SACRAMENTO
STEPS FORWARD

Ending Homelessness. Starting Fresh.

REQUEST FOR PROPOSAL

Information Technology Services

For

Sacramento Steps Forward

INQUIRIES AND PROPOSALS SHOULD BE DIRECTED TO:

Chief Operating Officer
Sacramento Steps Forward
2150 River Plaza Drive, Suite 385
Sacramento, CA 95833
RFP@sacstepsforward.org

I. **GENERAL INFORMATION.**

I. **Purpose**. This request for proposal (RFP) is to contract for design, implementation, and on-call support services for a new Information Technology (IT) infrastructure at **Sacramento Steps Forward for a three-year period**

II. **Who May Respond**. Technology Consultants with in-person support services in Sacramento County.

III. **Instructions on Proposal Submission**.

1. **Closing Submission Date**. Proposals must be submitted no later than **11:59 pm** on **October 11, 2020**

2. **Inquiries**. Inquiries concerning this RFP should be emailed to:

Chief Operating Officer
Sacramento Steps Forward
2150 River Plaza Drive, Suite 385
Sacramento, CA 95833
RFP@sacstepsforward.org

3. **Conditions of Proposal**. All costs incurred in the preparation of a proposal responding to this RFP will be the responsibility of the Proposer and will not be reimbursed by Sacramento Steps Forward (hereinafter referred to as SSF).

4. **Instructions to Prospective Contractors**. Your proposal should be addressed as follows:

Chief Operating Officer
Sacramento Steps Forward
2150 River Plaza Drive, Suite 385
Sacramento, CA 95833

It is important that all proposals be sent to RFP@sacstepsforward.org with the subject line **"RFP for IT Services October 11, 2020"** and submitted in PDF format clearly marking in the lower left-hand corner of the cover page with the following information:

Request for Proposal
October 11, 2020
Proposal for IT Services

It is the responsibility of the Proposer to ensure that the proposal is received by SSF, by the date, time and in the manner specified above. Late proposals will not be considered.

5. Small and/or MinorityOwned Businesses. Efforts will be made by SSF to utilize small, women and/or minority owned businesses.

6. **Notification of Award**. It is expected that a decision selecting the successful proposal will be made within four (4) weeks of the closing date. Upon conclusion of final negotiations regarding the successful proposal, all other Proposers will be informed by email of the results. It is expected that the contract shall be a three-year contract, starting with an executed contract.

IV. **Description of Entity**. Sacramento Steps Forward (SSF), a private non-profit organization (State ID: C3356574) is committed to ending homelessness in our region through collaboration, innovation and connecting people to services. Walking side-by-side with our partners, we seek to provide people experiencing homelessness with the support and services they need to find stability and long-term housing.

Sacramento Steps Forward is the lead agency for the Sacramento Continuum of Care and as such, directly reports to the U.S. Department of Housing and Urban Development (HUD) on more than 20 different homeless service agencies. Agencies apply for funding through a competitive program that that uses performance metrics and expected program outcomes to allocate funds. Currently, 20 agencies are operating over 120 different programs that provide a wide range of services to people experiencing homelessness.

As the HUD designated administrator of the Homeless Management Information System (HMIS), Sacramento Steps Forward is responsible for Sacramento County's Annual Homeless Assessment Report, Housing Inventory Count, and Point-in-Time Count reports to HUD. In addition, Sacramento Steps Forward oversees and ensures quality control for monthly performance reports generated by HUD funded sub-recipients.

For direct outreach services, Sacramento Steps Forward generates 11 unique reports per month that provide a wide variety of information for funding agencies. Specific information includes demographics, housing resolutions, and service linkages.

Additional information on SSF, including our Annual Report, is available on our web site: https://sacramentostepsforward.org/

II. Background

Currently, SSF uses a G-Suite environment with on-call support services from Quorum Technologies. The agency has outgrown this environment and has started implementing Microsoft 365, One-Drive and SharePoint in expectation of the coordinated plan to move the functions described **Attachment A** into a coordinated Microsoft environment. **Attachment B** provides a list of software used at SSF.

While most staff use Microsoft laptops or workstations, around 30 percent use Apple Macbooks. SSF also has field staff, currently six, but historically larger, who use iPads or iPhones as their primary connection to email, documents and the HMIS. Currently, the Chief

Operating Officer supports all the mobile devices and requests assistance on laptops workstations and software when necessary. All software is procured through Tech Soup non-profit plans.

Most of the organization's staff use a large amount personally identifiable information regarding homeless clients and their history of program interactions in Sacramento County. Bit Focus' Clarity HMIS will continue to be the core database managing client data. The database is accessible through Software as a Service menus and through a read-only direct database access. SSF receives funding for these activites from the Department of Housing and Urban Development (HUD) A copy of the HUD's Data Security Policy is included in **Attachment C**.

Our organization's staffing plan includes an HMIS administrator and Lead Data Analyst who manage the relationship with BitFocus, and two-programmer data/analysts who maintain the processes that use client data. There is a desire across this team to create a regularly replicated version of the HMIS data tables on an internally accessible physical or cloud-based server to provide quicker access to queries and downloads than are currently available from BitFocus.

III. **SCOPE OF SERVICES**. Proposer shall be readily available to perform the following services, as requested by the Chief Operating Officer. The contracted services will include all services under Section A and potentially any of the additional lettered sections below that SSF may contract for independently:

A. Operationally support for one-year a network for SSF Offices that includes both cabled and secure Wi-Fi connection throughout a 4,593 square foot office space.

B. Provide Draft and Final Designs for SSF's IT Infrastructure, including costs for hardware, software, and annual software licensing costs. Draft Design should include:

1. Two separate options priced as separate line items with annual maintenance for servers. First Option, physically installed network servers. We envision the servers operating, a MySQL server with four terabytes of file storage that replicates the Bit Focus Clarity Sacramento and Yolo County HMIS Databases daily, a SFTP server with port forwarding access to the public network, a Tableau Server with port forwarding access to the public network, an eMail server with message and attachment encryption feature. General file storage could be configured on any above or located in Microsoft OneDrive configured as HIPPA Compliant. Second Option should include a discussion of how SSF could leverage existing cloud-based services to achieve the functions described above. This option may still require a locally installed version of MySQL for the replicated HMIS data but might save on infrastructure and maintenance costs. Both options should include costs for one-time infrastructure purchases on specific line items and estimated annual maintenance costs for software or subscriptions purchased through Tech Soup type providers for non-profits.
2. Help Desk support for eight hours a day seven days a week with 24/7 access to files and

databases.

3. List of recommended Microsoft applications functions and discuss any known migration issues or limitations from G-Suite.
4. Data Sharing – SFTP remote access PII Compliant access for internal and external requests with port forwarding. SFTP required.
5. VPN access for data servers under all options.
6. A one-year support plan that includes the following:
    a) On-going network security
    b) Network administration including permissions management and user administration.
    c) Identify and manage IT system vulnerabilities and risks
    d) Maintain the network and recommend changes to hardware, systems, policies, and processes, as needed.
    e) Ensure backup systems, security patches, and virus and malware updates occur.
    f) Develop and annual testing of Business Continuity Plan.
    g) Manage and schedule hardware replacement.
    h) Manage and schedule software upgrades.
    i) Consult and advise at least annually on how new technology can help SSF meet its operational goals.

C. Additional Years of Support – Provide options for multi-year support for SSF Technology excluding mobile devices.
D. Software – Optional – This option would include managing all software purchases through the IT Services Vendor with a list of all licenses accessible to SSF Staff.
E. Provide a Staff Training Plan and cost estimate that includes at least 10 hours of administrator training and at least 6 hours of live remote training on Microsoft Outlook, OneDrive and SharePoint software. Proposers should also include augmented staff support following the deployment of the system.
F. Provider a mobile device support plan that includes semi-annual checks for security compliance and software upgrade maintenance on each device.
G. Develop a Business Continuity Plan that supports remote access for all staff functions in the event of a pandemic or natural disaster.
H. Data Security Policy evaluation and update
I. On-call support for new initiatives – SSF will continue to search for new techniques and to discover new opportunities to better respond to crisis of homelessness. Staff may need additional support on short notice to pursue these opportunities. The Proposer's response should discuss their firm's capacity provide additionally priced support on short notice.

Although it is preferable for a firm to submit a proposal covering all of the above areas, SSF will consider proposals emphasizing expertise in subsets of these areas.

IV. **PROPOSAL CONTENTS.** The Proposer, in its proposal, shall, as a minimum, include the following:

A. **IT Experience**. The Proposer should describe its experience related to the areas outlined in the scope of services above. There is a particular interest in the following topic areas:

B. **Organization, Size, Structure, and Areas of Practice**. The Proposer should describe its organization in terms of the following:

- size,
- structure,
- areas of practice,
- office location(s), and
- if appropriate, if the firm is a small or minority-owned business.

Please include a copy of the Equal Opportunity/Affirmative Action Policy, if available.

C. **Qualifications**. The Proposer should separately attach a description of the qualifications of consultants to be assigned to the representation. Descriptions should include:

1. Professional experience with similar size organizations.
2. Professional experience migrating an organization to new software
3. References available for Help Desk Services including any historical information on response times.

D. **Price**. The Proposer's proposed price should include

1. Hourly billing rates of each staff who are expected to work on this project representation and charges for expenses.
2. Price to prepare standard contract for services.

E. Expected timeline for implementation.

V. PROPOSAL EVALUATION.

A. **Submission of Proposals**. All proposals shall consist of all documents together in one PDF format.

B. **Evaluation Procedure and Criteria**. SSF's CEO and appropriate staff will review proposals and make recommendations to the Board of Directors for final approval. The CEO and/or Board of Directors may request a meeting with some qualified Proposers prior to final selection.

Proposals will be reviewed in accordance with the following criteria:

1.	Proposed approach to scope of work	20 points
2.	Level of experience of the individuals identified to work on this matter	20 points
3.	Proposer's experience with similar clients	20 points
4.	Cost Consciousness	40 points
5.	Interviews, if conducted,	additional 25 points

C. **Required Format for Proposals.** All proposals must follow the required format. Failure to follow the required format may result in disqualification of a proposal:

1. Page Limit: 13, including cover page
2. Page Size: 8 ½ x 11; portrait
3. Font Size: 12
4. Font Type: Arial
5. Margins: 1" minimum on the top, bottom, and sides of all pages
6. All pages must be numbered

V. PROPOSAL/PROJECT TIMELINE.

During the period from your organization's receipt of this Request for Proposals and until a contract is awarded, your organization shall send all questions to SFF at RFP@sacstepsforward.org. Dates following contract award below are estimated based on the organizational need.

Release RFP Date: September 9, 2020
Question Submission Deadline: September 23, 2020, 11:59pm
Question Response Deadline: September 30, 2020, 11:59pm
Proposal Submission Deadline: October 11, 2020, 11:59pm
Contractor Selection Date: October 16, 2020
Contract Execution Date: October 23, 2020
Project Start Date: October 30, 2020
SSF New IT Infrastructure Implementation and Training Begins: November 23, 2020

VI. QUESTIONS.

Questions for the purpose of clarifying the RFP must be submitted **in writing by email** to RFP@sacstepsforward.org and must be received no later than **11:59 p.m. on September 23, 2020**. All questions and responses will be posted on https://sacramentostepsforward.org/ by 5:00 PM on September 30, 2020.

VII. RESERVATION OF RIGHTS.

A. **Contract Award**

SSF reserves the right to award the contract in a manner deemed to be in the best interests of SSF.

SSF reserves the right to reject any or all proposals, to waive any informality in the RFP process, or to terminate the RFP process at any time, if deemed by SSF to be in its best interests.

B. **Stability of Proposed Prices**

Any price offerings from Proposers must be valid for a period of 45 days from the due date of the proposals.

C. **Amendment or Cancellation of the RFP**
SSF reserves the right to cancel, amend, modify, or otherwise change this RFP at any time if it deems it to be in the best interests of SSF.

D. **Proposal Modifications**
No additions or changes to any proposal will be allowed after the proposal due date, unless such modification is specifically requested by SSF in writing. SSF, at its option, may seek Proposer retraction and clarification of any discrepancy or contradiction found during its review of proposals.

E. **Proposer Presentation of Supporting Evidence**
Proposers must be prepared to provide any evidence of experience, performance, ability, and/or financial surety that SSF deems necessary or appropriate to fully establish the performance capabilities represented in their proposals.

F. **Proposer Demonstration of Proposed Services and/or Products**
Proposers must be able to confirm their ability to provide all proposed services.

G. **Erroneous Awards**
SSF reserves the right to correct inaccurate awards. This includes revoking the awarding of a contract to a Proposer and subsequently awarding the contract to a different Proposer. Such action shall not constitute a breach of contract on the part of SSF because the contract with the initial Proposer will be deemed voided as if no contract were ever in place.

H. **Ownership of Proposals**
All proposals shall become the property of SSF and will not be returned.

I. **Ownership of Subsequent Products**
Any product, whether acceptable or unacceptable, developed under a contract awarded as a result of this RFP shall be the sole property of SSF unless otherwise stated in the contract.

J. **Oral Agreement or Arrangements**
Any alleged oral agreements or arrangements made by Proposers with SSF will be disregarded in any proposal evaluation or associated award.

K. **Not a Contract**
This RFP is not a contract and, alone, shall not be interpreted as such. Rather, this RFP serves only as the instrument through which proposals are solicited. SSF will pursue negotiations with the highest scoring proposal. If, for some reason, SSF and the initial Proposer fail to reach consensus on the issues relative to a contract, then SSF may commence contract negotiations

with other Proposers. SSF may decide at any time to start the RFP process again. The selected Proposer will be required to sign a formal contract.

L. **Subcontractors**

SSF must approve, in writing, any and all subcontractors utilized by the successful Proposer prior to any such subcontractor commencing any work. Proposers acknowledge by the act of submitting a proposal that any work provided under the contract is work conducted on behalf of SSF and that the SSF CEO or designee may communicate directly with any subcontractor as SSF deems necessary or appropriate.

It is also understood that the successful Proposer shall be responsible for all payment of fees charged by the subcontractor(s). A performance evaluation of any subcontractor shall be provided promptly by the successful Proposer to SSF upon request. The successful Proposer must provide the majority of services described in the specifications.

Attachment A
SSF Agency IT Existing Profile by Functional Area

Leadership/Admin/Contract - 8 staff

- Communication/Data Collection: Workstation with email, chat and call abilities.
- Network Connectivity/File Sharing: Internet, Google Drives
- Current File Storage: Google Drive
- Additional Software:

Outreach - 5 staff

- Communication/Data Collection: Agency issue iPhone iPads. Workstation with email, chat and call abilities.
- Network Connectivity: Sharesync secure file storage and file transfers, Internet, Google Drives
- Live connection Bit Focus software
- File Storage: Google Drive
- Additional Software: None

CES Team – 7 staff

- Communication: Agency softphone, Workstation with email, chat and call abilities.
- Network Connectivity: Secure access to file storage: Live connection Bit Focus Database. Connection to replicated MS SQL Server database for data analysis. Internet, Google Drives
- File Storage: Google Drive
- Additional Software: Tableau, Viscosity DB connection

COC Team – 4 Staff

- Communication/Data Collection: Workstation with email, chat and call abilities.
- Network Connectivity/File Sharing: Google Drives
- File Storage: Google Drive
- Additional Software: None

Communications/Strategic Initiatives Team – 2 staff

- Communication/Data Collection: Workstation with email, chat and call abilities.
- Network Connectivity/File Sharing: Secure access for file transfer: Google Drives
- File Storage: Google Drive
- Additional Software: None

Data Analytics – 4 staff

- Communication: Agency softphone, Workstation with email, chat and call abilities.
- Remote secure VPN access to the MySQL server, Tableau server, SFTP server, and the file storage system
- Network Connectivity: Secure access to file storage: Live connection Bit Focus Database. Connection to replicated MS SQL Server database for data analysis.
- File Storage: Google Drive, **SFTP Strongly Desired**
- Additional Software: Tableau, Viscosity DB connection

Finance Team – 2 staff

- Communication/Data Collection: Workstation with email, chat and call abilities.
- Network Connectivity/File Sharing: Secure access for file transfer: Google Drives
- File Storage: Google Drive
- Additional Software: QuickBooks – 5 instances

System Performance Team – 2 Staff

- Communication: Agency softphone, Workstation with email, chat and call abilities.
- Network Connectivity: Secure access to file storage: Live connection Bit Focus Database. Connection to replicated MS SQL Server database for data analysis. Internet, Google Drives
- File Storage: Google Drive
- Additional Software: Tableau, Viscosity DB connection

Attachment B
SSF Current IT Infrastructure Inventory

5 iPhone 7s
2 iPhone 6s
28 PC Laptops
4 Macbooks

Network Controllers: **Note: These will be used to for the WiFi Network in the new office.**

2 Cisco Air AP 1852E Access Points
1 Cisco 3504 Wireless Controller
1 Cisco ASA 5516 Security Appliance
1 Cisco 2960 Managed Switch

Desktop Software

- Microsoft Windows
- Microsoft Office 365
- Google Chrome
- Mozilla Firefox
- Adobe Acrobat 11 Standard
- R/Python
- Tableau
- Quick Books

Attachment C
SSF Data Security Plan

Appendix C

U.S. DEPARTMENT OF HOUSING AND URBAN DEVELOPMENT

INFORMATION TECHNOLOGY SECURITY POLICY

HUD Handbook 2400.25 REV4

August 2014

Document Change History

Version Number	Date	Description	Author
2.0	November 2006	Revised to match latest draft of NIST framework and incorporate new HUD requirements	N/A
2.1	April 2007	Revised to match latest draft of NIST framework and incorporate new HUD requirements	N/A
2, CHG-1	November 2009	Revised to and incorporate new HUD requirements	N/A
2, CHG-2	August 2011	Revised to incorporate new HUD requirements	N/A
3.0	August 2013	Revised to incorporate NIST v3 and new HUD requirements	N/A
4.0	March/May 2014	Revised to incorporate NIST v4 and new HUD requirements	Cyrus Management Solutions, LLC

Table of Contents

1.0 INTRODUCTION

The U.S. Department of Housing and Urban Development (HUD) relies extensively on information systems 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, guidance and HUD security policies and procedures.

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

All HUD components must comply with the basic requirements of this policy and its associated operational standards and technical documentation. Also, for each component, it must be determined if there is any need for additional safeguards that exceed beyond this baseline level. Additional safeguards should be based on an assessment of risk and local conditions and then implemented appropriately.

1.1. Purpose

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

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

1.2. Scope

This policy provides a comprehensive view of information security considerations. It addresses technical security services, as well as the management and operational requirements for information security. It identifies all relevant security roles and responsibilities and affected organizations. It also reflects the increasing requirements needed for internal and external security oversight from the HUD Office of Inspector General (OIG) and for responding to the requirements of the Federal Information Security Management Act (FISMA).

This policy is intended to provide a set of basic protection goals and standards; however, the procedural details normally found in operational and technical documentation are not within the scope of this document. Procedures supporting the HUD information security policies are defined in the document, HUD *Information Technology Security Procedures*.

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

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

As a result, this policy has implications for more than Security Specialists and will affect System Owners, developers, practitioners of non-IT security disciplines, operations personnel (e.g., security training and awareness personnel, contract managers), and personnel interacting with the HUD Privacy Officer, Office of the Inspector General, external auditors, HUD Enterprise Architecture organization, developers, and other agencies.

The policy applies to all HUD employees, contractors, and service providers and requires compliance with day-to-day provisions of HUD policy (e.g. proper password choice and management, security awareness maintenance, incident reporting, and prompt system upgrades).

As important, this information security policy applies to HUD Program Offices that have security-specific or security-relevant roles and responsibilities, such as system security planning, security assessment and authorization, security audit, configuration management, continuity of operations activities, and security incident response.

1.3. Authority for Policy

The authority for the issuance of this policy rests with the HUD Chief Information Officer (CIO) and is assigned to the Office of Information Technology Security (OITS).

1.4. Policy Basis

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

This document 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 the NIST Special Publication (SP) 800-53, *Recommended Security Controls for Federal Information Systems, as amended,* with HUD-specific requirements.

1.5. NIST Framework

To simplify compliance with FIPS 200 and NIST SP 800-53, as amended, the HUD policies are organized by "NIST class and family." This format facilitates preparing security documentation, as required in the HUD Project Planning and Management (PPM) Life Cycle v. 2.0, and establishing the security assessment criteria used during the security authorization and accreditation process.

As each new class begins, there is an overview and description of the class and associated controls. At the beginning of each family, the FIPS 200 requirement is documented to establish the framework, followed by the associated NIST SP 800-53, as amended, security control. Each

control is labeled with the NIST control number; the two letters indicate the control family followed by the sequential number within the family. For example, PE-7 is the seventh control in the Physical Security family.

The numbering scheme in the document relates to the order of controls within NIST SP 800-53, as amended. For example, Section Number 3.1.1 represents the *Management* class, *Risk Assessment* family, and the first control within the family, the *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; and 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- Policy Organization Framework) by NIST or through an assessment of risk to individual information systems.

X.0 Class

A brief overview of the class – management, operational, and technical

X.1 Family

A brief description of each of the seventeen FIPS 200 requirements and supporting NIST SP 800-53 families

FIPS 200 Requirement
Text of FIPS 200 requirement

...

X.1.2 Specific NIST SP 800-53 Control

NIST SP 800-53 Control: XX-2
XX-2: Text of NIST SP 800-53 Control and required baseline *Security Baseline: Low, Moderate, and High*
E-1: Text of Control Enhancement, if provided by NIST and required baseline *Security Baseline: Low, Moderate, and High*
HUD Policy: 3.1.2 *Text of HUD security policy requirement that is related to the NIST SP 800-53 control*

Figure 1. Policy Organization Framework

When a HUD-specific policy is not addressed in NIST SP 800-53 Rev 4 security controls, the HUD-specific requirement is placed within a NIST class and control family. These additional controls are inserted at the end of the control family. HUD-specific policy requirements are labeled with HUD, followed by the two letters that indicate the control family, followed by a

sequential letter within the family. For example, HUD-PL-B is the second HUD-specific requirements within the planning family, and is included at the end of the planning family (see Figure 2 - HUD-Specific Policy Sample).

3.2.8 ISSO

HUD Policy: HUD-PL-B
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. Security Baseline: Low, Moderate, and High

Figure 2. HUD-Specific Policy Sample

The first control within each family is a requirement to develop policies and procedures for that family. These controls are satisfied by this document, the HUD *Information Technology Security Policy Handbook 2400.25 Rev. 4* and the supporting HUD *Information Technology Security Procedures*. Therefore, the Supporting Procedures section is replaced with an Implementation section as seen in Figure 3 – Initial Policy and Procedure Control Sample.

NIST SP 800-53 Control: MP-1
MP-1: The organization: a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]: 1. A Media Protection Policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the media protection policy and associated media protection controls. b. Reviews and updates the current: 1. Media Protection Policy [Assignment: organization-defined frequency]; and 2. Media protection procedures [Assignment: organization-defined frequency]. Security Baseline: Low, Moderate, and High
Implementation
This control is implemented by the *Information Technology Security Policy, Handbook 2400.25 Rev. 4,* that defines HUD's formal security policies and the HUD *Information Technology Security Procedures* that defines HUD's formal security procedures. HUD reviews the policies and procedures minimally every year or when impacted by a significant change or underlying standard. The HUD security policies and procedures are disseminated via the HUD Intranet for all HUD's users to access.

Figure 3. Initial Policy and Procedure Control Sample

1.6. Relationship to Other Documents and Processes

As the primary information source for fundamental requirements for maintaining the confidentiality, integrity, and availability of IT resources, the policy identifies and characterizes a comprehensive set of basic protection goals without stipulating how the goals should be met (i.e., the specific technologies, mechanisms, or procedures involved). Procedural details are documented separately.

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

The requirements of this policy complement other agency measures for effective management of assets and regulatory compliance (e.g., with the federal privacy laws). References are made to those sources throughout this document (latest version published shall be sought regarding all references).

Guidance on HUD information security standards, methodologies, procedures, and adaptations to ongoing legislation and federal regulations and standards is expanded in the *Information Technology Security Procedures* document. The procedures document provides guidance on how to implement information security policies with examples that include password enforcement mechanisms, auditing procedures, and incident-response procedures.

