients to obtain origin authentication and integrity verification assurance for the name/address resolution information obtained through the service consistent with the guidance in NIST SP 800-81. (Program Office/System Owner, Deputy CIO for IT Operations)

5.4.21 Secure Name/Address Resolution Service (Recursive or Caching Resolver)

NIST SP 800-53 Control: SC-21
<p>SC-21: The information system that provides name/address resolution service for local clients performs data origin authentication and data integrity verification on the resolution responses it receives from authoritative sources when requested by client systems.</p> <p>Security Baseline: High</p>
<p>E-1: The information system performs data origin authentication and data integrity verification on all resolution responses whether or not local clients explicitly request this service.</p> <p>Security Baseline: High</p>
<p>Related HUD Policy: 5.4.21</p>
Supporting Procedures
<ol style="list-style-type: none"> 1. Provide name/address resolution service for local clients that perform data origin authentication and data integrity verification on the resolution responses it receives from authoritative sources when requested by client systems following the guidance in NIST SP 800-81. (Program Office/System Owner, Deputy CIO for IT Operations)

5.4.22 Architecture and Provisioning for Name/Address Resolution Service

NIST SP 800-53 Control: SC-22
<p>SC-22: The information systems that collectively provide name/address resolution service for an organization are fault tolerant and implement role separation.</p> <p>Security Baseline: Moderate and High</p>
<p>Related HUD Policy: 5.4.22</p>
Supporting Procedures
<ol style="list-style-type: none"> 1. Implement both primary and secondary DNS servers following the guidance in NIST SP 800-81. The servers must be located on different subnets and geographically separated. (Deputy CIO for IT Operations) 2. Specify the clients who can access the authoritative DNS server. (Deputy CIO for IT Operations)

5.4.23 Secure Name/Address Resolution Service (Recursive or Caching Resolver)

NIST SP 800-53 Control: SC-23
<p>SC-23: The information system provides mechanisms to protect the authenticity of communications sessions.</p> <p>Security Baseline: Moderate and High</p>
<p>Related HUD Policy: 5.4.23</p>

NIST SP 800-53 Control: SC-23
Supporting Procedures
<ol style="list-style-type: none">1. Implement session-level protection following the guidance in NIST SP 800-52 and NIST SP -800-77. (Deputy CIO for IT Operations)2. Provide session-level protection using FIPS 140-2 (as amended) approved cryptographic modules for high-impact systems. (Deputy CIO for IT Operations)

Acronyms

3DES	Triple Data Encryption Standard
AC	Access Control
AES	Advanced Encryption Standard
AT	Awareness and Training
AU	Audit and Accountability
CA	Certificate Authority
CA	Certification, Accreditation, and Security Assessment
CCB	Configuration Control Board
CFR	Code of Federal Regulations
CISO	Chief Information Security Officer
CM	Configuration Management
CO	Contracting Officer
COTS	Commercial Off-the-Shelf
CP	Contingency Planning
CSIRC	Computer Security Incident Response Center
DMZ	Demilitarized Zone
FAR	Federal Acquisition Regulation
FIPS	Federal Information Processing Standard
FISMA	Federal Information Security Management Act
GMT	Greenwich Mean Time
GSA	General Services Administration
GTM	Government Technical Monitor
HSPD	Homeland Security Presidential Decision Directive
HUD	Department of Housing and Urban Development
IA	Identification and Authentication
IAS	Inventory of Automated Systems
ID	Identification
IEEE	Institute of Electrical and Electronics Engineers
IG	Inspector General
IR	Incident Response

ISSO	Information System Security Officer
IT	Information Technology
MA	Maintenance
MBI	Minimum Background Investigations
MOA/U	Memorandum or Agreement/Understanding
MP	Media Protection
N/A	Not Applicable
NIST	National Institute of Standards and Technology
NIST SP	National Institute of Standards and Technology Special Publication
NSA	National Security Agency
NSTISSI	National Security Telecommunications and Information Systems Security Instruction
OCIO	Office of the Chief Information Officer
OHR	Office of Human Resources
OIG	Office of the Inspector General
OITS	Office of Information Technology Security
OMB	Office of Management and Budget
OCPO	Office of the Chief Procurement Officer
OPM	Office of Personnel Management
OSEP	Office of Security and Emergency Planning
PDS	Protective Distribution Services
PE	Physical and Environmental Protection
PIA	Privacy Impact Assessment
PIV	Personal Identity Verification
PKI	Pubic Key Infrastructure
PL	Planning
POA&M	Plan Of Action & Milestones
PS	Personnel Security
RA	Risk Assessment
SA	System and Services Acquisition
SC	Systems and Security Control
SDM	System Development Methodology
SEO&PMD	Systems Engineering, Oversight & Performance Management Division

SI	System and Integrity Information
SLA	Service Level Agreement
SP	Special Publication
SSL3.0	Secure Sockets Layer Version 3.0
TLS1.0	Transport Layer Security Version 1.0
TRM	Technical Reference Model
TSP	Telecommunications Service Priority
USCERT	United States Computer Emergency Readiness Team
VoIP	Voice Over Internet Protocol
Wi-Fi	Wireless Fidelity
WLAN	Wireless Local Area Networks

Definitions

The following definitions are applicable to HUD policies and procedures.

Sensitive Information	FIPS 199 provides federal departments with a more detailed categorization of their information assets than the Computer Security Act of 1987 recognized. FIPS 199 distinguishes among <i>low</i> , <i>moderate</i> , and <i>high</i> 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.
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).
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.
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.

General Support System	<p>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.</p>
Major Applications	<p>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.</p>
Minor Applications	<p>A minor application is an information system that generally operates on accredited general support systems and utilizes the security controls of the general support system to provide an adequate level of security (although additional security controls may also be implemented within the application).</p>
Mission Critical Information System	<p>Mission-critical information systems are systems that an organization designates as critical to fulfilling its mission, including certain administrative systems.</p>