Where necessary, the most detailed, procedure-intensive or volatile information security guidance will be issued in topic-specific guidelines. Generally, technical specialists are the principal users of such guidelines (e.g., specifications of product version-specific configuration settings, detailed security assessment and authorization guidance, or business continuity procedures).

This Handbook becomes the foundation for secure HUD information system design, operation, and maintenance.

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

1.7. Laws and Regulations

HUD established a department-wide information security policy based on the following Executive Orders (EO), public laws, and national policies: (latest version published shall be sought regarding all references).

- Electronic Government Act (includes FISMA) (Public Law [P.L.] 107-347), December 2002

- Federal Information Security Management Act (FISMA) (P.L. 107-347), December 2002
- Paperwork Reduction Act (P.L. 104-13), May 1995
- Section 508 of the Rehabilitation Act of 1973
- Government Paperwork Elimination Act (P.L. 105-277), October 1998
- Privacy Act of 1974, as amended, (P.L. 93-579), December 1974
- Clinger-Cohen Act (P.L. 104–106), February 1996
- USA Patriot Act (P.L. 107-56), October 2001
- Electronic Signatures in Global and National Commerce Act (P.L. 106-229), June 2000
- Health Insurance Portability and Accountability Act (P.L. 104-191), 1996
- Office of Management and Budget, Circular A-130, Appendix III, Transmittal Memorandum #4, *Management of Federal Information Resources*, November 2000
- Office of Management and Budget Memorandum M-03-19, *Reporting Instructions for the Federal Information Security Management Act and Updated Guidance on Quarterly IT Security Reporting,* August 2003
- Office of Management and Budget Memorandum M-03-22, *OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002,* September 2003
- Office of Management and Budget Memorandum M-04-04, *E-Authentication Guidance for Federal Agencies*, December 2003
- Office of Management and Budget Memorandum M-05-24, *Implementation of Homeland Security Presidential Directive (HSPD) 12—Policy for a Common Identification Standard for Federal Employees and Contractors*, August 2005
- Office of Management and Budget Memorandum M-06-20, *FY 2006 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*, July 2006
- Office of Management and Budget Memorandum M-06-16, *Protection of Sensitive Information*, June 2006
- Office of Management and Budget Memorandum M-06-19, *Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments*, July 2006
- FIPS 140–2, *Security Requirements for Cryptographic Modules*, May 2001
- FIPS 199, *Standards for Security Categorization of Federal Information and Information Systems*, February 2004
- FIPS 200, *Minimum Security Requirements for Federal Information and Information Systems*, March 2006
- FIPS 201-1, *Personal Identity Verification for Federal Employees and Contractors*, March 2006
- NIST Special Publications
- General Accounting Office, *Federal Information Systems Controls Audit Manual* (FISCAM), January 1999

1.8. Exceptions

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

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 programs. The CIO appoints, in writing, the CISO and reviews and evaluates the HUD Information Security Program at least annually.

2.3. Senior Agency Information Security Officer

The HUD Senior Agency Information Security Officer (SAISO) is the CISO. The CISO directs the management of HUD's Information Security Program. The CISO, with the support of the OITS staff, establishes a strong foundation for HUD security by maintaining the HUD information security program. The CISO interacts with internal and external resources, sponsors an Information System Security Forum, and coordinates security compliance across HUD's organizational elements. The CISO serves as the CIO's primary liaison with the HUD's authorizing officials, information system owners, and Information Security System Officers (ISSO's).

2.4. Risk Executive

A Risk Executive ensures that risks are managed consistently across the organization. The Risk Executive provides a holistic view of risk beyond that associated with the operation and use of individual information systems. The Risk Executive inputs are documented and become part of the security authorization decision. The HUD CIO should be the HUD Risk Executive. (The

HUD CISO may be designated by the HUD CIO as the Risk Executive.) The Risk Executive will:

- Ensure that the management of information system-related security risks is consistent across the HUD organization, reflects organizational risk tolerance, and is performed as part of a HUD-wide process that considers other organizational risks affecting mission/business success;
- Ensure that information security considerations for individual information systems, including the specific authorization decisions for those systems, are viewed from a HUD-wide perspective with regard to the overall strategic goals and objectives of the organization;
- Provide visibility into the decisions of Authorizing Officials and a holistic view of risk to the organization beyond the risk associated with the operation and use of individual information systems; and
- Facilitate the sharing of security-related and risk-related information among authorizing officials and other senior leaders within HUD in order to help officials consider all types of risks that may affect mission and business success and the overall interests of HUD at large.

2.5. Office of Information Technology Security

The 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. The OITS reviews and approves the processes, techniques, and methodologies planned for securing information system assets.

2.6. Physical Security/Facilities Group/Security Officer

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

The Physical Security Officer and security staff will:

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

2.7. Deputy Chief Information Officer for Infrastructure and Operations (IOO)

The Deputy CIO for IOO is responsible for the IT infrastructure (e.g., general support systems) that provides shared services across HUD and ensuring the implementation of security components to secure these information system assets.

2.8. HUD Computer Incident Response Team

The HUD Computer Incident Response Team (CIRT) administers the incident response program to include monitoring, tracking, response coordination and reporting of HUD computer security incidents. HUD-CIRT manages and responds to computer security incidents that involve HUD systems and data, to help improve the overall security posture of HUD by independently verifying the security of HUD systems, and to ensure the timely dissemination of security information to the appropriate stakeholders.

2.9. HUD Chief Privacy Officer

The HUD Privacy Officer assures that service and service arrangement meet privacy policies regarding the protection, dissemination, and disclosure of information. The Chief Privacy Officer must review program and system Privacy Threshold Analyses (PTAs), Privacy Impact Assessments (PIAs), and System of Records Notices (SORNs), providing approval as appropriate. Ultimately, the HUD Chief Privacy Officer is responsible for the HUD Privacy Policy and its compliance.

2.10. Office of the Chief Procurement Officer (OCPO)

The Office of the Chief Procurement Officer (OCPO) ensures that HUD contracts for IT systems and services include the appropriate information security requirements. The OCPO, along with the OITS, other interested stakeholders (e.g., the program office sponsoring the acquisition) and the Office of General Counsel, develops IT security contract clauses, and other contract terms and conditions, as appropriate. The contract terminology is based on current federal and HUD policies, regulations, and guidance for the HUD information systems and services.

2.11. Contracting Officer

The HUD Contracting Officers (COs) have authority to enter into, administer, and terminate contracts up to the limit of their individual delegations of authority. For the IT systems and services contracts, the CO will ensure that:

- New contracts include appropriate clauses and other terms and conditions to enforce HUD IT security policy including the requirements for:
  - The contractor to conduct IT security awareness training for its employees and, where appropriate, role-based training for specific job categories with security responsibilities;

  - The contractor's compliance with HUD computer security incident identification and reporting policy and procedures;
  - The contractor and any subcontractors to provide copies of their internal IT security plans and procedures to the CISO upon request;
  - To perform site surveys at non-HUD facilities by qualified HUD security representatives (e.g., CISO, ISSO, or other designated HUD Program Office personnel);
- New contracts incorporate IT security functional and assurance requirements in accordance with the HUD IT Security Policy;
- All IT security terms and conditions comply with departmental acquisition policy, the HUD Acquisition Regulation (HUDAR), the Federal Acquisition Regulation (FAR), and applicable statutes and government-wide policies; and,
- Existing contracts are modified, when necessary, to include appropriate terms and conditions to enforce HUD IT Security Policy (as described above), in the event:
  - The contracts did not originally include such terms and conditions at time of award,
  - The contract's requirements have changed subsequent to award to require such terms and conditions, or
  - Such terms and conditions should have been included at time of contract award.

2.12. Contracting Officer Representative

In accordance with the HUD Handbook 2210.3, "Procurement Policies and Procedures," the Contracting Officer Representative (COR) acts as the Contracting Officers' representative in all matters concerning the technical (i.e., not contractual) aspects of a contract. The COR is often the department's primary point of contact with a contractor, giving contractors technical guidance related to the work required by the contract. The COR is also the principal judge of a contractor's performance, including the quality and timeliness of work and when appropriate the contractor's ability to control costs of performance. Typically, the COR is an employee of the HUD Program Office initiating a contract. Security responsibilities will also be included in the annual performance plans for CORs assigned to contracts to which IT security requirements are applicable.

The COR is responsible for overseeing a subdivision of the overall contract (e.g., monitoring the services provided by a contractor to a specific field office under a nationwide contract) or a specific aspect of the contract. The COR may be from the program office that initiates a contract action or from another part of HUD that is associated with the work done under the contract. A COR may be delegated many duties. Chapters 11 and 12 of the HUD Handbook 2210.3, provide detailed guidance on the COR's functions and responsibilities. For most HUD information technology (IT) contract resources, the COR fulfills the role of the Technical Project Manager and as such, is responsible for understanding the scope of the contract or task order, its associated tasks, and deliverables. For the majority of HUD's IT contracts, the COR function is delegated to a representative from the OCIO. The following duties and responsibilities are usually delegated to the COR for IT contracts:

- Developing the statements of work or objectives;
- Initiating Request for Contract Services (RCS) packages;

- Participating in technical proposal evaluations;
- Monitoring contractor performance, including reviewing schedule, costs, and deliverables, and providing official feedback to the CO monitoring the contract;
- Serving as the liaison between the contractor, the program sponsor, and the COR; and
- Ensuring on a routine basis that the contractor is providing appropriate, timely and quality service to the customer and bringing to the attention of the COR any issues with the contract or any disagreements over scope, deliverables, schedule or cost.
- Ensuring that new IT development and maintenance contracts include deliverables of system documentation and updates, as required, documenting significant changes. The system documentation and updates are required for security assessment and authorization, corrective action plans, audits, etc.
    - Therefore, when requested, the OCIO COR is also responsible for providing technical guidance and information to the system owner to assist in resolving data calls.

The COR may appoint any individual in the sponsoring office or OCIO who meets HUD's qualification and certification requirements for a COR. Security responsibilities will also be included in the annual performance plans for those CORs assigned to contracts in which IT security requirements are applicable.

2.13. Office Technical Coordinator

The Office Technical Coordinator (OTC) is a designated HUD staff member that assists Program Office personnel on a variety of issues that may include obtaining local area network (LAN) and email access, office space, data security, and computer hardware and software resources. The OTC interfaces with the IOO staff, as needed, to help resolve IT problems.

2.14. Office of the Chief Human Capital for Services

The Office of the Chief Human Capital Officer, Office of Human Capital for Services (OCHCO) 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.

2.15. Office of the Inspector General

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

2.16. HUD General Counsel

The HUD Office of General Counsel (OGC) develops security clauses, as appropriate, based on current federal and HUD policies, regulations, and guidance for HUD information systems and services in conjunction with the OITS and OCPO.

2.17. Configuration Control Management Board

The Configuration Control Management Board (CCMB) serves as the decision-making body for vendor-specific system changes, as well as approving requested changes in accordance with HUD policies and procedures.

2.18. System Owner

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 information systems and ultimately accountable for the security of their information systems. System Owners are also responsible for implementing management, operational, and technical security controls to ensure that they are effective in protecting the information and information systems under their purview. Moreover, System Owners are responsible for ensuring that System Owners of major and minor applications coordinate with System Owners of General Support Systems (GSS) that host their applications so they can better determine the adequacy of those GSS security controls, and identify and implement compensatory controls when vulnerabilities in the GSS controls exist. Security responsibilities must be included in the annual performance plans. Additionally, System Owners must ensure that:

- An ISSO is designated (in writing) for each information system under their purview;
- Security Assessment and Authorization (SA&A) and continuous monitoring activities are completed; and
- Plan of Action & Milestones (POA&Ms) are maintained and reported.

2.19. Common Control Provider

The Common Control Provider is an organizational official responsible for the planning, development, implementation, assessment, authorization, and maintenance of common controls. In most cases, the System Owner is the Common Control Provider. The Common Control Provider must ensure the Security Plans, Security Assessment Reports (SARs), and POA&Ms for common controls are accessible to the information system owners inheriting those controls after the information is reviewed and approved by a senior official.

2.20. 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. The ISSOs are the principal points of contact (POCs) for information systems security and actively participate in the Information Security System Forum. They are responsible for all security aspects of their assigned systems from inception through disposal, as well as for ensuring system availability. An ISSO must be designated for every information system and serve as the POC for all security matters related to that information system. Security responsibilities will be included in their annual performance plans.

2.21. 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. They must maintain an environment that creates a strong technical foundation for enforcement of information system security.

2.22. System Security Administrator

The System Security Administrator (SSA) is responsible for approving access to the data in an application. The SSA grants/modifies/revokes user access via the Centralized HUD Account Management Process (CHAMP). Security responsibilities will be included in the SSAs annual performance plans.

2.23. Security Control Assessor

The Security Control Assessor (SCA) is an individual, group, or organization responsible for conducting a comprehensive assessment of the management, operational, and technical security controls employed within or inherited by an information system to determine the overall effectiveness of the controls (i.e., the extent to which the controls are implemented correctly, operate as intended, and produce the desired outcome with respect to meeting the security requirements for the system).

2.24. 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 for 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, empowering them to make certain decisions regarding the planning and resources for security activities, acceptability of security and/or SA&A 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.

2.25. 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.

2.26. 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 that provide services and resources to HUD.

The User must:

- Comply with the HUD Information Security Policy and apply the defined guidance to their daily work activities;
- Enforce the Information Security Policy and ensure that employees and contractors comply with the information security policies and procedures;
- Assume accountability for protecting sensitive information under their control in accordance with this Policy;
- Attend and/or participate in the annual Information Security Awareness training;
- Attend the required role-based security training pertaining to those having a security-related role (e.g., system and network administrators);
- Report information security incidents (e.g., virus and malicious code attacks) to HUD-CIRT according to the established and documented procedures;
- Cooperate with the HUD-CIRT team members in the investigation of security incidents;
- Cooperate with the Information Security Program representatives or other designated HUD Program Office personnel during security compliance reviews/audits at HUD Program Office facilities and/or during site surveys at non-HUD facilities;
- Ensure that information security data is collected in accordance with direction from the CISO and/or ISSO, Managers, or Supervisors; and
- Understand and comply with HUD policies, standards, and procedures regarding the protection of sensitive HUD information assets.

2.27. 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/roles as defined in those plans.

2.28. Service Provider

Service Providers include vendors, contractors, other federal government organizations and entities that provide IT services, information systems, and facilities housing HUD information systems. Service Providers are responsible for ensuring and maintaining security controls are compliant with HUD security policy and procedures.

2.29. Office of Customer Relations and Performance Management (OCRPM)

The Office of Customer Relations and Performance Management (OCRPM) Project Leaders and COR staff are responsible for working with the System Owners to perform as Technical Leads for the following tasks:

- Application Security Plan initial development in accordance with NIST Special Publication 800-18, as amended;
- Application Security Plan review and update on an annual basis in accordance with NIST Special Publication 800-18, as amended;
- Application Security Plan review and update at any point in time that a change is made to application software or system function which affects security controls in accordance with NIST Special Publication 800-18, as amended, to be completed prior to the production status for the changes involved;
- The initial development of a Business Impact Analysis(BIA) in accordance with NIST Special Publication 800-34;
- Business Impact Analysis review and update on an annual basis in accordance with NIST Special Publication 800-34;
- Business Impact Analysis update at any point in time that a change is made to application software which affects system function or infrastructure support configuration;
- The initial development of an Application Risk Assessment in accordance with NIST Special Publication 800-30, as amended;
- Application Risk Assessment review and update on an annual basis in accordance with NIST Special Publication 800-30; and
- Application Risk Assessment review and update at any point in time that a change is made to application software or system function which affects security controls in accordance with NIST Special Publication 800-30, to be completed prior to production status for the changes involved.

Security responsibilities of the OCRPM Project Leaders will be included in their annual performance plans.

2.30. Developers

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

2.31. User Representative

User Representatives are individuals that represent the operational interests of the user community and serve as liaisons for that community throughout the system development life cycle of the information system. The User Representative assists in the security assessment and authorization (SA&A) process, when needed, to ensure mission requirements are satisfied while meeting the security requirements and employing the security controls defined in the System Security Plan (SSP).

3.0 MANAGEMENT POLICIES

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.

3.1. Risk Assessment

Risk Assessment is a process to identify system security risks, determine the impact if the event occurred, and select safeguards that protect, mitigate, or eliminate this impact. Risk management is a process that allows Program Offices to balance the operational and economic costs of protective measures to achieve gains in mission capability by protecting the information systems and information that support their organization's missions.

The following policies 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

The following policy addresses the requirement for developing, implementing, and maintaining risk assessment policy and procedures.

NIST SP 800-53 Control: RA-1
The organization: a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]: 1. A risk assessment policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the risk assessment policy and associated risk assessment controls; and b. Reviews and updates the current: 1. Risk assessment policy [Assignment: organization-defined frequency]; and 2. Risk assessment procedures [Assignment: organization-defined frequency]. Security Baseline: Low, Moderate, and High
Implementation
This control is implemented by the *Information Technology Security Policy, Handbook 2400.25 Rev. 4* that defines HUD's formal security policies and the HUD *Information Technology Security Procedures* that defines HUD's formal security procedures. HUD reviews/updates the policies and procedures minimally every year or when impacted by a significant change or underlying standard. The HUD security policies and procedures are disseminated via the HUD Intranet for all HUD's users to access.

3.1.2. Security Categorization

The FIPS Pub 199, *Standards for Security Categorization of Federal Information and Information Systems,* provides a common framework and understanding for expressing the security needs of federal information and information systems.

The framework establishes security categories based on the potential impact on an organization's ability to accomplish its mission should its information and information systems experience a breach of confidentiality, integrity or availability. A loss of ***confidentiality*** is the unauthorized disclosure of information; a loss of ***integrity*** is the unauthorized modification or destruction of information; a loss of ***availability*** is the disruption of access to, or use of, information or an information system. The framework defines three levels of impact: *low, moderate, high;* the application of these definitions takes place within the context of each organization's mission and interest.

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

The following policy provides relevant guidance to ensure that there is consistency in the security categorization.

NIST SP 800-53 Control: RA-2
RA-2: The organization: a. Categorizes information and the information system in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance; b. Documents the security categorization results (including supporting rationale) in the security plan for the information system; and c. Ensures the security categorization decision is reviewed and approved by the authorizing official or authorizing official designated representative. Security Baseline: Low, Moderate, and High
HUD Policy: 3.1.2 a. Program Offices/System Owners are responsible for ensuring that all systems and information under their control have been categorized in accordance with FIPS 199, *Standards for Security categorization of Federal Information and Information Systems,* following the guidance in NIST SP 800-60 Rev.2, *Guide for Mapping Types of Information and Information Systems to Security Categories*. b. Program Offices/System Owners review and validate, annually, their categorization decisions and supporting rationale. This can be accomplished as part of the annual security assessment. c. Program Offices and System Owners shall maintain an accurate record of the system categorization in HUD's centralized information security management tool, CSAM, and the Inventory of Automated Systems (IAS). Additionally, System Owners must ensure that the Authorizing Official reviews and approves the security categorization decision.

3.1.3. Risk Assessment

Assessing the risks to HUD information and information systems provides the necessary information for Program Offices and System Owners to make well-informed risk management decisions related to acceptable risk levels. The following policy defines how risk assessments are conducted for HUD information systems and the frequency of the risk assessments.

NIST SP 800-53 Control RA-3
RA-3: The organization: a. Conducts an assessment of risk, including the likelihood and magnitude of harm, from the unauthorized access, use, disclosure, disruption, modification, or destruction of the information system and the information it processes, stores, or transmits; b. Documents risk assessment results in [Selection: security plan; risk assessment report; [Assignment: organization-defined document]]; c. Reviews risk assessment results [Assignment: organization-defined frequency]; d. Disseminates risk assessment results to [Assignment: organization-defined personnel or roles]; and e. Updates the risk assessment [Assignment: organization-defined frequency] or whenever there are significant changes to the information system or environment of operation (including the identification of new threats and vulnerabilities), or other conditions that may impact the security state of the system. Security Baseline: Low, Moderate, and High
HUD Policy: 3.1.3 a. System Owners must conduct risk assessments for all systems under their purview, in accordance with the NIST SP 800-30, *Guide for Conducting Risk Assessments*, as amended, to support Authorizations to Operate (ATO). b. System Owners must document the risks assessment results within CSAM. c. Systems Owners monitor and assess the risks annually or whenever there are significant changes to the information system or environment of operation for all systems to ensure the risk assessment remains accurate and up-to-date. Acceptable annual assessments can include the annual FISMA self-assessment, annual validation of the system categorization decision, business impact assessments, and security control compliance reviews. d. System Owners shall assess security risks when a significant change is planned for any system under their control. e. Any changes or updates must be noted and maintained in the Department's central security management tool, CSAM.

3.1.4. Vulnerability Scanning

A vulnerability is a weakness in an information system, system security procedure, internal control, or implementation that could be exploited or triggered by a threat. HUD must conduct periodic vulnerability assessments to determine security risks that should be mitigated. The following policy identifies the needs for vulnerability scans and the frequency of the scans.

NIST SP 800-53 Control: RA-5
RA-5: The organization: a. Scans for vulnerabilities in the information system and hosted applications [Assignment: organization-defined frequency and/or randomly in accordance with organization-defined process] and when new vulnerabilities potentially affecting the system/applications are identified and reported; b. Employs vulnerability scanning tools and techniques that facilitate interoperability among tools and automate parts of the vulnerability management process by using standards for: 1. Enumerating platforms, software flaws, and improper configurations; 2. Formatting checklists and test procedures; and 3. Measuring vulnerability impact; c. Analyzes vulnerability scan reports and results from security control assessments; d. Remediates legitimate vulnerabilities [Assignment: organization-defined response times] in accordance with an organizational assessment of risk; and e. Shares information obtained from the vulnerability scanning process and security control assessments with [Assignment: organization-defined personnel or roles] to help eliminate similar vulnerabilities in other information systems (i.e., systemic weaknesses or deficiencies). Security Baseline: Low, Moderate and High
E-1: The organization employs vulnerability scanning tools that include the capability to readily update the information system vulnerabilities to be scanned. Security Baseline: Moderate and High
E-2: The organization updates the information system vulnerabilities scanned [Selection (one or more): [Assignment: organization-defined frequency]; prior to a new scan; when new vulnerabilities are identified and reported]. Security Baseline: Moderate and High
E-4: The organization determines what information about the information system is discoverable by adversaries and subsequently takes [Assignment: organization-defined corrective actions]. Security Baseline: High
E-5: The information system implements privileged access authorization to [Assignment: organization-identified information system components] for selected [Assignment: organization-defined vulnerability scanning activities]. Security Baseline: Moderate and High
HUD Policy: 3.1.4 a. OCIO ensures HUD's infrastructure, including the LAN, wide area network (WAN), Internet, Intranet, Enterprise mainframe(s), etc., is regularly scanned. Vulnerability scans of subnets are conducted weekly such that the entire network is scanned over a 12 month period. OCIO shall ensure monthly scans for patch status. b. Program Offices/System Owners shall ensure applications under their control are scanned for vulnerabilities, (e.g. code reviews including static, dynamic & web based code), during system development, prior to new releases, or when there are major changes to the application or at least annually during the annual self-assessment if no event driven scans have been performed. c. OCIO uses the National Vulnerability Database (NVD) repository as its vulnerability checklist and stays current with NVD updates as well as vendor advisories and system vulnerability scanning information to ensure that significant vulnerabilities impacting HUD information systems are identified and reported. d. OCIO shall ensure that vulnerabilities with a CVE score of 7.5 or higher are remediated within ninety days or a remediation task is created in the System's POA&M.

3.1.5. E-Authentication Risk Assessment

An E-Authentication risk assessment provides agencies with criteria for determining the level of e-authentication assurance required for specific electronic transactions and systems, based on the risks and their likelihood of occurrence. In other words, it helps you figure out the authentication requirements for each type of transaction. As the consequences of an authentication error become more serious, the required level of assurance increases. E-authentication security requirements must be applied to new and existing information systems that allow online transactions and are connected to the internet or the intranet. The first step in the e-authentication risk assessment is to determine whether the government e-authentication security requirements apply to the system. For those systems to which e-authentication security requirements apply, two additional steps are required:

- Determine the potential impact of authentication errors and the likelihood of their occurrence; and
- Determine the required assurance level for authentication.

The following policy defines the need to conduct the e-authentication risk assessment and the approval requirements.

HUD Policy: HUD-RA-A
HUD Policy: 3.1.5 a. Program Offices/System Owners shall conduct an e-authentication risk assessment (E-RA) of the transactional systems under their control that use the Internet and/or the Intranet. The risk assessment shall be conducted in accordance with OMB guidance under OMB-04-04, E-Authentication Guidance for Federal Agencies and E-Authentication Program Management Office guidance, E-Authentication e-RA Tool Activity Guide, and HUD specific guidance. b. Program Offices/System Owners shall select the technology appropriate for the assurance level that's been identified in the E-RA using NIST SP 800-63, Electronic Authentication Guideline, as amended, and implement and test the controls. c. Program Offices/System Owners shall save the e-authentication risk assessment in HUD's centralized information security management tool, CSAM. d. 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. Security Baseline: Low, Moderate, and High

3.2. Planning

The objective of system security planning is to improve protection of information and information system resources. All HUD systems have some level of sensitivity and require protection as part of good management practice. The protection of a system must be documented in a system security plan.

The following policies define mechanisms in place to address planning for the protection of information assets to include policies, procedures, rules of behavior, privacy impact assessment, and inventory.

FIPS 200 Requirement
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.

3.2.1. Security Planning Policy and Procedures

The following policy addresses the requirements for developing, implementing, and maintaining security planning policies and procedures.

NIST SP 800-53 Control: PL-1
PL-1: The organization: a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]: 1. A security planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the security planning policy and associated security planning controls; and b. Reviews and updates the current: 1. Security planning policy [Assignment: organization-defined frequency]; and 2. Security planning procedures [Assignment: organization-defined frequency]. Security Baseline: Low, Moderate, and High
Implementation
This control is implemented by the *Information Technology Security Policy, Handbook 2400.25 Rev. 4*, that defines HUD's formal security policies and the HUD *Information Technology Security Procedures* that defines HUD's formal security procedures. HUD reviews the policies and procedures minimally every year or when impacted by a significant change or underlying standard. The HUD security policies and procedures are disseminated via the HUD Intranet for all HUD users to access.

3.2.2. System Security Plan

The purpose of the System Security Plan (SSP) is to provide an overview of the security requirements of the system and describe the control(s) in place or planned for meeting those requirements. The plan also delineates responsibilities and expected behaviors of all individuals who access the system. The following policy provides guidance for the development of SSPs. Over time, all information systems change or the environments in which they operate change, resulting in potential new risks to the system. The System Security Plan needs to be reviewed regularly to validate that the security controls are still appropriate and implemented correctly. The following policy provides guidance on updating SSPs.

NIST SP 800-53 Control: PL-2
PL-2: The organization: a. Develops a Security Plan for the information system that: 1. Is consistent with the organization's enterprise architecture; 2. Explicitly defines the authorization boundary for the system; 3. Describes the operational context of the information system in terms of missions and business processes; 4. Provides the security categorization of the information system including supporting rationale; 5. Describes the operational environment for the information system and relationships with or connections to other information systems; 6. Provides an overview of the security requirements for the system; 7. Identifies any relevant overlays, if applicable; 8. Describes the security controls in place or planned for meeting those requirements including a rationale for the tailoring decisions; and 9. Is reviewed and approved by the authorizing official or designated representative prior to plan implementation; b. Distributes copies of the security plan and communicates subsequent changes to the plan to [Assignment: organization-defined personnel or roles]; c. Reviews the security plan for the information system [Assignment: organization-defined frequency]; d. Updates the plan to address changes to the information system/environment of operation or problems identified during plan implementation or security control assessments; and e. Protects the security plan from unauthorized disclosure and modification. Security Baseline: Low, Moderate, and High
E-3: The organization plans and coordinates security-related activities affecting the information system with the ISSO before conducting such activities in order to reduce the impact on other organizational entities. Security Baseline: Moderate and High
HUD Policy: 3.2.2 a. Program Offices/System Owners shall prepare and maintain an active and effective Security Plan for each applicable HUD information system under their purview. The Security Plan is required as part of the system development methodology and must comply with NIST SP 800-18, as amended. b. The Security Plan shall be maintained to satisfy current federal standards. c. The Security Plan shall be reviewed at least annually, and updated, as necessary. This review can be accomplished as part of the annual security assessment. d. The Security Plan must be made available within CSAM for the Authorizing Official to access.

3.2.3. Rules of Behavior

Rules of behavior clearly delineate responsibilities and expected behavior of all individuals with access to a system. The rules state the consequences of inconsistent behavior or non-compliance. The rules of behavior are made available to every user prior to receiving authorization for access to the system.

The following policy addresses the requirement to establish rules of behavior for HUD information systems.

NIST SP 800-53 Control: PL-4
PL-4: The organization: a. Establishes and makes readily available to individuals requiring access to the information system, the rules that describe their responsibilities and expected behavior with regard to information and information system usage; and b. Receives signed acknowledgment from Users indicating that they have read, understand, and agree to abide by the Rules of Behavior, before authorizing access to information and the information system; c. Reviews and updates the rules of behavior [Assignment: organization-defined frequency]; and d. Requires individuals who have signed a previous version of the Rules of Behavior to read and resign when the Rules of Behavior are revised/updated. Security Baseline: Low, Moderate, and High
E-1: The organization includes, in the Rules of Behavior, explicit restrictions on the use of social media/networking sites and the posting of organizational information on public websites. Security Baseline: Moderate and High
HUD Policy: 3.2.3 a. The OCIO shall define and maintain enterprise Rules of Behavior that can be used for all information systems. The Rules of Behavior must identify how personally identifiable information (PII) is protected. The Rules of Behavior will be reviewed and updated as necessary. b. Program Offices/System Owners shall define and maintain additional Rules of Behavior for all information systems under their purview if the generic Rules of Behavior are not sufficient for their system. c. ISSOs shall ensure that users of systems sign the Rules of Behavior and are given training regarding the Rules of Behavior and the disciplinary actions that may result if the rules are violated.

3.2.4. Information Security Architecture

HUD has an obligation to strategically allocate security safeguards (procedural, technical, or both) in the security architecture so that adversaries have to overcome multiple safeguards to achieve their objective.

NIST SP 800-53 Control: PL-8
PL-8: The organization: a. Develops an Information Security Architecture for the information system that: 1. Describes the overall philosophy, requirements, and approach to be taken with regard to protecting the confidentiality, integrity, and availability of organizational information; 2. Describes how the information security architecture is integrated into and supports the Enterprise Architecture; and 3. Describes any information security assumptions about, and dependencies on, external services; b. Reviews and updates the Information Security architecture annually to reflect updates in the Enterprise Architecture; and c. Ensures that the planned Information Security Architecture changes are reflected in the Security Plan, the Security Concept of Operations (CONOPS), and organizational procurements/acquisitions. Security Baseline: Moderate and High

NIST SP 800-53 Control: PL-8
HUD Policy: 3.2.4 a. The ISSO must review the Information Security architecture of the information system under their purview on an annual basis to ensure that the PL-8 (Information Security Architecture) security control is implemented. Security Baseline: Moderate and High

3.2.5. Information Systems Security Officer

An Information Systems Security Officer (ISSO) is the program office's principal point of contact for information security.

The following policy addresses the requirement for the designation of an ISSO and alternate for every HUD information system.

HUD Policy: HUD-PL-B
HUD Policy: 3.2.5 a. Program Offices shall designate an ISSO and an alternate ISSO for every HUD information system under their purview. Security Baseline: Low, Moderate, and High

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.

FIPS 200 Requirement
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.

3.3.1. System and Services Acquisition Policy and Procedures

The following policy addresses the requirement for developing, implementing, and maintaining policy and procedures for incorporating security considerations into HUD systems and services acquisitions.

NIST SP 800-53 Control: SA-1
SA-1: The organization: a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]: 1. A system and services acquisition policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the system and services acquisition policy and associated system and services acquisition controls; and b. Reviews and updates the current: 1. System and services acquisition policy [Assignment: organization-defined frequency]; and 2. System and services acquisition procedures [Assignment: organization-defined frequency]. Security Baseline: Low, Moderate, and High
Implementation
This control is implemented by the *Information Technology Security Policy, Handbook 2400.25 Rev. 4,* which defines HUD's formal security policies and the HUD *Information Technology Security Procedures* that defines HUD's formal security procedures. HUD reviews the policies and procedures minimally every year or when impacted by a significant change or underlying standard. The HUD security policies and procedures are disseminated via the HUD Intranet for all HUD's users to access.

3.3.2. Allocation of Resources

The following policy provides guidance for incorporating security resource requirements into the capital planning process.

NIST SP 800-53 Control: SA-2
SA-2: The organization: a. Determines information security requirements for the information system or information system service in mission/business process planning; b. Determines, documents, and allocates the resources required to protect the information system or information system service as part of its capital planning and investment control process; and c. Establishes a discrete line item for information security in organizational programming and budgeting documentation. Security Baseline: Low, Moderate and High
HUD Policy: 3.3.2 a. Program Officials shall include information security requirements in their capital planning and investment business cases in accordance with HUD CPIC Guidance and NIST SP 800-65 Rev 1, Integrating IT Security into the Capital Planning and Investment Control Process. b. Program Officials shall ensure that information security requirements are adequately funded and documented in accordance with current OMB budgetary guidance, HUD CPIC Guidance, and NIST SP 800-65, *Integrating IT Security into the Capital Planning and Investment Control Process*. c. The CIO shall certify in writing that adequate security funding is included for all IT infrastructure projects, as appropriate, for the projects' System Development Life Cycle (SDLC) and phase. d. The CIO shall not approve any capital investment in which the information security requirements are not adequately defined and funded.

3.3.3. System Development Life Cycle

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

In accordance with the provisions of FISMA, agencies are required to have an agency-wide Information Security Program and that Program must be effectively integrated into the SDLC. HUD's system development life cycle is documented in HUD's Project Planning and Management Life Cycle v2.0.

NIST SP 800-53 Control: SA-3
SA-3: The organization: a. Manages the information system using [Assignment: organization-defined system development life cycle] that incorporates information security considerations; b. Defines and documents information security roles and responsibilities throughout the system development life cycle; c. Identifies individuals having information security roles and responsibilities; and d. Integrates the organizational information security risk management process into system development life cycle activities. Security Baseline: Low, Moderate, and High
HUD Policy: 3.3.3 a. Program Offices/System Owners shall ensure that security is integrated into the SDLC from system inception to system disposal through adequate and effective management, personnel, operations, and technical control mechanisms in accordance with HUD's Project Planning and Management Life Cycle v2.0 and NIST SP 800-64, Security Considerations in the Information System Development Life Cycle. b. The CIO defines and documents information system security roles and responsibilities throughout the system development life cycle as stated in the HUD *Cyber Security Awareness and Training Program* document; and c. Identifies individuals having information system security roles and responsibilities, as stated in the HUD *Cyber Security Awareness and Training Program* document.

3.3.4. Acquisition Process

The following policy provides guidance to ensure that security is properly and adequately addressed as part of system acquisition and other contracting activities.

NIST SP 800-53 Control: SA-4
SA-4: The organization includes the following requirements, descriptions, and criteria, explicitly or by reference, in the acquisition contract for the information system, system component, or information system service in accordance with applicable federal laws, Executive Orders, Directives, policies, regulations, standards, guidelines, and organizational mission/business needs: a. Security functional requirements; b. Security strength requirements; c. Security assurance requirements; d. Security-related documentation requirements; e. Requirements for protecting security-related documentation; f. Description of the information system development environment and environment in which the system is intended to operate; and g. Acceptance criteria. Security Baseline: Low, Moderate, and High
E-1: The organization requires the developer of the information system, system component, or information system service to provide a description of the functional properties of the security controls to be employed. Security Baseline: Moderate and High
E-2: The organization requires the developer of the information system, system component, or information system service to provide design and implementation information for the security controls to be employed that includes: [Selection (one or more): security-relevant external system interfaces; high-level design; low-level design; source code or hardware schematics; [Assignment: organization-defined design/implementation information]] at [Assignment: organization-defined level of detail]. Security Baseline: Moderate and High
E-9: The organization requires the developer of the information system, system component, or information system service to identify early in the system development life cycle, the functions, ports, protocols, and services intended for organizational use. Security Baseline: Moderate and High
E-10: The organization employs only information technology products on the FIPS 201 *approved products list* for Personal Identity Verification (PIV) capability implemented within organizational information systems. Security Baseline: Low, Moderate, and High

NIST SP 800-53 Control: SA-4
HUD Policy: 3.3.4 a. The Office of the Chief Procurement Officer (OCPO) shall ensure that all applicable solicitation documents (including work descriptions) and contracts identify and document the specific security requirements for information systems, services and operations that are required of the contractor. b. Solicitation documents for moderate- and high-impact systems shall include requirements stating 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. c. The security requirements shall include how sensitive information is to be handled and protected at the contractor's site. The requirements shall apply to any information stored, processed, or transmitted using the contractor's computer systems, as well as background investigations, clearances, and/or required facility security. d. Contracts shall require that at the end of the contract, the contractor must return all information and IT resources HUD provided to the contractor, or which the contractor obtained on HUD's behalf during the life of the contract; purge all HUD information from any contractor-owned system used to process or store it; and certify that all HUD information has been purged from such systems. e. The OCPO shall ensure that all applicable solicitation documents and contracts contain a statement requiring contractors to adhere to HUD's information security policies. f. Program Offices/System Owners ensure that for each information system under their purview, all information system components are explicitly identified and reflected in the Security Plan and the system's Inventory of Automated Systems (IAS) record.

3.3.5. Information System Documentation

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

NIST SP 800-53 Control: SA-5
SA-5: The organization: a. Obtains administrator documentation for the information system, system component, or information system service that describes: 1. Secure configuration, installation, and operation of the system, component, or service; 2. Effective use and maintenance of security functions/mechanisms; and 3. Known vulnerabilities regarding configuration and use of administrative (i.e., privileged) functions; b. Obtains user documentation for the information system, system component, or information system service that describes: 1. User-accessible security functions/mechanisms and how to effectively use those security functions/mechanisms; 2. Methods for user interaction, which enables individuals to use the system, component, or service in a more secure manner; and 3. User responsibilities in maintaining the security of the system, component, or service; c. Documents attempt to obtain information system, system component, or information system service documentation when such documentation is either unavailable or nonexistent and [Assignment: organization-defined actions] in response; d. Protects documentation as required, in accordance with the risk management strategy; and e. Distributes documentation to [Assignment: organization-defined personnel or roles]. Security Baseline: Low, Moderate, and High

NIST SP 800-53 Control: SA-5
HUD Policy: 3.3.5 a. Program Offices/System Owners shall ensure that adequate documentation for the information system is available, current, protected when required, in compliance with NIST guidance and distributed to authorized personnel. Documentation includes, but is not limited to: • Security Assessment, Authorization to Operate, and SDLC documentation; • Vendor-supplied documentation of purchased software and hardware; • Network diagrams; • Application documentation for in-house applications; • System build and configuration documentation, which includes optimization of system security settings, when applicable; • User manuals; • Standard Operating Procedures; and • Baseline Configuration standards and guidance. b. For moderate- or high-impact systems, the documentation, if available from the vendor/manufacturer, shall describe: • Functional properties of the security controls employed within the information system with sufficient detail to permit analysis and testing of the controls; and • High-level design of the information system in terms of subsystems and implementation details of the security controls employed within the system with sufficient detail to permit analysis and testing. c. For high-impact systems, vendor/manufacturer documentation is made available to authorized personnel that describe the security-relevant external interfaces to the information system with sufficient detail to permit analysis and testing.

3.3.6. Security Engineering Principles

The effectiveness of protective mechanisms in HUD systems depends on having these mechanisms incorporated into the system during the development process. The following policy provides guidance to ensure that sound security engineering principles are applied to the development of HUD information systems.

NIST SP 800-53 Control: SA-8
SA-8: The organization applies information system security engineering principles in the specification, design, development, implementation, and modification of the information system. Security Baseline: Moderate and High
HUD Policy: 3.3.6 a. Program Offices/System Owners shall ensure information systems that have been rated moderate or high are designed and implemented using security engineering principles in accordance with NIST SP 800-27, *Engineering Principles for Information Technology Security (A Baseline for Achieving Security)*, as amended. b. Program Offices/System Owners shall ensure information systems are designed and implemented consistent with HUD's Enterprise Architecture (EA) including the Enterprise Security and Network Security Architectures, and the EA Reference Models.

3.3.7. External Information System Services

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

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

The following policy addresses the requirement for service providers to use adequate security controls and monitor security control compliance.

NIST SP 800-53 Control: SA-9
SA-9: The organization: a. Requires that providers of external information system services comply with organizational information security requirements and employ [Assignment: organization-defined security controls] in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance; b. Defines and documents government oversight and user roles and responsibilities with regard to external information system services; and c. Employs [Assignment: organization-defined processes, methods, and techniques] to monitor security control compliance by external service providers on an ongoing basis. Security Baseline: Low, Moderate, and High
E-2: The organization requires providers of [Assignment: organization-defined external information system services] to identify the functions, ports, protocols, and other services required for the use of such services. Security Baseline: Moderate and High
HUD Policy: 3.3.7 a. All security policies set forth in this document apply to external information systems operated on behalf of the Department by contractors, vendors, and agents of HUD. b. Program Offices/System Owners shall ensure that external information systems operated on behalf of the Department comply with federal information security standards. c. HUD Contract Officer Representatives (CORs) shall review contracts for external information systems (e.g., commercial telecommunications services, network services, manned security services, or application services) to validate that adequate security requirements have been included. d. Program Offices/System Owners shall determine that an acceptable chain of trust has been established with external service providers. A chain of trust requires that HUD establish and retain a level of confidence that each participating service provider deliver adequate protection. Where a sufficient level of trust cannot be established in the external services and/or service providers, the Program Office/System Owners shall establish compensating security controls or document the acceptance of a greater degree of risk. e. Providers of external information systems shall not prohibit qualified government security representatives (e.g., CISO, ISSO, Inspector General, Physical/Facilities Security or other designated HUD Program Office personnel) from conducting independent site surveys at non-HUD facilities as a part of the Department's regular oversight capability.

3.3.8. Developer Configuration Management

The following policy addresses the requirement for developers of HUD information systems to implement a configuration management plan to ensure that changes to the system are tracked during the development process.

NIST SP 800-53 Control: SA-10
SA-10: The organization requires the developer of the information system, system component, or information system service to: a. Perform configuration management during system, component, or service [Selection (one or more): design; development; implementation; operation]; b. Document, manage, and control the integrity of changes to [Assignment: organization-defined configuration items under configuration management]; c. Implement only organization-approved changes to the system, component, or service; d. Document approved changes to the system, component, or service and the potential security impacts of such changes; and e. Track security flaws and flaw resolution within the system, component, or service and report findings to [Assignment: organization-defined personnel]. Security Baseline: Moderate and High
HUD Policy: 3.3.8 a. Program Offices/System Owners of moderate and high-impact systems under development shall require that the system developer create and implement a Configuration Management Plan (CMP) that controls changes to the system during development, tracks security flaws, requires authorization of changes, and provides documentation of the plan and its implementation.

3.3.9. Developer Security Testing and Evaluation

The following policy addresses the requirement for developers of HUD information systems to create security test plans.

NIST SP 800-53 Control: SA-11
SA-11: The organization requires the developer of the information system, system component, or information system service to: a. Create and implement a Security Assessment Plan; b. Perform [Selection (one or more): unit; integration; system; regression] testing/evaluation at [Assignment: organization-defined depth and coverage]; c. Produce evidence of the execution of the Security Assessment Plan and the results of the security testing/evaluation; d. Implement a verifiable flaw remediation process; and e. Correct flaws identified during security testing/evaluation. Security Baseline: Moderate and High
HUD Policy: 3.3.9 a. Program Offices/System Owners of moderate- or high-impact systems under development shall require that the system developer create a Security Test and Evaluation (ST&E) Plan, implement the plan, and document the results. Developmental security test results may also be used in support of the system's authorization to operate for the delivered information system. Developmental security test results are used to the greatest extent feasible after verification of the results and recognizing that these results are impacted whenever there have been security relevant modifications to the information system subsequent to developer testing.

3.3.10. Supply Chain Protection

HUD maintains a comprehensive defense strategy to protect the organization's information systems against supply chain threats. The following is a list of standard practices HUD has in place to protect information systems and technology products that compose those systems throughout the system development life cycle against supply chain threats.

NIST SP 800-53 Control: SA-12
SA-12 The organization protects against supply chain threats to the information system, system component, or information system service by employing [Assignment: organization-defined security safeguards] as part of a comprehensive, defense-in-breadth information security strategy. Security Baseline: High
HUD Policy: 3.3.10 HUD protects against supply chain threats by employing and implementing the following measures as part of a comprehensive, defense-in-breadth information security strategy: a. HUD relies on USCERT to identify threats targeted at US Government information technology assets; and b. Program Offices/System Owners manage threats of all levels at each phase of the system development life cycle by employing standards and baselines, continuous monitoring and testing of systems and audits all systems routinely to reinforce strategies to mitigate risk. Information systems categorized as "High" must use the acquisition/procurement processes to require supply chain entities to implement necessary security safeguards to: (i) reduce the likelihood of unauthorized modifications at each stage in the supply chain; and (ii) protect information systems and information system components, prior to taking delivery of such systems/components. Security Baseline: High

3.3.11. Development Process, Standards, and Tools

HUD information system categorized as 'High' must maintain the integrity of changes to development tools (i.e., programming languages and computer-aided design [CAD] systems) and processes to enable accurate supply chain risk assessment and mitigation. Also, must maintain a robust configuration control throughout the life cycle (including design, development, transport, delivery, integration, and maintenance) to track authorized changes and prevent unauthorized changes.

NIST SP 800-53 Control: SA-15
SA-15 The organization: a. Requires the developer of the information system, system component, or information system service to follow a documented development process that: 1. Explicitly addresses security requirements; 2. Identifies the standards and tools used in the development process; 3. Documents the specific tool options and tool configurations used in the development process; and 4. Documents, manages, and ensures the integrity of changes to the process and/or tools used in development; and b. Reviews the development process, standards, tools, and tool options/configurations on an annual basis to determine if the process, standards, tools, and tool options/configurations selected and employed can satisfy HUD's information system security requirements. Security Baseline: High

NIST SP 800-53 Control: SA-15
HUD Policy: 3.3.11 The system owner and/or ISSO must ensure that developers for their respective information system categorized as "High" document a process that: a. Explicitly addresses security requirements; b. Identifies the standards and tools used in the development process; c. Documents the specific tool options and tool configurations used in the development process; and d. Documents, manages, and ensures the integrity of changes to the process and/or tools used in development. Furthermore, the system owner must review the development process, standards, tools, and tool options/configurations on an annual basis to determine if the process, standards, tools, and tool options/configurations selected and employed can satisfy HUD's information system security requirements. Security Baseline: High

3.3.12. Developer-Provided Training

Training of external and internal (in-house) developers is an essential element to ensure the effectiveness of security controls implemented within HUD's information systems.

NIST SP 800-53 Control: SA-16
SA-16 The organization requires the developer of the information system, system component, or information system service to provide annual training to the Information System ISSO on the correct use and operation of the implemented security functions, controls, and/or mechanisms. Security Baseline: High
HUD Policy: 3.3.12 a. The developer of the information system, system component, or information system service is to provide annual training to the information system ISSO and system owner on the correct use and operation of the implemented security functions, controls, and/or mechanisms. Security Baseline: High

3.3.13. Developer-Security Architecture and Design

HUD employs this security control to help ensure that developers for HUD develop information security architecture and such security architecture is integrated or tightly coupled to the HUD enterprise architecture.

NIST SP 800-53 Control: SA-17
SA-17 The organization requires the developer of the information system, system component, or information system service to produce a design specification and security architecture that: a. Is consistent with and supportive of the organization's security architecture which is established within, and is an integrated part of the organization's enterprise architecture; b. Accurately and completely describes the required security functionality, and the allocation of security controls among physical and logical components; and c. Expresses how individual security functions, mechanisms, and services work together to provide required security capabilities and a unified approach to protection. Security Baseline: High

NIST SP 800-53 Control: SA-17
HUD Policy: 3.3.13 The System Owner/ISSO must ensure that developers for their respective system produce a design specification and security architecture that: a. Is consistent with and supportive of the HUD's security architecture which is established within, and is an integrated part of the HUD's enterprise architecture; b. Accurately and completely describes the required security functionality, and the allocation of security controls among physical and logical components; and c. Expresses how individual security functions, mechanisms, and services work together to provide required security capabilities and a unified approach to protection. Security Baseline: High

3.4. Security Assessment and Authorization

Security Control Assessment is the final testing and/or evaluation of the management, operational, and technical security controls in an 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. By authorizing operation of an information system, the Authorizing Official assumes responsibility for the security of the system and explicitly accepts the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation based on the implementation of an agreed-upon set of security controls.

The following policies 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. Security Assessment and Authorization Policy and Procedures

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

The following policy addresses the requirement to develop policy and procedures for certification, accreditation and security assessments.

NIST SP 800-53 Control: CA-1
CA-1: The organization: a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]: 1. A security assessment and authorization policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the security assessment and authorization policy and associated security assessment and authorization controls. b. Reviews and updates the current: 1. Security assessment and authorization policy [Assignment: organization-defined frequency]; and 2. Security assessment and authorization procedures [Assignment: organization-defined frequency]. Security Baseline: Low, Moderate and High
Implementation
This control is implemented by the *Information Technology Security Policy, Handbook 2400.25 Rev. 4,* that defines HUD's formal security policies and the HUD *Information Technology Security Procedures* that defines HUD's formal security procedures. HUD reviews the policies and procedures minimally every year or when impacted by a significant change or underlying standard. The HUD security policies and procedures are disseminated via the HUD Intranet for all HUD's users to access.

3.4.2. Security Assessments

The results of the security assessment are used to re-evaluate the risks and update the system security plan, providing the factual basis for a security assessment decision. The following policy provides guidance to ensure that an assessment is conducted.

NIST SP 800-53 Control: CA-2
CA-2: The organization: The organization: a. Develops a Security Assessment Plan that describes the scope of the assessment including: 1. Security controls and control enhancements under assessment; 2. Assessment procedures to be used to determine security control effectiveness; and 3. Assessment environment, assessment team, and assessment roles and responsibilities; b. Assesses the security controls in the information system and its environment of operation [Assignment: organization-defined frequency] to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting established security requirements; c. Produces a Security Assessment Report that documents the results of the assessment; and d. Provides the results of the security control assessment to [Assignment: organization-defined individuals or roles]. Security Baseline: Low, Moderate, and High
E-1: The organization employs assessors or assessment teams with [Assignment: organization-defined level of independence] to conduct security control assessments. Security Baseline: Moderate and High

NIST SP 800-53 Control: CA-2
E-2: The organization includes as part of security control assessments, [Assignment: organization-defined frequency], [Selection: announced; unannounced], [Selection (one or more): in-depth monitoring; vulnerability scanning; malicious user testing; insider threat assessment; performance/load testing; [Assignment: organization-defined other forms of security assessment]]. Security Baseline: High
HUD Policy: 3.4.2 a. Program Offices/System Owners shall conduct a security assessment for all systems under their purview every three years in accordance with NIST SP 800-53, *Recommended Security Controls for Federal Information Systems, as amended,* and NIST SP 800-53A, *Guide for Assessing the Security Controls in Federal Information Systems,* as amended. b. Program Offices/System Owners shall follow the guidelines contained in NIST SP 800-37, *Guide for Applying the Risk Management Framework to Federal Information Systems*, as amended, and the HUD authorization to operate methodology, in assessing their information systems. c. Program Offices/ System Owners shall ensure that the security assessment of moderate- and high-impact systems is conducted independently. d. Program Offices/System Owners shall ensure that whenever changes are made to information systems, networks, or to their physical environment, interfaces, or user-community makeup, the impact on the security of the information processed is reviewed via a documented security impact analysis as required by NIST SP 800-37, *Guide for Applying the Risk Management Framework to Federal Information Systems*, as amended.

3.4.3. System Connections

To protect HUD information assets, systems that are connected to or share data with the HUD systems must have an agreement that describes the rules governing the interconnection. The following policy provides guidance to ensure that formal agreements governing connections are instituted.

NIST SP 800-53 Control: CA-3
CA-3: The organization: a. Authorizes connections from the information system to other information systems through the use of Interconnection Security Agreements; b. Documents, for each interconnection, the interface characteristics, security requirements, and the nature of the information communicated; and c. Reviews and updates Interconnection Security Agreements [Assignment: organization-defined frequency]. Security Baseline: Low, Moderate, and High
E-5: The organization employs [Selection: allow-all, deny-by-exception; deny-all, permit-by-exception] policy for allowing [Assignment: organization-defined information systems] to connect to external information systems. Security Baseline: Moderate and High
HUD Policy: 3.4.3 a. Program Offices/System Owners shall authorize, document, and monitor all (internal and external) interconnections outside of the system's accreditation boundary. Information systems that require an external connection (interconnection outside of the agency's infrastructure) shall be documented in a Memorandum of Agreement/Understanding (MOA/U) and Interconnection Security Agreement (ISA) in accordance with NIST SP 800-47, *Security Guide for Interconnecting Information Technology Systems*.

3.4.4. Plan of Action and Milestones

The Plan of Action and Milestones (POA&Ms) provides a listing of identified weaknesses in an information system as determined by the security assessments and testing during the process. It also includes a plan and timeframe for addressing each weakness. The following policy provides guidance for developing and updating a POA&M.

NIST SP 800-53 Control: CA-5
CA-5: The organization: a. Develops a Plan of Action and Milestones for the information system to document the organization's planned remedial actions to correct weaknesses or deficiencies noted during the assessment of the security controls and to reduce or eliminate known vulnerabilities in the system; and b. Updates existing Plan of Action and Milestones [*Assignment: organization-defined frequency*] based on the findings from security controls assessments, security impact analyses, and continuous monitoring activities. Security Baseline: Low, Moderate, and High
HUD Policy: 3.4.4 a. Program Offices/System Owners shall develop POA&Ms to correct weaknesses identified during any evaluation or assessment of security controls within 90 days of the identification of the weaknesses. b. Program Offices/System Owners shall capture all POA&Ms in the HUD's central security management repository, CSAM. c. Program Offices shall update their POA&Ms quarterly, at a minimum for systems under their purview.

3.4.5. Security Authorization

Security Authorization is the risk-based decision that determines whether a HUD information system should be allowed to operate under a particular security configuration. The following policy provides guidance for authorizing HUD information systems to operate.

NIST SP 800-53 Control: CA-6
CA-6: The organization: a. Assigns a senior-level executive or manager to the role of authorizing official for the information system; b. Ensures that the authorizing official authorizes the information system for processing before commencing operations; and c. Updates the security authorization [*Assignment: organization-defined frequency*]. Security Baseline: Low, Moderate, and High
HUD Policy: 3.4.5 a. The Deputy Secretary appoints senior management officials within the program and administrative offices to be Authorizing Officials. b. Program Offices/System Owners shall ensure that systems are assessed at their initial operating capability, every three years thereafter, and whenever a significant change occurs in accordance with NIST 800-37Rev1. c. Program Offices/System Owners shall review results obtained during the continuous monitoring process to evaluate the security posture of the information system and make modifications as necessary to ensure the system remains adequately secured. d. Existing assessments completed before the issuance of this policy shall remain in effect if the assessment complied fully with the policy in effect at the time of assessment, no significant deficiencies have been identified, and the system configuration has not changed since the assessment.

3.4.6. Continuous Monitoring

By regularly reviewing the effectiveness of security controls within HUD information systems, Program Offices and System Owners will be able to quickly detect and respond to new vulnerabilities. The following policy provides guidance to ensure that continuous monitoring of the security controls occurs.

NIST SP 800-53 Control: CA-7
CA-7: The organization develops a continuous monitoring strategy and implements a continuous monitoring program that includes: a. Establishment of [*Assignment: organization-defined metrics*] to be monitored; b. Establishment of [*Assignment: organization-defined freq*uencies] for monitoring and [*Assignment: organization-defined freq*uencies] for assessments supporting such monitoring; c. Ongoing security control assessments in accordance with the organizational continuous monitoring strategy; d. Ongoing security status monitoring of organization-defined metrics in accordance with the organizational continuous monitoring strategy; e. Correlation and analysis of security-related information generated by assessments and monitoring; f. Response actions to address results of the analysis of security-related information; and g. Reporting the security status of organization and the information system to [*Assignment: organization-defined personnel or roles*] [*Assignment: organization-defined frequency*]. Security Baseline: Low, Moderate, and High
E-1: The organization employs assessors or assessment teams with [Assignment: organization-defined level of independence] to monitor the security controls in the information system on an ongoing basis. Security Baseline: Moderate and High
HUD Policy: 3.4.6 a. The OCIO shall develop and establish a department-level continuous monitoring strategy for all information systems. The plan should include the configuration management process, determination of the security impact of changes to the information system, and ongoing security control assessments. b. Program Offices/System Owners shall implement the OCIO's continuous monitoring strategy to their information systems.

3.4.7. Penetration Testing

Penetration testing is a specialized type of assessment conducted on information systems or individual system components to identify vulnerabilities. The following penetration testing policy is for HUD information systems categorized as 'High' to ensure that identified vulnerabilities are not exploited by adversaries.

NIST SP 800-53 Control: CA-8
CA-8: The organization conducts penetration testing [Assignment: organization-defined frequency] on [Assignment: organization-defined information systems or system components]. Security Baseline: High
HUD Policy: 3.4.7 The ISSO must ensure that their respective system meet the CA-8 *Penetration Testing* security control requirement. Security Baseline: High

3.4.8. Internal System Connections

The following security control applies to connections between HUD information systems and (separate) constituent system components (i.e., intra-system connections) including, for example, system connections with mobile devices, notebook/desktop computers, printers, copiers, facsimile machines, scanners, sensors, and servers. Instead of authorizing each individual internal connection, organizations can authorize internal connections for a class of components with common characteristics and/or configurations, for example, all digital printers, scanners, and copiers with a specified processing, storage, and transmission capability or all smart phones with a specific baseline configuration.

NIST SP 800-53 Control: CA-9
CA-9: The organization: a. Authorizes internal connections of [Assignment: organization-defined information system components or classes of components] to the information system; and b. Documents, for each internal connection, the interface characteristics, security requirements, and the nature of the information communicated. Security Baseline: High
HUD Policy: 3.4.8 The ISSO must ensure that respective information system(s) under their purview meet the CA-9 *Internal System Connections* security control requirement. Security Baseline: High

4.0 OPERATIONAL POLICIES

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).

4.1. Personnel Security

The Housing and Urban Development (HUD) information systems face threats from many sources, including the actions of people (e.g., 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 policies 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 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 *(see FIPS PUB 200, Federal Information Processing Standards Publication).*

4.1.1. Personnel Security Policy and Procedures

The Personnel Security Policy and Procedures must be consistent with HUD personnel policies, applicable laws, Executive Orders, Directives, policies, regulations, standards, and guidance. Where applicable, the Personnel Security Policy and Procedures will refer to the references by the associated reference description or number, so that these policies are not repeating the reference. This may prevent the need to change the personnel security policy whenever modifications are made to the external references.

NIST SP 800-53 Control: PS-1
PS-1. The organization: a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]: 1. A personnel security policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the personnel security policy and associated personnel security controls. b. Reviews and updates the current: 1. Personnel security policy *[Assignment: organization-defined frequency]; and* 2. Personnel security procedures *[Assignment: organization-defined frequency]*. Security Baseline: Low, Moderate, and High

NIST SP 800-53 Control: PS-1
Implementation
This control is implemented by the *Information Technology Security Policy, Handbook 2400.25 Rev. 4,* that defines HUD's formal security policies and the HUD *Information Technology Security Procedures* that defines HUD's formal security procedures. HUD reviews the policies and procedures minimally every year or when impacted by a significant change or underlying standard. The HUD security policies and procedures are disseminated via the HUD Intranet for all HUD's users to access.

4.1.2. Position Risk Designation

Position risk categorizations or designations must be assigned to all positions within an organization that have access to information technology resources and must be consistent with 5CFR 731 and Office of Personnel Management (OPM) policy and guidance. These designations will be used to determine the level of investigation required for access to systems.

NIST SP 800-53 Control: PS-2
PS-2: The organization: a. Assigns a risk designation to all organizational positions; b. Establishes screening criteria for individuals filling those positions; and c. Reviews and updates position risk designations [Assignment: organization-defined frequency]. Security Baseline: Low, Moderate, and High
HUD Policy: 4.1.2 a. Program Offices/Human Resources Staff/System Owners shall designate the position sensitivity level for all government positions that use, develop, operate, or maintain information systems under their purview and shall determine risk levels for each position in accordance with the Office of Personnel Management (OPM) policy and guidance. Position sensitivity levels and risk levels shall be reviewed annually in accordance with OPM guidance.

4.1.3. Personnel Screening

To ensure the protection of information systems, it is essential that users are screened prior to gaining access to the information assets. Many security incidents are related to individuals within an organization.

NIST SP 800-53 Control: PS-3
PS-3: The organization: a. Screens individuals prior to authorizing access to the information system; and b. Rescreens individuals according to the Personnel Security/Suitability Handbook 732.3 Rev2. Security Baseline: Low, Moderate, and High

NIST SP 800-53 Control: PS-3
HUD Policy: 4.1.3 Personnel Security and System Owners shall: a. Screen individuals prior to receiving access to information systems. Ensure that no Federal employee or contractor employee has access to systems unless they have completed the required personnel security forms and submitted them through the System Security Administrator. The Investigation shall be consistent with: (i) OPM policy, regulations, and guidance; (ii) organizational policy, regulations, and guidance as identified by Personnel Security. b. Ensure that all Federal employees or contractor employees be re-screened every 5 years.

4.1.4. Personnel Termination

Critical to the protection of information assets is ensuring that all applicable access is terminated when an individual is terminated (whether voluntarily or involuntarily) to prevent misuse of privileges granted to an individual. The following policy provides guidance for an employee and contractor who terminate their employment with HUD.

NIST SP 800-53 Control: PS-4
PS-4 The organization, upon termination of individual employment; a. Disables information system access within [Assignment: organization-defined time period]; b. Terminates/revokes any authenticators/credentials associated with the individual; c. Conducts exit interviews that include a discussion of [Assignment: organization-defined information security topics]; d. Retrieves all security-related organizational information system-related property; e. Retains access to organizational information and information systems formerly controlled by the terminated individual; and f. Notifies [Assignment: organization-defined personnel or roles] within [Assignment: organization-defined time period]. Security Baseline: Low, Moderate, and High
E-2: The organization employs automated mechanisms to notify [Assignment: organization-defined personnel or roles] upon termination of an individual. Security Baseline: High
HUD Policy: 4.1.4 Program Offices/System Owners shall implement procedures to ensure that system accesses are revoked when HUD or contractor employees terminate their employment with HUD or the contractor organization working for HUD. The procedures shall include: a. Exit interviews. b. A process for returning all organizational information and system-related property (e.g., keys, ID cards). c. Access to official records created by the terminated employee/contractor that are stored on organizational information systems be revoked. d. Formal notification within 24 hours to the facilities group or Security Officer/ISSO. e. Completion of the Form HUD-58-A, *Clearance for Separation of Employee* for Headquarters employees and Form HUD-58, *Clearance for Separation of Employee* for Field Office employees.

4.1.5. Personnel Transfer

When personnel transfer within an organization, access to information resources must be reviewed to ensure that personnel access privileges are still applicable to the new role and responsibilities to prevent either accidental or intentional misuse.

NIST SP 800-53 Control: PS-5
PS-5: The organization: a. Reviews and confirms the ongoing operational need for current logical and physical access authorizations to information systems/facilities when individuals are reassigned or transferred to other positions within the organization; b. Initiates [Assignment: organization-defined transfer or reassignment actions] within [Assignment: organization-defined time period following the formal transfer action]; c. Modifies access authorization as needed to correspond with any changes in the operational need due to reassignment or transfer; and d. Notifies [Assignment: organization-defined personnel or roles] within [Assignment: organization-defined time period]. Security Baseline: Low, Moderate, and High
HUD Policy: 4.1.5 Program Offices/System Owners shall: a. Implement procedures to ensure that system access privileges are reviewed and are modified as needed when HUD or contractor employees are reassigned to other duties. b. Ensure any personnel access privilege modifications are completed within 30 days of the reassignment.

4.1.6. Access Agreements

Access agreements are necessary so that individuals and entities understand their responsibility in the protection of information and information assets. The acknowledgment of these responsibilities is achieved by having the individuals review and sign appropriate access agreements associated with the information or information asset. Individuals must acknowledge their understanding on a regular basis.

The following policy addresses the requirement for users to sign agreements prior to accessing HUD information assets.

NIST SP 800-53 Control: PS-6
PS-6: The organization: a. Develops and documents access agreements for organizational information systems; b. Reviews and updates the access agreements [Assignment: organization-defined frequency]; and c. Ensures that individuals requiring access to organizational information and information systems: 1. Sign appropriate access agreements prior to being granted access; and 2. Re-sign access agreements to maintain access to organizational information systems when access agreements have been updated or [Assignment: organization-defined frequency]. Security Baseline: Low, Moderate, and High
HUD Policy: 4.1.6 a. Program Offices/System Owners shall require all individuals that access HUD information and information systems complete appropriate access agreements (e.g., Non-Disclosure Agreements, Acceptable Use

NIST SP 800-53 Control: PS-6
Agreements, Rules of Behavior, Conflict-of-Interest Agreements) prior to gaining access to HUD information and information systems. The access agreements must be updated and resigned every three years or when an individual changes HUD organizations.

4.1.7. Third-Party Personnel Security

Third-party personnel must acknowledge and confirm their understanding and accountability for maintaining the security of the information assets for which they are responsible. The following policy addresses the requirement for establishing and monitoring personnel security requirements for third-party providers.

NIST SP 800-53 Control: PS-7
PS-7: The organization: a. Establishes personnel security requirements including security roles and responsibilities for third-party providers; b. Requires third-party providers to comply with personnel security policies and procedures established by the organization; c. Documents personnel security requirements; d. Requires third-party providers to notify [Assignment: organization-defined personnel or roles] of any personnel transfers or terminations of third-party personnel who possess organizational credentials and/or badges, or who have information system privileges within [Assignment: organization-defined time period]; and e. Monitors provider compliance. Security Baseline: Low, Moderate, and High
HUD Policy: 4.1.7 a. HUD contracting officers shall include personnel security requirements in all solicitation documents and contracts for IT services and systems.

4.1.8. Personnel Sanctions

To assist in the enforcement of security policies and to maintain accountability for individual actions, personnel sanctions must be employed. So that the sanctions are understood and acknowledged, personnel sanctions should be incorporated into all access agreements.

The following policy addresses the implementation of a formal sanctions process in the event personnel fail to comply with agreed-upon information security policies.

NIST SP 800-53 Control: PS-8
PS-8. The organization: a. Employs a formal sanctions process for individuals failing to comply with established information security policies and procedures; and b. Notifies [Assignment: organization-defined personnel or roles] within [Assignment: organization-defined time period] when a formal employee sanctions process is initiated, the individual sanctioned is identified, and the reason for the sanction is determined. Security Baseline: Low, Moderate, and High
HUD Policy: 4.1.8 a. HUD employees may be subject to disciplinary action for failure to comply with HUD security policies,

NIST SP 800-53 Control: PS-8
whether or not the failure results in criminal prosecution. For further information regarding disciplinable offenses see *HUD Handbook 752.2, Adverse Actions or Standards of Ethical Conduct for Employees of the Executive Branch, 5 C.F.R, section 2635.704, "Use of Government Property."* b. HUD contractors and external users who fail to comply with department security policies shall be subject to having their access to HUD information systems and facilities terminated, whether or not the failure results in criminal prosecution. c. Any person who improperly discloses sensitive information shall be subject to criminal and civil penalties and sanctions under a variety of laws (e.g., the Privacy Act).

4.2. Physical and Environmental Protection

Physical security represents the first line of defense against intruders and adversaries attempting to gain access to HUD 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 policies 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

The physical and environmental protection policy and procedures are consistent with all other HUD policies, applicable laws, Executive Orders, Directives, policies, regulations, standards, and guidance. Where applicable, the physical and environmental protection security policy and procedures will refer to the references by the associated reference description or number to avoid repetition of references.

NIST SP 800-53 Control: PE-1
PE-1. The organization: a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]: 1. A physical and environmental protection policy that addresses the purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the physical and environmental protection policy and associated physical and environmental protection controls. b. Reviews and updates the current: 1. Physical and environmental protection policy [Assignment: organization-defined frequency]; and 2. Physical and environmental protection procedures [Assignment: organization-defined frequency]. Security Baseline: Low, Moderate, and High

NIST SP 800-53 Control: PE-1
Implementation
This control is implemented by the *Information Technology Security Policy, Handbook 2400.25 Rev. 4*, that defines HUD's formal security policies and the HUD *Information Technology Security Procedures* that defines HUD's formal security procedures. HUD reviews the policies and procedures minimally every year or when impacted by a significant change or underlying standard. The HUD security policies and procedures are disseminated via the HUD Intranet for all HUD's users to access.

4.2.2. Physical Access Authorizations

Controlling physical access to facilities housing information assets to only authorized individuals requires HUD to follow an authorization process and maintain a list of authorized individuals. This control is one of the controls implemented to protect the physical access to the facility; physical access is one layer of defense in protecting the information assets.

The following policy addresses the requirement for organizations to maintain and monitor access control lists that identify individuals authorized to access facilities housing HUD information assets.

NIST SP 800-53 Control: PE-2
PE-2: The organization: a. Enforces physical access authorizations at [Assignment: organization-defined entry/exit points to the facility where the information system resides] by: 1. Verifying individual access authorizations before granting access to the facility; and 2. Controlling ingress/egress to the facility using [Selection (one or more): [Assignment: organization-defined physical access control systems/devices]; guards]; b. Maintains physical access audit logs for [Assignment: organization-defined entry/exit points]; c. Provides [Assignment: organization-defined security safeguards] to control access to areas within the facility officially designated as publicly accessible; d. Escorts visitors and monitors visitor activity [Assignment: organization-defined circumstances requiring visitor escorts and monitoring]; e. Secures keys, combinations, and other physical access devices; f. Inventories [Assignment: organization-defined physical access devices] every [Assignment: organization-defined frequency]; and g. Changes combinations and keys [Assignment: organization-defined frequency] and/or when keys are lost, combinations are compromised, or individuals are transferred or terminated. Security Baseline: Low, Moderate, and High

NIST SP 800-53 Control: PE-2
HUD Policy: 4.2.2 a. For information systems managed by the Deputy CIO for IOO ensures that the management of infrastructure service provider facilities that house HUD information systems develops and maintains a current list of personnel with authorized access to the facility, issues appropriate authorization credentials, and reviews and approves the access list and authorization credentials at least annually. b. For information systems managed by the Deputy CIO for IOO ensures that the management of infrastructure service provider facilities removes from the access list personnel no longer requiring access. c. For information systems not hosted/managed in an infrastructure service providers facility, the Authorizing Official for the information system ensures that the management of the facility housing the information system develops and maintains a current list of personnel with authorized access to the facility, issues appropriate authorization credentials, and reviews and approves the access list and authorization credentials at least annually. d. For information systems not hosted/managed in an infrastructure service provider's facility, the Authorizing Official for the information system ensures that the management of the facility housing the information system removes from the access list personnel no longer requiring access.

4.2.3. Physical Access Control

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

The Homeland Security Presidential Directive 12 (HSPD-12) mandates a government-wide standard for secure and reliable forms of identification issued by the federal government to its employees and contractors (including contractor employees).

It is important to ensure that physical access to a facility is based on the list of authorized individuals. This control is one of the controls implemented to protect the physical access to the facility; physical access is one layer of defense in protecting the information assets.

The following policy addresses the requirement for the HUD facilities group or Security Officer to maintain control over all physical access point to facilities housing HUD information systems.

NIST SP 800-53 Control: PE-3
PE-3: The organization: a. Enforces physical access authorizations for all physical access points (including designated entry/exit points) to the facility where the information system resides (excluding those areas within the facility officially designated as publicly accessible); b. Verifies individual access authorizations before granting access to the facility; c. Controls entry to the facility containing the information system using physical access devices and/or guards; d. Controls access to areas officially designated as publicly accessible in accordance with the organizations assessment of risk; e. Secures keys, combinations, and other physical access devices; f. Inventories physical access devices [Assignment: organization-defined frequency]; and g. Changes combinations and keys [Assignment: organization-defined frequency] and when keys are lost, combinations are compromised, or individuals are transferred or terminated. Security Baseline: Low, Moderate, and High
E-1: The organization enforces physical access authorizations to the information system in addition to the physical access controls for the facility at [Assignment: organization-defined physical spaces containing one or more components of the information system]. Security Baseline: High
HUD Policy: 4.2.3 a. The Deputy CIO for IOO enforces the physical access authorizations to infrastructure service provider facilities housing HUD systems and limits access to authorized personnel. Controls shall be in place for deterring, detecting, monitoring, restricting, and regulating access to specific areas at all times. b. For information systems not hosted/managed in an infrastructure service provider's facility, the Authorizing Official enforces the access to facilities limiting access to authorized personnel. Controls shall be in place for deterring, detecting, monitoring, restricting, and regulating access to specific areas at all times. c. The Deputy CIO of IOO ensures control of all access points to infrastructure service provider facilities housing HUD systems with physical access devices and/or guards. Keys, combinations, and other access devices shall be secured and inventoried every six months and changed any time the keys are lost, combinations are compromised, or individuals are terminated or transferred. d. For information systems not hosted/managed in an infrastructure service provider's facility, the Authorizing Official controls all access points to facilities with physical access devices and/or guards. Keys, combinations, and other access devices shall be secured and inventoried every six months and changed any time the keys are lost, combinations are compromised, or individuals are terminated or transferred. e. The facilities group or security officer shall ensure that all visitors sign in and out when entering and leaving HUD facilities. f. The Deputy CIO for IOO ensures that infrastructure service provider facilities housing HUD information systems manages and controls physical access by authenticating visitors before authorizing access. g. For information systems not hosted/managed in an infrastructure service provider's facility, the Authorizing Official ensures that physical access is controlled by authenticating visitors before authorizing access. h. Contractors' access shall be limited to those work areas requiring their presence. i. For HUD facilities housing moderate- or high-impact systems, the facilities group or Security Officer shall ensure that all visitors are escorted.

4.2.4. Access Control for Transmission Medium

Protecting system distribution and transmission lines is important to protect the information from being intercepted during transmission. It is necessary to secure access to the transmission lines. The following policy addresses the requirement for organizations to maintain control of access to high-impact system transmission lines.

NIST SP 800-53 Control: PE-4
PE-4: The organization controls physical access to information system distribution and transmission lines within organizational facilities using [*Assignment: organization-defined security safeguards*]. Security Baseline: Moderate and High
HUD Policy: 4.2.4 a. For infrastructure service provider facilities housing HUD systems, the Deputy CIO for IOO shall control physical access to high-impact system's distribution and transmission lines by locking wire cabinets, disconnecting or locking spare jacks, protecting cabling by conduit or cable trays. b. For information systems not hosted in an infrastructure service provider's facility, the Authorizing Official shall control physical access to high-impact system's distribution and transmission lines by locking wire cabinets, disconnecting or locking spare jacks, protecting cabling by conduit or cable trays.

4.2.5. Access Control for Output Devices

Physical access to devices displaying information must be controlled. When sensitive information is displayed, it is important that the information not be visible to those that should not have access. The following policy addresses the requirement for organizations to maintain control of access to devices displaying information on high-impact systems.

NIST SP 800-53 Control: PE-5
PE-5: The organization controls physical access to information system output devices to prevent unauthorized individuals from obtaining the output. Security Baseline: Moderate and High
HUD Policy: 4.2.5 a. For moderate- or high-impact systems, the Program Offices/System Owners shall ensure that physical access to devices displaying information is controlled to prevent unauthorized disclosure.

4.2.6. Monitoring Physical Access

In order to ensure that physical access to facilities is secure, violations and suspicious activities must be responded to accordingly. The following policy addresses the requirement for organizations to monitor physical access to HUD information systems and respond to incidents.

NIST SP 800-53 Control: PE-6
PE-6: The organization: a. Monitors physical access to the facility where the information system resides to detect and respond to physical security incidents; b. Reviews physical access logs [Assignment: organization-defined frequency] and upon occurrence of [Assignment: organization-defined events or potential indications of events]; and c. Coordinates results of reviews and investigations with the organizational incident response capability. Security Baseline: Low, Moderate, and High
E-1: The organization monitors real-time physical intrusion alarms and surveillance equipment. Security Baseline: Moderate and High

NIST SP 800-53 Control: PE-6
E-4: The organization monitors physical access to the information system in addition to the physical access monitoring of the facility as [Assignment: organization-defined physical spaces containing one or more components of the information system]. Security Baseline: High
HUD Policy: 4.2.6 a. The Deputy CIO for IOO ensures that physical access to infrastructure service provider facilities is monitored to detect and respond to incidents. Logs shall be reviewed daily for apparent security violations or suspicious activities and responded to accordingly. For moderate- or high-impact systems, the monitoring shall be in real-time for intrusion alarms and surveillance equipment. For high-impact systems, the monitoring shall use automated mechanisms to recognize intrusions and to take appropriate action. b. For information systems not hosted/managed in an infrastructure service provider's facility, the Authorizing Official for the information system shall ensure that physical access is monitored to detect and respond to incidents. Logs shall be reviewed daily for apparent security violations or suspicious activities and responded to accordingly. For moderate- or high-impact systems, the monitoring shall be in real-time for intrusion alarms and surveillance equipment. For high-impact systems, the monitoring shall use automated mechanisms to recognize intrusions and to take appropriate action. c. For infrastructure service provider's facilities, the facility security officer coordinates results of reviews and investigations with the organization's incident response capability. d. For information systems not managed by the OCIO, the Authorizing Official for the information system coordinates results of reviews and investigations with the organization's incident response capability.

4.2.7. Visitor Access Records

One of the mechanisms to ensure the physical security controls are being employed is to review the visitor access records to the facilities on a regular basis. The following policy addresses the requirement for organizations to maintain visitor access records for facilities where HUD information assets are housed. The following policy addresses the requirement for organizations to maintain and review visitor access records.

NIST SP 800-53 Control: PE-8
PE-8: The organization: a. Maintains visitor access records to the facility where the information system resides for [Assignment: organization-defined time period]; and b. Reviews visitor access records [Assignment: organization-defined frequency]. Security Baseline: Low, Moderate, and High
E-1: The organization employs automated mechanisms to facilitate the maintenance and review of visitor access records. Security Baseline: High
HUD Policy: 4.2.7 a. The Deputy CIO for IOO ensures that infrastructure service provider facilities security Officer shall review visitor records monthly, maintain them on file, and have the access records available for further review for one year. For high-impact systems, the maintenance and review of access records shall use automated mechanisms. b. For information systems not hosted in an infrastructure service provider's facility, the Authorizing Official for the information system develops and maintains a current list of personnel with authorized access to the facility, issues appropriate authorization credentials, and reviews and approves the access list and

NIST SP 800-53 Control: PE-8
authorization credentials at least annually. c. For information systems not managed by the OCIO, the Authorizing Official for the information system ensures that the management of the facility housing the information system removes from the access list personnel no longer requiring access.

4.2.8. Power Equipment and Power Cabling

Power equipment and power cabling require protection from damage and destruction to safeguard the availability of the information assets. The following policy addresses the requirement for organizations to protect power equipment and cabling for HUD information systems.

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
HUD Policy: 4.2.8 a. For moderate- or high-impact systems, the facilities group or Security Officer at facilities housing HUD information systems shall ensure that power equipment and cabling are protected from damage and destruction.

4.3. Emergency Shutoff

The emergency shutoff is important in the protection of the personnel working in facilities and for the facility. The following policy addresses the requirement for organizations to have the capability of shutting off power to HUD information systems in the event of an emergency.

NIST SP 800-53 Control: PE-10
PE-10: The organization: a. Provides the capability of shutting off power to the information system or individual system components in emergency situations; b. Places emergency shutoff switches or devices in [Assignment: organization-defined location by information system or system component] to facilitate safe and easy access for personnel; and c. Protects emergency power shutoff capability from unauthorized activation. Security Baseline: Moderate and High
HUD Policy: 4.3 a. 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 at facilities housing HUD information systems shall provide for the capability of shutting off power to any IT component that may be malfunctioning or threatened without endangering personnel by requiring them to approach the equipment.

4.3.1. Emergency Power

Emergency power provides personnel with the ability to shutdown information systems in an orderly manner protecting possible compromise of the information assets in the event of a

primary power source failing. This may provide support staff a means to prevent major system problems. The following policy addresses the requirement for organizations to provide uninterruptible power supplies to be used to allow for the proper shutdown of HUD information systems during an emergency.

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
HUD Policy: 4.31 a. The facilities group or Security Officer at facilities housing HUD information systems shall provide a short-term uninterrupted power supply (UPS) to facilitate an orderly shutdown in the event of a primary power source loss. b. The facilities group or Security Officer at facilities housing HUD information systems shall provide a long-term alternate power supply to maintain minimal operational capability for moderate- or high-impact systems in the event of an extended loss of the primary power source.

4.3.2. Emergency Lighting

Automatic emergency lighting systems that activate in the event of a power outage or disruption are a physical control that will provide safety to support staff. The following policy addresses the requirement to provide automatic emergency lighting in facilities that house HUD information systems.

NIST SP 800-53 Control: PE-12
PE-12: The organization employs and maintains automatic emergency lighting for the information systems that activate in the event of a power outage or disruption and that covers emergency exits and evacuation routes within the facility. Security Baseline: Low, Moderate, and High
HUD Policy: 4.3.2 a. The facilities group or Security Officer at facilities housing HUD information systems shall provide automatic emergency lighting systems that activate in the event of a power outage or disruption and cover emergency exits and evacuation routes.

4.3.3. Fire Protection

Fire protection is a physical control that will provide safeguard to the information assets. The following policy addresses the requirement to provide fire detection and suppression mechanisms in facilities that house HUD information systems.

NIST SP 800-53 Control: PE-13
PE-13: The organization employs and maintains fire suppression and detection devices/systems for the information systems that are supported by an independent energy source. Security Baseline: Low, Moderate, and High
E-1: The organization employs fire detection devices/systems for the information systems that activate automatically and notify [Assignment: organization-defined personnel or roles] and [Assignment: organization-defined emergency responders] in the event of a fire. Security Baseline: High
E-2: The organization employs fire suppression devices/systems for the information systems that provide automatic notification of any activation to [Assignment: organization-defined personnel or roles] and [Assignment: organization-defined emergency responders]. Security Baseline: High
E-3: The organization employs an automatic fire suppression capability for the information systems when the facility is not staffed on a continuous basis. Security Baseline: Moderate and High
HUD Policy: 4.3.3 a. The facilities group or Security Officer at facilities housing HUD information systems shall provide for fire suppression and detection devices/systems that can be activated in the event of fire. The devices/systems shall include, but are not limited to: • Sprinkler systems; • Handheld fire extinguishers; • Fixed fire hoses; and • Smoke detectors. b. For moderate- or high-impact systems, the facilities group or Security Officer at facilities housing HUD information systems shall provide fire suppression devices/systems that activate automatically in the event of fire. c. For high-impact systems, the facilities group or Security Officer at facilities housing HUD information systems shall provide fire suppression devices/systems that automatically notify any activation to the organization and emergency responders in the event of fire. d. For high-impact systems housed in facilities that are not continuously monitored shall include an automatic fire suppression capability.

4.3.4. Temperature and Humidity Controls

System components are susceptible to damage based on temperature levels and humidity. Therefore, it is important to monitor these environmental controls to ensure the availability of HUD information systems. The following policy addresses the requirement to monitor and maintain acceptable temperature and humidity levels in facilities that house HUD information systems.

NIST SP 800-53 Control: PE-14
PE-14: The organization: a. Maintains temperature and humidity levels within the facility where the information system resides at [Assignment: organization-defined acceptable levels]; and

NIST SP 800-53 Control: PE-14
b. Monitors temperature and humidity levels [Assignment: organization-defined frequency]. Security Baseline: Low, Moderate, and High
HUD Policy: 4.3.4 a. The facilities group or Security Officer at facilities housing HUD information systems shall ensure that facilities containing information systems monitor and maintain acceptable levels of temperature and humidity in accordance with industry standards (e.g., American Society of Heating, Refrigerating and Air-Conditioning Engineers (ASHRAE), and hardware manufacturer recommendations. b. The facilities group or Security Officer at facilities housing HUD information systems shall ensure that facilities containing information systems monitor temperature and humidity levels constantly.

4.3.5. Water Damage Protection

System components are susceptible to damage based on water leakage, so protections must be in place to prevent the occurrence of damage due to water. The following policy addresses the requirement to maintain mechanisms to protect HUD information systems from water damage in the event of faulty plumbing.

NIST SP 800-53 Control: PE-15
PE-15: The organization protects the information system from damage resulting from water leakage by providing master shutoff or isolation valves that are accessible, working properly, and known to key personnel. Security Baseline: Low, Moderate, and High
E-1: The organization employs automated mechanisms to detect the presence of water in the vicinity of the information system and alerts [Assignment: organization-defined personnel or roles]. Security Baseline: High
HUD Policy: 4.3.5 a. The facilities group or Security Officer at facilities housing HUD information systems shall ensure that the information systems contained in the facility are protected from water damage resulting from broken plumbing lines or other sources of water leakage by ensuring that master shutoff valves are accessible, working properly, and known to key personnel. b. For high-impact systems, the shutoff shall employ mechanisms that prevent water damage in the event of a significant water leak without manual intervention.

4.3.6. Delivery and Removal

Control procedures need to be followed and records maintained in order to monitor system-related items entering and exiting the facility. The following policy addresses the requirement for organizations to control the delivery and removal of information system-related items, as well as maintain documentation of these activities.

NIST SP 800-53 Control: PE-16
PE-16: The organization authorizes, monitors, and controls [Assignment: organization-defined types of information system components] entering and exiting the facility and maintains records of those items. Security Baseline: Low, Moderate, and High

NIST SP 800-53 Control: PE-16
HUD Policy: 4.3.6 a. The facilities group or Security Officer at facilities housing HUD information systems shall ensure that the facility has procedures to control the entering and exiting of information system-related items and maintains appropriate records. Delivery and removal of these items shall be authorized by a designated representative. If possible, the delivery area shall be separate from the system and media library area.

4.3.7. Alternate Work Site

In order to maintain security at alternate work sites, the level of security that exists at the primary work site must exist at the alternate work sites. The following policy addresses the requirement to maintain appropriate security controls at alternate work locations.

NIST SP 800-53 Control: PE-17
PE-17: The organization: a. Employs [Assignment: organization-defined security controls] at alternate work sites; b. Assesses the feasibility and the effectiveness of security controls at alternate work sites; and c. Provides a means for employees to communicate with information security personnel in case of security incidents or problems. Security Baseline: Moderate and High
HUD Policy: 4.3.7 a. For moderate- or high-impact systems, individuals within HUD shall employ appropriate security controls at alternate work sites in accordance with NIST SP 800-46, *Security for Telecommuting and Broadband Communications*. These individuals shall report security problems to the HUD's Computer Incident Response Team (HUD-CIRT).

4.3.8. Location of Information System Components

The placement of system components within a facility can prove an additional layer of physical security to minimize potential damage from physical and environmental hazards and to minimize the opportunity for unauthorized access. The following policy addresses the requirement to consider the placement of HUD information system components within facilities to minimize potential physical damage to the components.

NIST SP 800-53 Control: PE-18
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. Security Baseline: High
HUD Policy: 4.3.8 a. The Deputy CIO for IOO ensures that information system components hosted at infrastructure service provider facilities shall be stored to minimize potential damage from physical and environmental hazards Consideration shall be given to the location or site of the facility with regard to physical and environmental hazards. b. For information systems not hosted in an infrastructure service provider's facility, the Authorizing Official shall ensure that information system components shall be stored to minimize potential damage from physical and environmental hazards. Consideration shall be given to the location or site of the facility with regard to physical and environmental hazards.

4.4. Contingency Planning

Contingency planning relates to the establishment, maintainenance, 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 policies 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.

4.4.1. Contingency Planning Policy and Procedures

The contingency planning policy and procedures must be consistent with all other HUD policies, applicable laws, Executive Orders, Directives, policies, regulations, standards, and guidance. Where applicable, these policies and procedures will reference related HUD documents, either by name or document number, rather than repeating the requirements herein.

NIST SP 800-53 Control: CP-1
CP-1: The organization: a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]: 1. A contingency planning policy that addresses the purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the Contingency Planning Policy and associated contingency planning controls. b. Reviews and updates the current: 1. Contingency Planning Policy [Assignment: organization-defined frequency]; and 2. Contingency Planning procedures [Assignment: organization-defined frequency]. Security Baseline: Low, Moderate, and High
Implementation
This control is implemented by the *Information Technology Security Policy, Handbook 2400.25 Rev. 4,* that defines HUD's formal security policies and the HUD *Information Technology Security Procedures* that defines HUD's formal security procedures. HUD reviews the policies and procedures minimally every year or when impacted by a significant change or underlying standard. The HUD security policies and procedures are disseminated via the HUD Intranet for all HUD's users to access.

4.4.2. Contingency Plan

A Contingency Plan is a set of management policies and procedures designed to maintain or restore business operations, including computer operations, in the event of emergencies, system failures, or disaster. The following policy addresses the requirement to develop and maintain Contingency Plans and Business Impact Assessments for HUD information systems.

NIST SP 800-53 Control: CP-2
CP-2: The organization: a. Develops a Contingency Plan for the information system that: 1. Identifies essential missions and business functions and associated contingency requirements; 2. Provides recovery objectives, restoration priorities, and metrics; 3. Addresses contingency roles, responsibilities, assigned individuals with contact information; 4. Addresses maintaining essential missions and business functions despite an information system disruption, compromise, or failure; and 5. Addresses eventual, full information system restoration without deterioration of the security safeguards originally planned and implemented. b. Is reviewed and approved by [Assignment: organization-defined personnel or roles]; c. Distributes copies of the Contingency Plan to [Assignment: organization-defined key contingency personnel (identified by name and/or by role) and organizational elements]; d. Coordinates contingency planning activities with incident handling activities; e. Reviews the Contingency Plan for the information system [Assignment: organization-defined frequency]; f. Updates the Contingency Plan to address changes to the organization, information system, or environment of operation as well as problems encountered during contingency plan implementation, execution, or testing; g. Communicates contingency plan changes to [Assignment: organization-defined key contingency personnel (identified by name and/or by role) and organizational elements]; and h. Protects the Contingency Plan from unauthorized disclosure and modification. 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
E-2: The organization conducts capacity planning so that necessary capacity for information processing, telecommunications, and environmental support exists during contingency operations. Security Baseline: High
E-3: The organization plans for the resumption of essential missions and business functions within [*Assignment: organization-defined time period*] of contingency plan activation. Security Baseline: Moderate and High
E-4: The organization plans for the resumption of all missions and business functions within [Assignment: organization-defined time period] of contingency plan activation. Security Baseline: High
E-5: The organization plans for the continuance of essential missions and business functions with little or no loss of operational continuity and sustains that continuity until full information system restoration at primary processing and/or storage sites. Security Baseline: High

NIST SP 800-53 Control: CP-2
E-8: The organization identifies critical information system assets supporting essential missions and business functions. Security Baseline: Moderate and High
HUD Policy: 4.4.2 a. Program Offices/System Owners shall develop Contingency Plans, including a Business Impact Analysis, for information systems under their purview in accordance with the HUD *Contingency Plan Guidance* and NIST SP 800-34: *Contingency Planning Guide for Federal Information Systems*. b. Program Offices/System Owners shall, as part of their Business Impact Analyses, complete a HUD Mission Critical Questionnaire which becomes part of the system security planning package. c. For moderate- or high-impact systems, Program Offices/System Owners shall coordinate with the Program Office(s) responsible for Critical Infrastructure Protection (CIP) and Continuity of Operations (COOP). d. For high-impact systems, Program Offices/System Owners shall conduct capacity planning so that the necessary capacity for information processing, telecommunications, and environmental support exists during crisis situations. e. Program Offices/System Owners shall develop a list of key individuals with contingency roles and responsibilities. f. Program Offices/System Owners shall make the Contingency Plans, and any updates, available to these key individuals. g. The OCIO shall establish and maintain a HUD-CIRT to prevent, detect, track, and respond to information security incidents and alerts in accordance with NIST SP 800-61, *Computer Security Incident Handling Guide*. (See IR-4). h. Program Offices/System Owners shall review Contingency Plans once a year (generally in conjunction with the annual contingency plan test), update the plans as necessary, and communicate any changes to the Program Office(s) responsible for COOP and CIP.

4.4.3. Contingency Training

In the event of an emergency, there is usually less time for planning and reacting, therefore, personnel with significant contingency planning roles need to be trained on their responsibilities to ensure that any delay in recovering critical systems is minimal. The following policy addresses the requirement for all personnel involved in information system contingency planning to receive training in contingency planning procedures and logistics.

NIST SP 800-53 Control: CP-3
CP-3: The organization provides contingency training to information system users consistent with assigned roles and responsibilities: a. Within [Assignment: organization-defined time period] of assuming a contingency role or responsibility; b. When required by information system changes; and c. [Assignment: organization-defined frequency] thereafter. Security Baseline: Low, 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
HUD Policy: 4.4.3 a. Program Offices/System Owners shall ensure that all personnel involved in information system contingency

NIST SP 800-53 Control: CP-3
planning efforts are identified and trained in the procedures and logistics of information system contingency planning, and implementation for moderate- and high-impact systems under their purview and in compliance with the HUD *Contingency Planning Guidance* and NIST SP 800-34. b. Refresher training shall be provided annually. For high-impact systems, the training shall include simulated events.

4.4.4. Contingency Plan Testing and Exercises

Executing Contingency Plans during controlled tests and/or exercises provides a mechanism to test the effectiveness of the contingency plans, the training provided, and to correct weaknesses in the plan in a controlled situation. The following policy addresses the requirement to conduct testing of contingency plans for HUD information systems on a regular basis.

NIST SP 800-53 Control: CP-4
CP-4: The organization: a. Tests the Contingency Plan for the information system [Assignment: organization-defined frequency] using [Assignment: organization-defined tests] to determine the effectiveness of the plan and the organizational readiness to execute the plan; b. Reviews the contingency plan test results; and c. Initiates corrective actions, if needed. Security Baseline: Low, Moderate and High
E-1: The organization coordinates contingency plan testing and/or exercises with organizational elements responsible for related plans. Security Baseline: Moderate and High
E-2: The organization tests the Contingency Plan at the alternate processing site: (a) To familiarize contingency personnel with the facility and available resources; and (b) To evaluate the capabilities of the alternate processing site to support contingency operations. Security Baseline: High
HUD Policy: 4.4.4 a. Program Offices/System Owners shall ensure that Contingency Plans are tested/exercised at least once during a federal Fiscal Year (FY) in compliance with the HUD *Contingency Planning Guidance* and NIST SP 800-34. Testing should be coordinated with elements responsible for Disaster Recovery, COOP, CIP, and incident response. b. Program Offices/System Owners should review the Mission Critical designation as part of the annual contingency plan test to ensure no change in status. The OCIO shall be notified of any changes in status. c. For high-impact systems, the Program Offices/System Owners shall ensure annual testing at the alternate processing site and provide, as part of contingency plan testing, full recovery of the information system to a known state.

4.4.5. Alternate Storage Site

In order to support events requiring the recovery of information systems, the information necessary to recover the system must be stored at an alternate site. The following policy addresses the requirement for organizations to identify alternate sites for storage of information system backups.

NIST SP 800-53 Control: CP-6
CP-6: The organization: a. Establishes an alternate storage site including necessary agreements to permit the storage and retrieval of information system backup information; and b. Ensures that the alternate storage site provides information security safeguards equivalent to that of the primary site. Security Baseline: Moderate and High
E-1: The organization identifies an alternate storage site that is separated from the primary storage site to reduce susceptibility to the same threats. Security Baseline: Moderate and High
E-2: The organization configures the alternate storage site to facilitate recovery operations in accordance with recovery time and recovery point objectives. Security Baseline: High
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. Security Baseline: Moderate and High
HUD Policy: 4.4.5 a. The OCIO shall provide an alternate site for storing system backup information. The alternate site must be geographically separated from the primary storage site for backup information of moderate- or high-impact systems and shall: • Be configured to facilitate recovery operations in accordance with recovery time and recovery point objectives for high-impact systems. • Identify potential accessibility problems in the event of an area-wide disruption or disaster and outline explicit mitigation actions

4.4.6. Alternate Processing Site

In order to support the recovery of information systems in an emergency, it may be necessary to recover at an alternate processing site as the primary site might not be accessible. The following policy addresses the requirement for organizations to identify alternate sites for the resumption of information system operations in the event of a disaster or major disruption of services.

NIST SP 800-53 Control: CP-7
CP-7: The organization: a. Establishes an alternate processing site including necessary agreements to permit the transfer and resumption of [Assignment: organization-defined information system operations] for essential missions/business functions within [Assignment: organization-defined time period consistent with recovery time and recovery point objectives] when the primary processing capabilities are unavailable; b. Ensures that equipment and supplies required to transfer and resume operations are available at the alternate processing site or contracts are in place to support delivery to the site within the organization-defined time period for transfer/resumption; and c. Ensures that the alternate processing site provides information security safeguards equivalent to that of the primary site. Security Baseline: Moderate and High

NIST SP 800-53 Control: CP-7
E-1: The organization identifies an alternate processing site that is separated from the primary processing site to reduce susceptibility to the same threats. Security Baseline: Moderate and High
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. Security Baseline: Moderate and High
E-3: The organization develops alternate processing site agreements that contain priority-of-service provisions in accordance with organizational availability requirements (including recovery time objectives). Security Baseline: Moderate and High
E-4: The organization prepares the alternate processing site so that the site is ready to be used as the operational site supporting essential missions and business functions. Security Baseline: High
HUD Policy: 4.4.6 a. The OCIO shall provide an alternate processing site for systems with a moderate- or high-impact availability rating and ensure that the equipment and supplies required to resume operations are either available at the alternate site or contracts are in place to support delivery to the site. The alternate site shall: • Be geographically separated from the primary processing site; • Be reviewed to identify potential accessibility problems in the event of an area-wide disruption or disaster and outline explicit mitigation actions; • Have priority-of-service provisions in accordance with HUD's availability requirements; and • Provides information security measures equivalent to the primary site. b. For high-impact systems, the Program Offices/System Owners shall ensure site is fully configured to support essential missions and business functions and be ready to use as the operational site.

4.4.7. Telecommunications Services

Telecommunications services are a key in technology operations. As such, the organization needs to identify both the primary and alternate services that will support the IT operations. The following policy addresses the requirement for organizations to identify alternate telecommunications services for the resumption of information system operations in the event of a disaster or major disruption of services.

NIST SP 800-53 Control: CP-8
CP-8: The organization establishes alternate telecommunications services including necessary agreements to permit the resumption of [*Assignment: organization-defined information system operations*] for essential missions and business functions within [*Assignment: organization-defined time period*] when the primary telecommunications capabilities are unavailable at either the primary or alternate processing or storage sites. Security Baseline: Moderate and High

NIST SP 800-53 Control: CP-8
E-1: The organization: a. Develops primary and alternate telecommunications service agreements that contain priority-of-service provisions in accordance with organizational availability requirements (including recovery time objectives); and b. Requests Telecommunications Service Priority for all telecommunications services used for national security emergency preparedness in the event that the primary and/or alternate telecommunications services are provided by a common carrier. Security Baseline: Moderate and High
E-2: The organization obtains alternate telecommunications services to reduce the likelihood of sharing a single point of failure with primary telecommunications services. Security Baseline: Moderate and High
E-3: The organization obtains alternate telecommunications services from providers that are separated from primary service providers to reduce susceptibility to the same threats. Security Baseline: High
E-4: The organization: a. Requires primary and alternate telecommunications service providers to have Contingency Plans; b. Reviews provider Contingency Plans to ensure that the plans meet organizational contingency requirements; and c. Obtains evidence of contingency testing/training by providers [Assignment: organization-defined frequency]. Security Baseline: High

NIST SP 800-53 Control: CP-8
HUD Policy: 4.4.7 a. In the event that the primary and/or alternate telecommunications services are provided by a wire line carrier, the OCIO shall request Telecommunications Service Priority (TSP) for all telecommunications services used for national security emergency preparedness available within 24 hours. b. The Deputy CIO for IOO shall provide for primary and alternate telecommunications services to support moderate- and high-impact systems that reside on HUD's infrastructure. The Deputy CIO for IOO shall also initiate the necessary agreement to permit the resumption of system operations for critical business functions within 24 hours when primary telecommunications are unavailable. The Deputy CIO for IOO shall ensure that: • Agreements contain priority-of-service provisions in accordance with HUD's availability requirements; and • Alternate service does not share a single point of failure with the primary service. • Providers of alternate sites are sufficiently separated from primary service providers so they are not susceptible to the same hazards. c. For information systems not host on the infrastructure platform, the Authorizing Official shall provide for primary and alternate telecommunications services to support moderate- and high-impact systems. The Authorizing Official shall also initiate the necessary agreement to permit the resumption of system operations for critical business functions within 24 hours when primary telecommunications are unavailable and that: • Agreements contain priority-of-service provisions in accordance with HUD's availability requirements; and • Alternate service does not share a single point of failure with the primary service. • Providers of alternate sites are sufficiently separated from primary service providers so they are not susceptible to the same hazards. d. For high-impact systems, the Program Officers/System Owners shall ensure that: • Providers of primary and alternate services have adequate Contingency Plans; • Providers of primary and alternate services provide evidence of contingency testing/planning.

4.4.8. Information System Backup

In order to successfully recover an information system, the components of the system and data must be backed up successfully. For each system, it must be determined what information must be backed up and necessary for the successful recovery of the system.

The frequency in which the backups are performed will depend on the availability requirement of the data. It is important that these backups be tested to ensure their usability.

The following policy addresses the requirement for organizations to conduct backups of system-level and user-level information contained in the information system.

NIST SP 800-53 Control: CP-9
CP-9: The organization: a. Conducts backups of user-level information contained in the information system [Assignment: organization-defined frequency consistent with recovery time and recovery point objectives]; b. Conducts backups of system-level information contained in the information system [Assignment: organization-defined frequency consistent with recovery time and recovery point objectives]; c. Conducts backups of information system documentation including security-related documentation [Assignment: organization-defined frequency consistent with recovery time and recovery point objectives]; and d. Protects the confidentiality, integrity, and availability of backup information at storage locations. Security Baseline: Low, Moderate, and High
E-1: The organization tests backup information [Assignment: organization-defined frequency] to verify media reliability and information integrity. Security Baseline: Moderate and High
E-2: The organization uses a sample of backup information in the restoration of selected information system functions as part of contingency plan testing. Security Baseline: High
E-3: The organization stores backup copies of [Assignment: organization-defined critical information system software and other security-related information] in a separate facility or in a fire-rated container that is not co-located with the operational system. Security Baseline: High
E-5: The organization transfers information system backup information to the alternate storage site [Assignment: organization-defined time period and transfer rate consistent with the recovery time and recovery point objectives]. Security Baseline: High
HUD Policy: 4.4.8 a. Program Offices/System Owners shall ensure that a backup strategy and procedures are established, implemented, and tested in accordance with the Contingency Plan. b. The OCIO shall implement and enforce backup procedures for all sensitive information systems, data, and information that reside on HUD's infrastructure. The backups shall include user-level and system-level information. c. The OCIO shall store backups at a secure off-site location in accordance with the Contingency Plans. d. The OCIO shall test backup information quarterly for moderate- and high-impact systems that reside on HUD's infrastructure to verify media reliability and information integrity. e. For high-impact systems, the Program Offices/System Owners shall ensure: • Test backup information in the restoration of information system functions as part of contingency planning for high-impact systems; • Store backup copies of the operating system and other critical information systems software in a fire-rated container that is not co-located with the operational software or in a separate facility; and • Protect system backup information from unauthorized modification whenever it is removed from a HUD facility.

4.4.9. Information System Recovery and Reconstitution

The goal of contingency planning is the successful recovery and reconstitution of the information system to a secure and usable state. The following policy addresses the requirement for organizations to implement mechanisms and procedures for the recovery of an information system after a disruption.

NIST SP 800-53 Control: CP-10
CP-10: The organization provides for the recovery and reconstitution of the information system to a known state after a disruption, compromise, or failure. Security Baseline: Low, Moderate, and High
E-2: The information system implements transaction recovery for systems that are transaction-based. Security Baseline: Moderate and High
E-4: The organization provides the capability to restore information system components within [Assignment: organization-defined restoration time-periods] from configuration-controlled and integrity-protected information representing a known, operational state for the components. Security Baseline: High
HUD Policy: 4.4.9 a. The OCIO shall ensure that HUD has mechanisms with supporting procedures to allow the information system to be recovered and reconstituted to a known secure state after a disruption or failure. b. For high-impact systems, the OCIO shall ensure that the systems are fully recovered and reconstituted as part of the contingency plan test.

4.5. Configuration Maintenance

Configuration management is the act of managing the configuration of all hardware and software elements of information systems and networks and assessing 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.

Configuration Management has security implications in three areas to ensure:

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

The following procedures ensure that there are mechanisms in place to establish and maintain the configuration baseline and monitor 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.

4.5.1. Configuration Management Policy and Procedures

The configuration management policy and procedures must be consistent with HUD policies, applicable laws, Executive Orders, Directives, policies, regulations, standards, and guidance. Where applicable, the configuration management policy and procedures will refer to the references by the associated reference description or number, so that these policies are not repeating the reference.

NIST SP 800-53 Control: CM-1
CM-1: The organization: a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]: 1. A Configuration Management Policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the Configuration Management Policy and associated configuration management controls. b. Reviews and updates the current: 1. Configuration Management Policy [Assignment: organization-defined frequency]; and 2. Configuration Management procedures [Assignment: organization-defined frequency]. Security Baseline: Low, Moderate, and High
Implementation
This control is implemented by the *Information Technology Security Policy, Handbook 2400.25 Rev. 4,* that defines HUD's formal security policies and the HUD *Information Technology Security Procedures* that defines HUD's formal security procedures. HUD reviews the policies and procedures minimally every year or when impacted by a significant change or underlying standard. The HUD security policies and procedures are disseminated via the HUD Intranet for all HUD's users to access.

4.5.2. Baseline Configuration

Baseline configurations must be developed and documented for the information systems and serve as a reference point for the system. The baseline should be updated whenever configuration changes are made to the system and can be changed only through change control procedures.

NIST SP 800-53 Control: CM-2
CM-2: The organization develops, documents, and maintains under configuration control, a current baseline configuration of the information system.

NIST SP 800-53 Control: CM-2
Security Baseline: Low, Moderate, and High
E-1: The organization reviews and updates the baseline configuration of the information system: a. [Assignment: organization-defined frequency]; b. When required due to [Assignment organization-defined circumstances]; and c. As an integral part of information system component installations and upgrades. 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
E-3: The organization retains [Assignment: organization-defined previous versions of baseline configurations of the information system] to support rollback. Security Baseline: Moderate and High
E-7: The organization: a. Issues [Assignment: organization-defined information systems, system components, or devices] with [Assignment: organization-defined configurations] to individuals traveling to locations that the organization deems to be of a significant risk; and b. Applies [Assignment: organization-defined security safeguards] to the devices when the individuals return. Security Baseline: Moderate and High
HUD Policy: 4.5.2 a. The OCIO shall develop, document, and maintain current baseline configurations that are consistent with Federal Directives, the National Institute of Standards and Technology (NIST), the National Security Agency (NSA), the US Government Configuration Baseline (USGCB), checklists from the Defense Information Systems Agency (DISA), and the HUD Enterprise Architecture Policy. b. The OCIO shall review and update baseline configurations of the information systems annually or as required and retain one previous version to support rollback. c. The OCIO maintains an inventory of software programs authorized to execute on HUD's network and uses a 'deny-by-exception' policy to identify unauthorized software on the information system.

4.5.3. Configuration Change Control

Configuration Change Control provides a method for moving a configuration change from an initial request to a release into the operational environment. In order to maintain change control of operational information systems, it is important that changes are documented, tested and approved. All changes made to HUD information systems will be made in a controlled fashion to preserve the confidentiality, integrity and availability of the system. In order to facilitate the changes, a configuration change control process must be implemented. The following policy addresses the establishment of a configuration control process.

NIST SP 800-53 Control: CM-3
CM-3: The organization: a. Determines the types of changes to the information system that are configuration-controlled; b. Reviews proposed configuration-controlled changes to the information system and approves or disapproves such changes with explicit consideration for security impact analyses;

NIST SP 800-53 Control: CM-3

c. Documents configuration change decisions associated with the information system;
d. Implements approved configuration-controlled changes to the information system;
e. Retains records of configuration-controlled changes to the information system for [Assignment: organization-defined time period];
f. Audits and reviews activities associated with configuration-controlled changes to the information system; and
g. Coordinates and provides oversight for configuration change control activities through [Assignment: organization-defined configuration change control element (e.g., committee, board)] that convenes [Selection (one or more): [Assignment: organization-defined frequency]; [Assignment: organization-defined configuration change conditions]].

Security Baseline: Moderate and High

E-1: The organization employs automated mechanisms to:

a. Document proposed changes to the information system;
b. Notify [Assignment: organized-defined approval authorities] of proposed changes to the information system and request change approval;
c. Highlight proposed changes to the information system that have not been approved or disapproved by [Assignment: organization-defined time period];
d. Prohibit changes to the information system until designated approvals are received;
e. Document all changes to the information system; and
f. Notify [Assignment: organization-defined personnel] when approved changes to the information system are completed.

Security Baseline: High

E-2: The organization tests, validates, and documents changes to the information system before implementing the changes on the operational system.

Security Baseline: Moderate and High

HUD Policy: 4.5.3

a. Program Offices/System Owners shall prepare Configuration Management Plans for all information systems and networks under their purview.
b. The OCIO infrastructure is subject to a change control process that:
   - Determines and reviews types of changes to the infrastructure;
   - Reviews audit activities associated with configuration changes to the infrastructure;
   - Documents approved changes; and
   - Approves security-related changes to the infrastructure.
c. The OCIO shall establish, implement, and enforce change management and configuration management controls on all information systems and networks under their control. The security impact of any proposed change must be analyzed and considered during the change management process. Changes to the information system must be documented and they must include emergency change procedures.
d. The OCIO established a Software Configuration Control Board (SCCB) that has the authority for managing the project's software baselines. Guidelines for the SCCB are provided in the Software Configuration Management (SCM) procedures document located on the HUD website.
e. For high-impact systems, the system shall use automated mechanisms to:
   - Document proposed changes;
   - Notify appropriate approval authorities;
   - Obtain approval for each proposed change prior to implementation;
   - Highlight approvals that have not been received in a timely manner;
   - Inhibit change until necessary approvals are received; and

NIST SP 800-53 Control: CM-3
• Document completed changes.

4.5.4. Security Impact Analysis

Security Impact Analyses include reviewing information system documentation such as security plans to understand how specific controls are implemented within the system and how the changes might affect the controls. It also includes an assessment of risk to understand the impact of the changes and to determine if additional security controls are required.

NIST SP 800-53 Control: CM-4
CM-4: The organization analyzes changes to the information system to determine potential security impacts prior to change implementation. Security Baseline: Low, Moderate and High
E-1: The organization analyzes changes to the information system in a separate test environment before implementation in an operational environment, looking for security impacts due to flaws, weaknesses, incompatibility, or intentional malice. Security Baseline: High
HUD Policy: 4.5.4 a. The OCIO shall monitor and audit changes to the infrastructure under their control and check the security features of the system to ensure the features are still functioning properly.

4.5.5. Access Restrictions for Change

In order to maintain control of changes to information systems, only authorized personnel based on their job responsibilities should be able to implement changes to the system. This provides control over the system and the configuration and ensures that no unplanned changes are made either accidentally or intentionally. The following policy addresses the requirement for organizations to approve and restrict individual access to those persons who are responsible for making changes to HUD information systems.

NIST SP 800-53 Control: CM-5
CM-5: The organization defines documents, approves, and enforces physical and logical access restrictions associated with changes to the information system. Security Baseline: Moderate and High
E-1: The information system enforces access restrictions and supports auditing of the enforcement actions. Security Baseline: High
E-2: The organization reviews information system changes [Assignment: organization-defined frequency] and [Assignment: organization-defined circumstances] to determine whether unauthorized changes have occurred. Security Baseline: High

NIST SP 800-53 Control: CM-5
E-3: The information system prevents the installation of [Assignment: organization-defined software and firmware components] without verification that the component has been digitally signed using a certificate that is recognized and approved by the organization. Security Baseline: High
HUD Policy:4.5.5 a. The OCIO limits personnel authorized to make changes to the infrastructure based on their job responsibilities and approve individuals (in writing) that are authorized to make changes to the infrastructure. b. The OCIO reviews and updates access restrictions based on changes in staff responsibilities, transfers, and terminations. c. The OCIO uses automated mechanisms to enforce access restrictions and supports auditing for high-impact systems.

4.5.6. Configuration Settings

IT products are configured based on organizational requirements. IT products should be configured to the most restrictive security settings while continuing to allow the product to meet the organization's needs. The following policy addresses the requirement to establish and implement standard configuration settings for HUD information systems.

NIST SP 800-53 Control: CM-6
CM-6: The organization: a. Establishes and documents configuration settings for information technology products employed within the information system using [Assignment: organization-defined security configuration checklists] that reflect the most restrictive mode consistent with operational requirements; b. Implements the configuration settings; c. Identifies, documents, and approves any deviations from established configuration settings for [Assignment: organization-defined information system components] based on [Assignment: organization-defined operational requirements]; and d. Monitors and controls changes to the configuration settings in accordance with organizational policies and procedures. Security Baseline: Low, Moderate, and High
E-1: The organization employs automated mechanisms to centrally manage, apply, and verify configuration settings for [Assignment: organization-defined information system components]. Security Baseline: High
E-2: The organization employs [Assignment: organization-defined security safeguards] to respond to unauthorized changes to [Assignment: organization-defined configuration settings]. Security Baseline: High
HUD Policy: 4.5.6 a. The OCIO relies on the National Institute of Standards and Technology SP 800-70, *Security Configuration Checklists Program for IT Products and Federal Desktop Core Configurations, the National Security Agency Guide*, and the checklists from the *DISA Security Technical Implementation Guide*, and configures the system accordingly. b. For high-impact systems, the system shall use automated mechanisms to centrally apply and verify configuration settings.

NIST SP 800-53 Control: CM-6
c. If there are no configuration checklists, HUD will rely on vendor-specific configurations set to the most restrictive posture. d. The OCIO shall ensure detection of unauthorized, security-relevant configuration changes are incorporated into the HUD's incident response capability.

4.5.7. Least Functionality

Least functionality helps to minimize the potential for security vulnerabilities. Functionality that is not critical to support essential organizational operations may introduce an unnecessary threat to the system. The following policy addresses the requirement to configure systems/interfaces to prohibit the use of any unauthorized protocol or service.

NIST SP 800-53 Control: CM-7
CM-7: The organization: a. Configures the information system to provide only essential capabilities; and b. Prohibits or restricts the use of the following functions, ports, protocols, and/or services: [Assignment: organization-defined prohibited or restricted functions, ports, protocols, and/or services]. Security Baseline: Low, Moderate and High
E-1: The organization: a. Reviews the information system [Assignment: organization-defined frequency] to identify unnecessary and/or nonsecure functions, ports, protocols, and services; and b. Disables [Assignment: organization-defined functions, ports, protocols, and services within the information system deemed to be unnecessary and/or nonsecure]. Security Baseline: Moderate and High
E-2: The information system prevents program execution in accordance with [Selection (one or more): [Assignment: organization-defined policies regarding software program usage and restrictions]; rules authorizing the terms and conditions of software program usage]. Security Baseline: Moderate and High
E-4: The organization: a. Identifies [Assignment: organization-defined software programs not authorized to execute on the information system]; b. Employs an allow-all, deny-by-exception policy to prohibit the execution of unauthorized software programs on the information system; and c. Reviews and updates the list of unauthorized software programs [Assignment: organization-defined frequency]. Security Baseline: Moderate
E-5: The organization: a. Identifies [Assignment: organization-defined software programs authorized to execute on the information system]; b. Employs a deny-all, permit-by-exception policy to allow the execution of authorized software programs on the information system; and c. Reviews and updates the list of authorized software programs [Assignment: organization-defined frequency]. Security Baseline: High

NIST SP 800-53 Control: CM-7
HUD Policy: 4.5.7 a. The OCIO manages HUD's ports, protocols and services. b. The OCIO operates in accordance with the principle to "Deny All" except those ports, protocols and services that are permitted, maintains an inventory of allowed ports, and protocol services. c. The OCIO actively monitors ports, protocols and services and eliminates as threats and vulnerabilities are identified.

4.5.8. Information System Component Inventory

In order for HUD to maintain information systems security, it is essential that a current inventory of system components be maintained. The inventory provides a means of tracking the security posture of HUD's IT assets and tracking system responsibility and compliance with security requirements for those assets. The following policy addresses the requirement to develop and maintain a current inventory of all HUD information system assets.

NIST SP 800-53 Control: CM-8
CM-8: The organization: a. Develops and documents an inventory of information system components that: 1. Accurately reflects the current information system; 2. Includes all components within the authorization boundary of the information system; and 3. Is at the level of granularity deemed necessary for tracking and reporting. b. Includes [Assignment: organization-defined information deemed necessary to achieve effective information system component accountability]; and c. Reviews and updates the information system component inventory [Assignment: organization-defined frequency]. Security Baseline: Low, Moderate, and High
E-1: The organization updates the inventory of information system components as an integral part of component installations, removals, and information system updates. Security Baseline: Moderate and High
E-2: The organization employs automated mechanisms to help maintain an up-to-date, complete, accurate, and readily available inventory of information system components. Security Baseline: High
E-3: The organization: a. Employs automated mechanisms [Assignment: organization-defined frequency] to detect the presence of unauthorized hardware, software, and firmware components within the information system; and b. Takes the following actions when unauthorized components are detected: [Selection (one or more): disables network access by such components; isolates the components; notifies [Assignment: organization-defined personnel or roles]]. Security Baseline: Moderate and High

NIST SP 800-53 Control: CM-8
E-4: The organization includes in the information system component inventory information, a means for identifying by [Selection (one or more): name; position; role], individuals responsible/accountable for administering those components. Security Baseline: High
E-5: The organization verifies that all components within the authorization boundary of the information system are not duplicated in other information system component inventories. Security Baseline: Moderate and High
HUD Policy: 4.5.8 a. The Office of Administration and Management Services (OAMS) in conjunction with OCIO tracks and documents the inventory of information system components. The inventory is maintained in a central repository, (i.e., Facilities Integrated Resource Management System, D67A). b. The OAMS is accountable for inventorying all systems hardware and micro-computers using HUD's Central repository. c. Program Offices/System Owners record and maintain current information system components in System Security Plans. d. The OAMS updates and documents changes that are made to the inventory of system components and records updates into HUD's central repository. e. Program Offices/System Owners verify that all system components are inventoried tri-annually as part of their information systems Authorization to Operate process.

4.5.9. Configuration Management Plan

A Configuration Management Plan (CMP) is a comprehensive description of the roles, responsibilities, policies, and procedures that apply when managing the configuration of products and systems. The purpose of HUD's Software Configuration Management Plan (SCMP) is to establish and maintain the integrity of products of software projects throughout the project's software life cycle. The following policy addresses the requirement to develop a Configuration Management Plan.

NIST SP 800-53 Control: CM-9
CM-9: The organization develops, documents, and implements a Configuration Management Plan for the information system that: a. Addresses roles, responsibilities, and configuration management processes and procedures; b. Establishes a process for identifying configuration items throughout the system development life cycle and for managing the configuration of the configuration items; c. Defines the configuration items for the information system and places the configuration items under configuration management; and d. Protects the Configuration Management Plan from unauthorized disclosure and modification. Security Baseline: Moderate and High

NIST SP 800-53 Control: CM-9
HUD Policy: 4.5.9 a. The OCIO develops and maintains HUD's Software Configuration Management Policy which identifies roles and responsibilities at the organizational level, as well as a configuration management process, and procedures in accordance with *HUD's Software Configuration Management Plan* and NIST 800-128, *Guide for Security Configuration Management of Information Systems.* b. Program Offices/System Owners create a Configuration Management Plan for the systems under their control which identifies roles and responsibilities at the system level, as well as a configuration management process and procedures in accordance with *HUD's Software Configuration Management Plan* and NIST 800-128, *Guide for Security Configuration Management of Information Systems.* c. The OCIO defines and identifies the configuration items, components, and products that will be placed in the HUD Software Configuration Management Plan. d. Program Offices/System Owners ensures that all HUD system releases go through HUD's formal release processes.

4.6. Maintenance

Regular maintenance of information systems mitigates some of the threats to the system. The maintenance control addresses policies to ensure that regular system maintenance and repairs occur. This policy reflects the predominant business model under which maintenance functions are generally outsourced to IT service providers. The federal function, assigned to the CIO, is one of oversight to ensure service providers maintain IT assets consistent with federal standards. As a result, responsibilities are assigned to designated agents of the Federal CIO which can include HUD Program Offices, Private Contractor, or other federal agencies.

FIPS 200 Requirement
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.

4.6.1. System Maintenance Policy and Procedures

The system maintenance policy and procedures must be consistent with HUD policies, applicable laws, Executive Orders, Directives, policies, regulations, standards, and guidance. Where applicable, the system maintenance policy and procedures will refer to the references by the associated reference description or number, so that these policies are not repeating the reference.

NIST SP 800-53 Control: MA-1
MA-1: The organization: a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]: 1. A System Maintenance Policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the System Maintenance Policy and associated system maintenance controls. b. Reviews and updates the current: 1. System Maintenance Policy [Assignment: organization-defined frequency]; and 2. System maintenance procedures [Assignment: organization-defined frequency]. Security Baseline: Low, Moderate, and High
Implementation
This control is implemented by the *Information Technology Security Policy, Handbook 2400.25 Rev. 4,* that defines HUD's formal security policies and the HUD *Information Technology Security Procedures* that defines HUD's formal security procedures. HUD reviews the policies and procedures minimally every year or when impacted by a significant change or underlying standard. The HUD security policies and procedures are disseminated via the HUD Intranet for all HUD's users to access.

4.6.2. Controlled Maintenance

Controlled maintenance of system components will provide some assurance that the component will not fail or become vulnerable to a security threat. The following policy addresses the requirement to conduct routine preventive and regular maintenance on HUD owned/leased hardware and software and equipment operated on HUD's behalf.

NIST SP 800-53 Control: MA-2
MA-2: The organization: a. Schedules, performs, documents, and reviews records of maintenance and repairs on information system components in accordance with manufacturer or vendor specifications and/or organizational requirements; b. Approves and monitors all maintenance activities, whether performed on site or remotely and whether the equipment is serviced on site or removed to another location; c. Requires that [Assignment: organization-defined personnel or roles] explicitly approve the removal of the information system or system components from organizational facilities for off-site maintenance or repairs; d. Sanitizes equipment to remove all information from associated media prior to removal from organizational facilities for off-site maintenance or repairs; e. Checks all potentially impacted security controls to verify that the controls are still functioning properly following maintenance or repair actions; and f. Includes [Assignment: organization-defined maintenance-related information] in organizational maintenance records. Security Baseline: Low, Moderate, and High
E-2: The organization: a. Employs automated mechanisms to schedule, conduct, and document maintenance and repairs; and b. Produces up-to date, accurate, and complete records of all maintenance and repair actions requested, scheduled, in process, and completed. Security Baseline: High

NIST SP 800-53 Control: MA-2
HUD Policy: 4.6.2 The CIO or designated agent shall: a. Ensure that routine preventive and regular maintenance is performed on software and hardware according to manufacturer/vendor specifications and/or organizational requirements. For moderate- or high-high impact systems, a log shall be maintained for such maintenance and include the following: • Date and time of the maintenance; • Name of the individual performing the maintenance; • Name of the escort, if necessary; • Description of the maintenance performed; and • A list of the equipment removed or replaced (including identification numbers, if applicable). b. Ensure that an appropriate organizational official approves the removal of the information system or its components from the facility when repairs are necessary. c. Ensure that the security features of the system are checked to ensure proper functioning when it is returned. d. That maintenance ports are disabled by default and enabled only during maintenance. e. That the maintenance is scheduled and conducted, as required.

4.6.3. Maintenance Tools

HUD must ensure that all maintenance tools are controlled, monitored and approved for use to conduct maintenance on system components. The following policy addresses the requirement that all tools utilized for maintaining HUD information systems be approved and controlled.

NIST SP 800-53 Control: MA-3
MA-3: The organization approves, controls, and monitors information system maintenance tools. Security Baseline: Moderate and High
E-1: The organization inspects the maintenance tools carried into a facility by maintenance personnel for improper or unauthorized modifications. Security Baseline: Moderate and High
E-2: The organization checks media containing diagnostic and test programs for malicious code before the media are used in the information system. Security Baseline: Moderate and High
E-3: The organization prevents the unauthorized removal of maintenance equipment containing organizational information by: a. Verifying that there is no organizational information contained on the equipment; b. Sanitizing or destroying the equipment; c. Retaining the equipment within the facility; or d. Obtaining an exemption from [Assignment: organization-defined personnel or roles] explicitly authorizing removal of the equipment from the facility. Security Baseline: High
HUD Policy: 4.6.3 a. The CIO or designated agent shall ensure that appropriate organization officials approve, control, and monitor the use of information system maintenance tools and maintain such tools on an ongoing basis.

4.6.4. Nonlocal Maintenance

Remote maintenance presents several opportunities for compromising the security of a system; first, HUD has no control over the security of the maintenance provider's network and, secondly, identification and authentication of the provider is challenging. During maintenance of system components, the provider is modifying the system component while increasing the possibility of accidental or intentional compromise.

The following policy addresses the requirement that all remote maintenance on HUD information systems is authorized and controlled by HUD personnel.

NIST SP 800-53 Control: MA-4
MA-4: The organization: a. Approves and monitors non-local maintenance and diagnostic activities; b. Allows the use of non-local maintenance and diagnostic tools only as consistent with organizational policy and documented in the Security Plan for the information system; c. Employs strong authenticators in the establishment of non-local maintenance and diagnostic sessions; d. Maintains records for non-local maintenance and diagnostic activities; and e. Terminates session and network connections when non-local maintenance is completed. Security Baseline: Low, Moderate, and High
E-2: The organization documents in the Security Plan for the information system, the policies and procedures for the establishment and use of non-local maintenance and diagnostic connections. Security Baseline: Moderate, and High
E-3: The organization: a. Requires that non-local maintenance and diagnostic services be performed from an information system that implements a security capability comparable to the capability implemented on the system being serviced; or b. Removes the component to be serviced from the information system and prior to non-local maintenance or diagnostic services, sanitizes the component (with regard to organizational information) before removal from organizational facilities, and after the service is performed, inspects and sanitizes the component (with regard to potentially malicious software) before reconnecting the component to the information system. Security Baseline: High

NIST SP 800-53 Control: MA-4
HUD Policy: 4.6.4 The CIO or designated agent ensures that: a. The appropriate organizational officials approve, control, and monitor remotely executed maintenance and diagnostic activities. b. All sessions are terminated when remote maintenance is completed. c. If password-based authentication is used, the passwords are changed following each maintenance service. d. For high-impact systems, the CIO or designated agent ensures that: • Remote diagnostic or maintenance services are performed by a service or organization that implements for its own information system the same level of security as that implemented on the information system being serviced. • The system being serviced is sanitized and physically separated from other information systems prior to the connection of the remote access line, if remote diagnostic or maintenance services are required from a service or organization that does not implement security controls at the same level of security as that implemented on the system being serviced. If the information system cannot be sanitized (e.g., due to a system failure), remote maintenance is not allowed. • Records for such activities are maintained and periodically reviewed. e. Program Offices/System Owners of high-impact systems addresses the installation and use of remote diagnostic links in the System Security Plan.

4.6.5. Maintenance Personnel

Since maintenance personnel are making modifications to the system or system components, the opportunity for accidental or intentional compromises or mistakes exists.

NIST SP 800-53 Control: MA-5
MA-5: The organization: a. Establishes a process for maintenance personnel authorization and maintains a list of authorized maintenance organizations or personnel; b. Ensures that non-escorted personnel performing maintenance on the information system have required access authorizations; and c. Designates organizational personnel with required access authorizations and technical competence to supervise the maintenance activities of personnel who do not possess the required access authorizations. Security Baseline: Low, Moderate, and High
E-1: The organization: a. Implements procedures for the use of maintenance personnel that lack appropriate security clearances or are not U.S. citizens, that include the following requirements: 1. Maintenance personnel who do not have needed access authorizations, clearances, or formal access approvals are escorted and supervised during the performance of maintenance and diagnostic activities on the information system by approved organizational personnel who are fully cleared, have appropriate access authorizations, and are technically qualified; and 2. Prior to initiating maintenance or diagnostic activities by personnel who do not have needed access authorizations, clearances or formal access approvals, all volatile information storage components within the information system are sanitized and all non-volatile storage media are removed or physically disconnected from the system and secured. b. Develops and implements alternate security safeguards in the event an information system component cannot be sanitized, removed, or disconnected from the system. Security Baseline: High

NIST SP 800-53 Control: MA-5
HUD Policy: 4.6.5 a. The CIO or designated agent ensures that only authorized individuals perform maintenance on information systems. If maintenance personnel need access to organizational information, they must be supervised by organizational personnel with authorized access to such information.

4.6.6. Timely Maintenance

If a system or system component is critical for the system to remain available, HUD must ensure that maintenance can be performed within a pre-determined and agreed time in order to avoid a greater interruption to the business functions that the system supports.

NIST SP 800-53 Control: MA-6
MA-6: The organization obtains maintenance support and/or spare parts for [*Assignment: organization-defined information system components*] within [*Assignment: organization-defined time period*] of failure. Security Baseline: Moderate and High
HUD Policy: 4.6.6 a. The Program Offices/System Owners identifies critical components that support their moderate- or high-impact systems that are hosted on infrastructure services provided platforms and works with the Deputy CIO for IOO to ensure that maintenance support and parts are provided within 48 hours of failure. b. For information systems not hosted on the infrastructure platform, the Program Offices/System Owners identifies critical components that support their moderate- or high-impact systems that are hosted on infrastructure services provided platforms and ensures that maintenance support and parts are provided within 48 hours of failure.

4.7. 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.

4.7.1. System and Information Integrity Policy and Procedures

NIST SP 800-53 Control: SI-1
SI-1: The organization: a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]: 1. A system and Information Integrity Policy that addresses the purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the system and Information Integrity Policy and associated system and information integrity controls. b. Reviews and updates the current: 1. System and Information Integrity Policy [Assignment: organization-defined frequency]; and 2. System and information integrity procedures [Assignment: organization-defined frequency]. Security Baseline: Low, Moderate, and High
Implementation
This control is implemented by the *Information Technology Security Policy, Handbook 2400.25 Rev. 4,* that defines HUD's formal security policies and the HUD *Information Technology Security Procedures* that defines HUD's formal security procedures. HUD reviews the policies and procedures minimally every year or when impacted by a significant change or underlying standard. The HUD security policies and procedures are disseminated via the HUD Intranet for all HUD's users to access.

4.7.2. Flaw Remediation

Flaws in information systems provide an opportunity for systems to be compromised, therefore, flaws particularly those related to security, must be remediated. Flaw remediation must follow the configuration management process.

NIST SP 800-53 Control: SI-2
SI-2: The organization: a. Identifies, reports, and corrects information system flaws; b. Tests software and firmware updates related to flaw remediation for effectiveness and potential side effects before installation; c. Installs security-relevant software and firmware updates within [Assignment: organization-defined time period] of the release of the updates; and d. Incorporates flaw remediation into the organizational configuration management process. Security Baseline: Low, Moderate, and High
E-1: The organization centrally manages the flaw remediation process. Security Baseline: High
E-2: The organization employs automated mechanisms [Assignment: organization-defined frequency] to determine the state of information system components with regard to flaw remediation. Security Baseline: Moderate and High

NIST SP 800-53 Control: SI-2
HUD Policy: 4.7.2 The OCIO: a. Establishes and maintains a flaw remediation program for HUD's network infrastructure, testing patches, service packs, and hot fixes for effectiveness and potential side effects prior to installation in accordance with NIST SP 800-40, *Procedures for Handling Security Patches.* b. For moderate- and high-impact systems, the Program Offices/System Owners use automated mechanisms to manage and install updates and to determine monthly, and upon demand, the state of information system components with regard to flaw remediation. c. Ensures Program Offices/System Owners manage software changes and updates for HUD mission/business applications in accordance with the Software Configuration Management Policy Handbook, 3252.1, which establishes and maintains integrity of software products throughout a project's software life-cycle.

4.7.3. Malicious Code Protection

Software is vulnerable to malicious code so it is essential that HUD provide protection against malicious code and ensure that mechanisms and tools are in place to assist in this protection.

NIST SP 800-53 Control: SI-3
SI-3: The organization: a. Employs malicious code protection mechanisms at information system entry and exit points to detect and eradicate malicious code; b. Updates malicious code protection mechanisms whenever new releases are available in accordance with organizational configuration management policy and procedures; c. Configures malicious code protection mechanisms to: 1. Perform periodic scans of the information system [Assignment: organization-defined frequency] and real-time scans of files from external sources at [Selection (one or more); endpoint; network entry/exit points] as the files are downloaded, opened, or executed in accordance with organizational security policy; and 2. [Selection (one or more): block malicious code; quarantine malicious code; send alert to administrator; [Assignment: organization-defined action]] in response to malicious code detection. d. Addresses the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the information system. 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

NIST SP 800-53 Control: SI-3
HUD Policy: 4.7.3 a. The Deputy CIO for IOO implements a defense-in-depth strategy for systems hosted on the infrastructure services platform that: • Installs and centrally manages antivirus software at each critical information entry point (e.g., firewalls, email servers, and remote-access servers) and at each workstation, server, and mobile computing device. The software shall be configured to check all files automatically on access, downloads, and email. • Installs updates to antivirus software and signature files at each critical information entry point (e.g., firewalls, email servers, and remote-access servers) and at each workstation, server, and mobile computing device promptly without requiring that end users specifically request the update. • Configures the software to prevent users from disabling or modifying configuration settings. • Installs security patches to servers and desktops promptly. • Automatically forwards alerts generated by anti-virus software to HUD's intrusion detection system. b. The Deputy CIO for IOO implements appropriate file/protocol/content filtering to protect data and networks against malicious code in accordance with HUD's Internet Usage Policy. c. For information systems not hosted on the infrastructure platform, the Program Office System Owner implements a defense-in-depth strategy for systems hosted on the infrastructure services platform that: • Installs and centrally manages antivirus software at each critical information entry point (e.g., firewalls, email servers, and remote-access servers) and at each workstation, server, and mobile computing device. The software shall be configured to check all files automatically on access, downloads, and email. • Installs updates to antivirus software and signature files at each critical information entry point (e.g., firewalls, email servers, and remote-access servers) and at each workstation, server, and mobile computing device promptly without requiring that end users specifically request the update. • Configures the software to prevent users from disabling or modifying configuration settings. • Installs security patches to servers and desktops promptly. • Automatically forwards alerts generated by anti-virus software to HUD's intrusion detection system. d. For information systems not hosted on the infrastructure platform, the Program Office System Owner implements appropriate file/protocol/content filtering to protect data and networks against malicious code in accordance with HUD's Internet Usage Policy.

4.7.4. Information System Monitoring

Because of the number of attempted attacks against information systems and the amount of data produced as a result of an event, the use of monitoring tools and techniques is important in the detection, containment and analysis of attacks.

NIST SP 800-53 Control: SI-4

SI-4: The organization:

a. Monitors the information system to detect:
   1. Attacks and indicators of potential attacks in accordance with [Assignment: organization-defined monitoring objectives]; and
   2. Unauthorized local, network, and remote connections.
b. Identifies unauthorized use of the information system through [Assignment: organization-defined techniques and methods];
c. Deploys monitoring devices: (i) strategically within the information system to collect organization-determined essential information; and (ii) at ad hoc locations within the system to track specific types of transactions of interest to the organization;
d. Protects information obtained from intrusion-monitoring tools from unauthorized access, modification, and deletion;
e. Heightens the level of information system monitoring activity whenever there is an indication of increased risk to organizational operations and assets, individuals, other organizations, or the Nation based on law enforcement information, intelligence information, or other credible sources of information;
f. Obtains legal opinion with regard to information system monitoring activities in accordance with applicable federal laws, Executive Orders, Directives, policies, or regulations; and
g. Provides [Assignment: organization-defined information system monitoring information] to [Assignment: organization-defined personnel or roles] [Selection (one or more): as needed; [Assignment: organization-defined frequency]].

Security Baseline: Moderate and High

E-2: The organization employs automated tools to support near real-time analysis of events.

Security Baseline: Moderate and High

E-4: The information system monitors inbound and outbound communications traffic [Assignment: organization-defined frequency] for unusual or unauthorized activities or conditions.

Security Baseline: Moderate and High

E-5: The information system alerts [Assignment: organization-defined personnel or roles] when the following indications of compromise or potential compromise occur: [Assignment: organization-defined compromise indicators].

Security Baseline: Moderate and High

HUD Policy: 4.7.4

a. The Deputy CIO for IOO ensures the HUD network infrastructure is monitored for information system attacks and unauthorized access and use. The Monitoring Program consists of monitoring devices deployed within the Departmental network boundaries, at the network infrastructure perimeter, and external devices managed by the US Computer Emergency Readiness Team (US-CERT). The Program monitors inbound and outbound communications and provides near-real-time alerts based on intrusion detection system (IDS) signatures maintained by the IDS manufacturer and threat analyses conducted by US CERT. Monitoring activity is heightened whenever there is an indication of increased risk to organizational operations and assets.
b. The Deputy CIO for IOO ensures that unprivileged users may not circumvent network infrastructure intrusion detection and prevent capabilities.
c. The OCIO ensures coordination with the legal, enforcement and oversight on all matters related to information system monitoring activities.
d. For high-impact systems, the information system provides a real time alert when the following events occur:
   - Access to selected privileged files of applications; and
   - Activities inconsistent with the user's profile or pattern of use.

4.7.5. Security Alerts, Advisories and Directives

External security alerts and advisories provide information to personnel prior to an incident, providing a possible opportunity to correct system vulnerabilities that might potentiality compromise a system.

NIST SP 800-53 Control: SI-5
SI-5: The organization: a. Receives information system security alerts, advisories, and directives from [Assignment: organization-defined external organizations] on an ongoing basis; b. Generates internal security alerts, advisories, and directives as deemed necessary; c. Disseminates security alerts, advisories, and directives to: [Selection (one or more): [Assignment: organization-defined personnel or roles]; [Assignment: organization-defined elements within the organization]; [Assignment: organization-defined external organizations]]; and d. Implements security directives in accordance with established time frames, or notifies the issuing organization of the degree of noncompliance. Security Baseline: Low, Moderate, and High
E-1: The organization employs automated mechanisms to make security alert and advisory information available throughout the organization. Security Baseline: High
HUD Policy: 4.7.5 a. The OCIO ensures the establishment and maintenance of a Program to receive, analyze applicability, and provide targeted security alerts to pertinent personnel within the Department and with applicable external stakeholders. This Program relies on advisories and alerts from the US Computer Emergency Readiness Team (US-CERT) and vendors for the hardware and software products implemented on the HUD network. b. This Program disseminates information on current risks, threats, attacks, exploits, and corresponding mitigation strategies through alerts and advisories. c. The HUD Computer Incident Response Team (HUD-CIRT) maintains a central repository of security alerts and advisories applicable to the Department including status of remediation activities. d. Program Offices/System Owners of moderate- or high-impact systems shall ensure that security alerts, advisories, Intrusion Detection System (IDS) alerts, and vulnerabilities identified during vulnerability scans and penetration tests are tracked and responded to as security incidents.

4.7.6. Security Functionality Verification

The system security functions are essential in the protection of information assets, consequently, it is important that these functions execute appropriately and should be verified during system startup and restart.

NIST SP 800-53 Control: SI-6
SI-6. The information system: a. Verifies the correct operation of [Assignment: organization-defined security functions]; b. Performs this verification [Selection (one or more): [Assignment: organization-defined system transitional states]; upon command by user with appropriate privilege; [Assignment: organization-defined frequency]]; c. Notifies [Assignment: organization-defined personnel or roles] of failed security verification tests; and d. [Selection (one or more): shuts the information system down; restarts the information system; [Assignment: organization-defined alternative action(s)]] when anomalies are discovered. Security Baseline: High
HUD Policy: 4.7.6 a. The Program Offices/System Owners ensures security functions for which automated self-tests can be executed, the information system verifies the correct operation of the security function at system startup and restart, and restarts the system when anomalies are discovered.

4.7.7. Software, Firmware, and Information Integrity

Software and Information Integrity refers to the processes and procedures used to control changes and maintain the integrity of the components for any system, including hardware and software. HUD's processes and procedures identify the configuration of software at a given point in time, control changes to configurations systematically, maintain software integrity, provide traceability, and establish a software baseline library. This minimizes and manages risks in developing and maintaining software.

NIST SP 800-53 Control: SI-7
SI-7: The organization employs integrity verification tools to detect unauthorized changes to [*Assignment: organization-defined software, firmware, and information*]. Security Baseline: Moderate and High
E-1: The information system performs an integrity check of [Assignment: organization-defined software, firmware, and information] [Selection (one or more): at startup; at [Assignment: organization-defined transitional states or security-relevant events]; [Assignment: organization-defined frequency]]. Security Baseline: Moderate and High
E-2: The organization employs automated tools that provide notification to [Assignment: organization-defined personnel or roles] upon discovering discrepancies during integrity verification. Security Baseline: High
E-5: The information system automatically [Selection (one or more): shuts the information system down; restarts the information system; implements [Assignment: organization-defined security safeguards]] when integrity violations are discovered. Security Baseline: High
E-7: The organization incorporates the detection of unauthorized [Assignment: organization-defined security-relevant changes to the information system] into the organizational incident response capability. Security Baseline: Moderate and High

NIST SP 800-53 Control: SI-7
E-14: The organization: a. Prohibits the use of binary or machine-executable code from sources with limited or no warranty and without the provision of source code; and b. Provides exceptions to the source code requirement only for compelling mission/operational requirements and with the approval of the authorizing official. Security Baseline: High
HUD Policy: 4.7.7 a. The OCIO ensures the establishment and maintenance of a software configuration management program that ensures the Departmental information and information systems are protected against unauthorized changes. The Program shall ensure software undergoes integrity assessments prior to initial deployment into production and periodically thereafter, but no less frequently than annually.

4.7.8. Spam Protection

Spam presents another mechanism to introduce vulnerabilities into a system. Spam is the use of electronic messaging systems to send unsolicited bulk messages, especially advertising, indiscriminately. Too often, vulnerabilities may be embedded in the spam in the form of executable programs, references to Internet addresses where malicious programs might be downloaded, or requests for personnel data from the recipient. The recipient may or may not know how to respond to spam which introduces additional vulnerabilities to the system.

NIST SP 800-53 Control: SI-8
SI-8: The organization: a. Employs spam protection mechanisms at information system entry and exit points to detect and take action on unsolicited messages; and b. Updates spam protection mechanisms when new releases are available in accordance with organizational configuration management policy and procedures. Security Baseline: Moderate and High
E-1: The organization centrally manages spam protection mechanisms. Security Baseline: Moderate and High
E-2: The information system automatically updates spam protection mechanisms. Security Baseline: Moderate and High
HUD Policy: 4.7.8 a. The Deputy CIO for IOO installs and centrally manages spam and spyware protection mechanisms at each critical information entry point (e.g., firewalls, email servers, and remote-access servers) and at workstations, servers, and mobile computing devices connected to the network. The mechanism shall have the capability for automatic updates. b. The Deputy CIO for IOO updates spam protection mechanisms (including signature definitions) when new releases are available in accordance with organizational configuration management policy and procedures.

4.7.9. Information Input Validation

Information systems are only legitimate if the information in the system is accurate, complete and has not been compromised.

NIST SP 800-53 Control: SI-10
SI-10: The information system checks the validity of [Assignment: organization-defined information inputs]. Security Baseline: Moderate and High
HUD Policy: 4.7.9 a. For moderate- or high impact systems, the Program Offices/System Owners ensure that the information system checks information inputs for accuracy, completeness, and validity. Valid syntax and semantics of information system inputs (e.g., character set, length, numerical range, acceptable values).

4.7.10. Error Handling

Information systems must identify and handle errors by only providing the necessary information required to handle the error, limiting the information that could be used to possibly compromise the system.

NIST SP 800-53 Control: SI-11
SI-11. The information system: a. Generates error messages that provide information necessary for corrective actions without revealing information that could be exploited by adversaries; and b. Reveals error messages only to [Assignment: organization-defined personnel or roles]. Security Baseline: Moderate and High
HUD Policy: 4.7.10 a. For moderate- or high-impact systems, the Program Offices/System Owners ensure the information system identifies and handles error conditions in an expeditious manner. b. Program Offices/System Owners ensure the information system generates error messages that provide information necessary for corrective actions without revealing sensitive information in error logs and administrative messages that could be exploited by adversaries. c. Program Offices/System Owners ensure the information system reveals error messages only to authorized personnel.

4.7.11. Information Handling and Retention

Information system outputs (i.e., reports, files) could be used to compromise the system or expose information that should be protected.

NIST SP 800-53 Control: SI-12
SI-12: The organization handles and retains information within the information system and information output from the system in accordance with applicable federal laws, Executive Orders, Directives, policies, regulations, standards, and operational requirements. Security Baseline: Low, Moderate and High
HUD Policy: 4.7.11 a. Program Offices/System Owners handle and retain information system output, both paper and digital, in accordance with federal laws and regulations, HUD policy, and organizational responsibilities.

4.8. 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. This policy 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.

4.8.1. Media Protection Policy and Procedures

The Media Protection Policy and procedures must be consistent with applicable laws, Executive Orders, Directives, policies, regulations, standards, and guidance. Where applicable, the Media Protection Policy and procedures will reference related HUD documents either by the document name or number, rather than repeating the requirements herein.

NIST SP 800-53 Control: MP-1
MP-1: The organization: a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]: 1. A Media Protection Policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the media protection policy and associated media protection controls. b. Reviews and updates the current: 1. Media Protection Policy [Assignment: organization-defined frequency]; and 2. Media protection procedures [Assignment: organization-defined frequency]. Security Baseline: Low, Moderate, and High
Implementation
This control is implemented by the *Information Technology Security Policy, Handbook 2400.25 Rev. 4,* that defines HUD's formal security policies and the HUD *Information Technology Security Procedures* that defines HUD's formal security procedures. HUD reviews the policies and procedures minimally every year or when impacted by a significant change or underlying standard. The HUD security policies and procedures are disseminated via the HUD Intranet for all HUD's users to access.

4.8.2. Media Access

In order to protect and secure sensitive information, the media used to store or present the information must be protected from improper access and properly destroyed when no longer required.

NIST SP 800-53 Control: MP-2
MP-2: The organization restricts access to [*Assignment: organization-defined types of digital and/or non-digital media*] to [*Assignment: organization-defined personnel or roles*].

NIST SP 800-53 Control: MP-2
Security Baseline: Low, Moderate, and High
HUD Policy: 4.8.2 a. Program Offices/System Owners establish procedures to ensure that moderate and high sensitive information in printed form or digital media cannot be accessed, removed, or stolen by unauthorized individuals. b. HUD implements physical and logical security controls to protect systems, buildings, and related supporting infrastructures from unauthorized media access.

4.8.3. Media Marking

In order to protect the information on stored media, the media should be appropriately labeled with its sensitivity so that individuals handling the media or information understand the level of protection that must be provided.

NIST SP 800-53 Control: MP-3
MP-3: The organization: a. Marks information system media indicating the distribution limitations, handling caveats, and applicable security markings (if any) of the information; and b. Exempts [Assignment: organization-defined types of information system media] from marking as long as the media remain within [Assignment: organization-defined controlled areas]. Security Baseline: Moderate and High
HUD Policy: 4.8.3 a. Program Offices/System Owners and Users ensure that all media containing moderate and high-impact sensitive information is appropriately marked with the sensitivity of the information stored on the media. At a minimum, printed output that is not otherwise appropriately marked shall have a cover sheet and digital media shall be labeled with the distribution limitations, handling caveats, and applicable security markings, if any, of the information.

4.8.4. Media Storage

An additional level of protection of information is provided by securely storing the media based on the information's required level of protection.

NIST SP 800-53 Control: MP-4
MP-4: The organization: a. Physically controls and securely stores [Assignment: organization-defined types of digital and/or non-digital media] within [Assignment: organization-defined controlled areas]; and b. Protects information system media until the media are destroyed or sanitized using approved equipment, techniques, and procedures. Security Baseline: Moderate and High

NIST SP 800-53 Control: MP-4
HUD Policy: 4.8.4 a. Program Offices/System Owners and Users control access to and securely store all information system media (i.e., both paper and digital) containing moderate or high-impact sensitive information, including backup and removable media, in a secure location when not in use. b. For high-impact systems, media is stored in locked canisters or encrypted if the information system media is removed from the primary storage area. c. Program Offices and Users ensure that unattended laptops in offices are secured via a locking cable, locked office, or a locked cabinet or desk. d. Program Offices/System Owners maintain records certifying that such destruction was performed.

4.8.5. Media Transport

To prevent a possible compromise to information, the media storing the information must be protected during transport outside of the controlled area.

NIST SP 800-53 Control: MP-5
MP-5: The organization: a. Protects and controls [Assignment: organization-defined types of information system media] during transport outside of controlled areas using [Assignment: organization-defined security safeguards]; b. Maintains accountability for information system media during transport outside of controlled areas; c. Documents activities associated with the transport of information system media; and d. Restricts the activities associated with the transport of information system media to authorized personnel. Security Baseline: Moderate and High
E-4: The information system implements cryptographic mechanisms to protect the confidentiality and integrity of information stored on digital media during transport outside of controlled areas. Security Baseline: Moderate and High
HUD Policy: 4.8.5 a. Program Offices/System Owners establish procedures to ensure that sensitive information in printed form or digital media can only be picked up, received, transferred, or delivered to authorized individuals. b. Program Offices/System Owners maintain records documenting any transportation of sensitive printed or digital media.

4.8.6. Media Sanitization

When media is disposed of, it is necessary to properly sanitize the media to prevent compromising the data by destroying the data or destroying the media.

NIST SP 800-53 Control: MP-6
MP-6: The organization: a. Sanitizes [Assignment: organization-defined information system media] prior to disposal, release out of organizational control, or release for reuse using [Assignment: organization-defined sanitization techniques and procedures] in accordance with applicable federal and organizational standards and policies; and b. Employs sanitization mechanisms with the strength and integrity commensurate with the security category or classification of the information. Security Baseline: Low, Moderate, and High
E-1: The organization reviews, approves, tracks, documents, and verifies media sanitization and disposal actions. Security Baseline: High
E-2: The organization tests sanitization equipment and procedures [Assignment: organization-defined frequency] to verify that the intended sanitization is being achieved. Security Baseline: High
E-3: The organization applies nondestructive sanitization techniques to portable storage devices prior to connecting such devices to the information system under the following circumstances: [Assignment: organization-defined circumstances requiring sanitization of portable storage devices]. Security Baseline: High
HUD Policy: 4.8.6 a. Program Offices/System Owners shall ensure that any sensitive information stored on media surplus or returned to the manufacturer shall be purged from the media before disposal. b. Disposal shall be performed following the guidance in NIST SP 800-88, *Guidelines for Media Sanitation.* c. Program Offices/System Owners shall maintain records certifying that such sanitization was performed. d. Program Offices/System Owners shall ensure that sensitive information is purged from the hard drives of any workstation or server returned to the equipment surplus pool or transferred to another individual. e. Program Offices/System Owners shall ensure that media (e.g., paper, diskettes, and removable disk drives) containing sensitive information is destroyed in such a manner that all sensitive information on that media cannot be recovered by ordinary means. Examples of appropriate methods are crosscut shredders, degaussing, and approved disk-wiping software.

4.8.7. Media Use

When media is disposed of, it is necessary to properly sanitize the media to prevent compromising the data by destroying the data or destroying the media.

NIST SP 800-53 Control: MP-7
MP-6: The organization [Selection: restricts; prohibits] the use of [Assignment: organization-defined types of information system media] on [Assignment: organization-defined information systems or system components] using [Assignment: organization-defined security safeguards]. Security Baseline: Low, Moderate, and High
E-1: The organization prohibits the use of portable storage devices in organizational information systems when such devices have no identifiable owner. Security Baseline: High

NIST SP 800-53 Control: MP-7
HUD Policy: 4.8.7 a. Program Offices/System Owners ensure that any sensitive information stored on media surplus or returned to the manufacturer is purged from the media before disposal. b. Disposal shall be performed following the guidance in NIST SP 800-88, *Guidelines for Media Sanitation.* c. Program Offices/System Owners maintain records certifying that such sanitization was performed. d. Program Offices/System Owners ensure that sensitive information is purged from the hard drives of any workstation or server returned to the equipment surplus pool or transferred to another individual. e. Program Offices/System Owners ensure that media (e.g., paper, diskettes, and removable disk drives) containing sensitive information is destroyed in such a manner that all sensitive information on that media cannot be recovered by ordinary means. Examples of appropriate methods are crosscut shredders, degaussing, and approved disk-wiping software.

4.9. 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. These incidents can severely disrupt computer-supported operations, compromise the confidentiality of sensitive information, and diminish the integrity of critical data. To help combat the disruptive short- and long-term effects of security incidents, each government agency is required to implement and maintain a security incident reporting and handling capability.

The following policies describe the mechanisms that must be 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.

4.9.1. Incident Response Policy and Procedures

The Incident Response Policy and procedures must be consistent with applicable laws, Executive Orders, Directives, policies, regulations, standards, and guidance. Where applicable, the Incident Response Policy and procedures will refer to the references by the associated reference description or number, so that these policies are not repeating the reference.

NIST SP 800-53 Control: IR-1
IR-1: The organization: a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]: 1. An Incident Response Policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the incident response policy and associated incident response controls. b. Reviews and updates the current: 1. Incident Response Policy [Assignment: organization-defined frequency]; and 2. Incident response procedures [Assignment: organization-defined frequency]. Security Baseline: Low, Moderate and High
Implementation
This control is implemented by the *Information Technology Security Policy, Handbook 2400.25 Rev. 4,* that defines HUD's formal security policies and the HUD *Information Technology Security Procedures* that defines HUD's formal security procedures. HUD reviews the policies and procedures minimally every year or when impacted by a significant change or underlying standard. The HUD security policies and procedures are disseminated via the HUD Intranet for all HUD's users to access.

4.9.2. Incident Response Training

Quickly responding to incidents provides a mechanism for controlling the impact of the incident on the information system; therefore, individuals must understand their incident response responsibilities and the actions they should take if an incident is suspected or occurred. To accomplish this, individuals require training in incident detection and response. The following policy addresses the requirement for all personnel involved in incident response activities to receive training in incident response procedures.

NIST SP 800-53 Control: IR-2
IR-2: The organization provides incident response training to information system users consistent with assigned roles and responsibilities: a. Within [Assignment: organization-defined time period] of assuming an incident response role or responsibility; b. When required by information system changes; and c. [Assignment: organization-defined frequency] thereafter. Security Baseline: Low, 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 incident response training environment. Security Baseline: High
HUD Policy: 4.9.2 a. Program Offices/System Owners ensure that personnel with incident response responsibilities receive training at least once a year. b. For high-impact systems, incident response training incorporates simulated events to facilitate effective response by personnel in a crisis and employ automated mechanisms.

4.9.3. Incident Response Testing

To determine the effectiveness and weaknesses of HUD's incident response capability and to improve on that capability requires that tests and exercises be performed in a controlled manner and the results analyzed.

NIST SP 800-53 Control: IR-3
IR-3: The organization tests the incident response capability for the information system [*Assignment: organization-defined frequency*] using [*Assignment: organization-defined tests*] to determine the incident response effectiveness and documents the results. Security Baseline: Moderate and High
E-1: The organization coordinates incident response testing with organizational elements responsible for related plans. Security Baseline: Moderate and High
HUD Policy: 4.9.3 a. Incident Response is a common control owned by OCIO. b. The OCIO tests the Department's incident response capability once a year and documents the test results. c. For high-impact systems the tests employ automated mechanisms.

4.9.4. Incident Handling

The HUD Computer Incident Response Team (HUD-CIRT) is the focal point for the implementation of HUD's incident response capability and requires participation by all Program Offices/System Owners. In order to protect information assets, HUD's security incident handling capability must provide the necessary steps for security incident detection and resolution. The following policy provides guidance for implementing an incident handling capability.

NIST SP 800-53 Control: IR-4
IR-4: The organization: a. Implements an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery; b. Coordinates incident handling activities with contingency planning activities; and c. Incorporates lessons learned from ongoing incident handling activities into incident response procedures, training, and testing/exercises, and implements the resulting changes accordingly. Security Baseline: Low, Moderate, and High
E-1: The organization employs automated mechanisms to support the incident handling process. Security Baseline: Moderate and High
E-4: The organization correlates incident information and individual incident responses to achieve an organization-wide perspective on incident awareness and response. Security Baseline: High
HUD Policy: 4.9.4 a. The OCIO establishes and maintains an incident response capability to prevent, detect, track, and respond to

NIST SP 800-53 Control: IR-4
information security incidents and alerts in accordance with NIST SP 800-61, *Computer Security Incident Handling Guide*. Lessons learned from ongoing incident handling activities are incorporated into the incident response training, procedures and implemented accordingly. b. For moderate- or high-impact systems, the OCIO provides automated mechanisms to support the incident handling process.

4.9.5. Incident Monitoring

In order to protect the information systems, it is necessary to monitor for incidents, as information assets are susceptible at any time to either intentional or unintentional damaging incidents. The following policy addresses the requirement that the organization utilizes mechanisms to monitor security incidents.

NIST SP 800-53 Control: IR-5
IR-5 The organization tracks and documents information system security incidents. Security Baseline: Low, 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
HUD Policy: 4.9.5 a. The OCIO ensures that the HUD-CIRT has a process to track and document information system security incidents on an ongoing basis. b. For high-impact systems, the tracking of security incidents and the collection and analysis of incident information employs automated mechanisms.

4.9.6. Incident Reporting

The timely reporting of incidents or suspected incidents assists in the incident containment, impact and mitigation. This includes reporting incidents dealing with Personally Identifiable Information (PII). A PII incident involves suspected and confirmed breaches in the protection of personally identifiable information in electronic or physical form.

The following policy addresses the requirement that organizations report security related incidents to the appropriate entities.

NIST SP 800-53 Control: IR-6
IR-6: The organization: a. Requires personnel to report suspected security incidents to the organizational incident response capability within [Assignment: organization-defined time period]; and b. Reports security incident information to [Assignment: organization-defined 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

NIST SP 800-53 Control: IR-6
HUD Policy: 4.9.6 a. All users of HUD information technology assets report computer security incidents to the HUD IT service provider immediately upon validation that an incident has occurred. b. The OCIO ensures that computer security incidents reported to the HUD IT service provider function are reported to the HUD-CIRT in accordance with established reporting time frames. c. The HUD-CIRT reports computer security incidents to appropriate authorities, including the United States Computer Emergency Readiness Team (US-CERT), in accordance with Federal incident reporting guidelines. d. For moderate- or high-impact systems, the HUD-CIRT uses automated mechanisms to assist in the reporting of security incidents. e. HUD-CIRT is responsible for providing OITS incident-related information for the Department's FISMA reports.

4.9.7. Incident Response Assistance

Since the handling of security incidents is not a primary duty of information system users, system users should have resources available to them to assist in responding to incidents from staff whose responsibilities include security incident response.

The following policy addresses the requirement to provide users with a source for incident support.

NIST SP 800-53 Control: IR-7
IR-7: The organization provides an incident response support resource, integral to the organizational incident response capability that offers advice and assistance to users of the information system for the handling and reporting of security incidents. Security Baseline: Low, Moderate, and High
E-1: The organization employs automated mechanisms to increase the availability of incident response-related information and support. Security Baseline: Moderate, and High
HUD Policy: 4.9.7 a. The HUD-CIRT provides all HUD's users with guidance and assistance (e.g., help desk) for handling and reporting of security incidents. b. For moderate- or high-impact systems, the HUD-CIRT employs automated mechanisms to increase the availability of incident response-related information and support.

4.9.8. Incident Response Plan

The following policy addresses the requirement for the Department to have an Incident Response Plan for incident support.

NIST SP 800-53 Control: IR-8
IR-8: The organization a. Develops an Incident Response Plan that: 1. Provides the organization with a roadmap for implementing its incident response capability; 2. Describes the structure and organization of the incident response capability; 3. Provides a high-level approach for how the incident response capability fits into the overall organization; 4. Meets the unique requirements of the organization, which relate to mission, size, structure, and functions; 5. Defines reportable incidents; 6. Provides metrics for measuring the incident response capability within the organization; 7. Defines the resources and management support needed to effectively maintain and mature an incident response capability; and b. Is reviewed and approved by [Assignment: organization-defined personnel or roles]; c. Distributes copies of the incident response plan to [Assignment: organization-defined incident response personnel (identified by name and/or by role) and organizational elements]; d. Reviews the Incident Response Plan [Assignment: organization-defined frequency]; e. Updates the Incident Response Plan to address system/organizational changes or problems encountered during plan implementation, execution, or testing; f. Communicates the Incident Response Plan changes to [Assignment: organization-defined incident response personnel (identified by name and/or by role) and organizational elements]; and g. Protects the Incident Response Plan from unauthorized disclosure and modification. Security Baseline: Low, Moderate, and High
HUD Policy: 4.9.8 a. The OCIO ensures that the HUD-CIRT develops and maintains the HUD's Incident Response Plan as part of the OCIO's responsibility as the common control provider for the Department. b. The OCIO ensures the Plan is distributed upon request, and on an as-needed basis, to incident response personnel. The HUD-CIRT maintains the list of incident response personnel. c. The OCIO ensures the HUD's Incident Response Plan is kept current and revised to address system/organizational changes or problems. At a minimum, the Plan is reviewed annually.

4.10. Awareness and Training

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

Each organization is required to make general users and personnel with significant security responsibilities for a system 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 specialized security training for personnel who have been designated as having significant security responsibilities.

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.

4.10.1. Security Awareness and Training Policy and Procedures

The Security Awareness and Training Policy and procedures must be consistent with applicable laws, Executive Orders, Directives, policies, regulations, standards, and guidance.

NIST SP 800-53 Control: AT-1
AT-1: The organization: a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]: 1. A Security Awareness and Training Policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the Security Awareness and Training Policy and associated security awareness and training controls; and b. Reviews and updates the current: 3. Security Awareness and Training Policy [Assignment: organization-defined frequency]; and 4. Security awareness and training procedures [Assignment: organization-defined frequency]. Security Baseline: Low, Moderate, and High
Implementation
This control is implemented by the *Information Technology Security Policy, Handbook 2400.25 Rev. 4,* that defines HUD's formal security policies and the HUD *Information Technology Security Procedures* that defines HUD's formal security procedures. HUD reviews the policies and procedures minimally every year or when impacted by a significant change or underlying standard. The HUD security policies and procedures are disseminated via the HUD Intranet for all HUD's users to access.

4.10.2. Security Awareness Training

All users with access to the Department's information have a responsibility to safeguard that information. The Department must ensure that users and personnel with significant security responsibilities for an IT system are aware of the security risks associated with their access to and use of Departmental information and management of IT systems. This control family ensures that users of Departmental information receive security awareness training, that personnel with significant security responsibilities receive specialized security training, and that all training is tracked.

NIST SP 800-53 Control: AT-2
AT-2: The organization provides basic security awareness training to information system users (including managers, senior executives, and contractors): a. As part of initial training for new users; b. When required by information system changes; and c. [Assignment: organization-defined frequency] thereafter. Security Baseline: Low, Moderate, and High
HUD Policy: 4.10.2 a. The OITS establishes an Information Security Awareness and Training Program in accordance with NIST 800 SP 800-50, *Building an Information Technology Security Awareness and Training Program*. The Program shall be consistent with CFR Part 5 Subpart C (5 CFR 930.301). b. Program Offices/System Owners ensure that HUD personnel and contractors accessing HUD information systems receive initial training in security awareness and accepted security practices as part of their orientation or when required by system changes. They shall sign the Rules of Behavior and receive refresher training by the determined date established by OMB to meet the FISMA legislation requirement for federal agencies. c. Unless a waiver is granted by the CISO, user accounts and access privileges, including access to email, will be disabled for those HUD employees and contractors who have not received annual refresher training.

4.10.3. Role-based Security Training

Individuals with responsibilities directly related to securing information assets must maintain the skills necessary to identify vulnerabilities, identify security incidents, implement security solutions to mitigate vulnerabilities, and ensure the security of information assets. This control requires that personnel assigned significant security responsibilities receive specialized security training.

NIST SP 800-53 Control: AT-3
AT-3: The organization provides Role-based Security Training to personnel with assigned security roles and responsibilities: a. Before authorizing access to the information system or performing assigned duties; b. When required by information system changes; and c. [Assignment: organization-defined frequency] thereafter. Security Baseline: Low, Moderate, and High
HUD Policy: 4.10.3 a. The OITS identify roles and responsibilities in HUD that must receive annual specialized security training. b. Program Offices/System Owners ensure that HUD personnel and contractors with significant security responsibilities (e.g., ISSOs and system administrators) receive annual specialized training specific to their security responsibilities. Training may be required more frequently due to system changes. The level of training shall be commensurate with the individual's duties and responsibilities and promote a consistent understanding of the principles and concepts of information system security. c. Program Offices/System Owners establish additional system-specific security training requirements when necessary. d. Unless a waiver is granted by the CISO, user accounts and access privileges, including access to email, will be disabled for those HUD employees who have not received annual refresher training.

4.10.4. Security Training Records

Security training records must be maintained and used as a mechanism for monitoring the status of security training.

NIST SP 800-53 Control: AT-4
AT-4: The organization: a. Documents and monitors individual information system security training activities including basic security awareness training and specific information system security training; and b. Retains individual training records for a period of [Assignment: organization-defined]. Security Baseline: Low, Moderate, and High
HUD Policy: 4.10.4 a. Program Offices retain training records that include the individual names and positions, types of training received, and cost of training for a period of 5 years. b. Program Offices prepare and submit awareness and training statistics to the OITS. These statistics shall include the (1) total number of personnel and the total number of personnel who received awareness training, and (2) total number of information security personnel with significant security responsibilities and the total number who were trained.

5.0 TECHNICAL POLICIES

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.

5.1. Identification and Authentication

Authentication is the process of establishing confidence in user identities electronically presented to an information system. Individual authentication is the process of establishing an understood level of confidence that an identifier refers to a specific individual. Authentication focuses on confirming an individual's identity, based on the reliability of the individual's credentials. Authentication of user identities is accomplished using passwords, tokens, PKI certificates, key cards, biometrics, or in the case of multifactor authentication, some combination therein.

The following policies ensure 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

The following policy addresses the requirement to develop policy and procedures for identification and authentication.

NIST SP 800-53 Control: IA-1
IA-1: The organization: a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]: 1. An Identification and Authentication Policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the Identification and Authentication Policy and associated identification and authentication controls. b. Reviews and updates the current: 1. Identification and Authentication Policy [Assignment: organization-defined frequency]; and 2. Identification and authentication procedures [Assignment: organization-defined frequency]. Security Baseline: Low, Moderate, and High
Implementation
This control is implemented by the *Information Technology Security Policy, Handbook 2400.25 Rev. 4,* that defines HUD's formal security policies and the HUD *Information Technology Security Procedures* that defines HUD's formal security procedures. HUD reviews the policies and procedures minimally every year or when impacted by a significant change or underlying standard. The HUD security policies and procedures are disseminated via the HUD Intranet for all HUD's users to access.

5.1.2. Identification and Authentication (Organizational Users)

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

NIST SP 800-53 Control: IA-2
IA-2: The information system uniquely identifies and authenticates organizational users (or processes acting on behalf of organizational users). Security Baseline: Low, Moderate, and High
E-1: The information system implements multi-factor authentication for network access to non-privileged accounts. Security Baseline: Low, Moderate, and High
E-2: The information system uses multi-factor authentication for network access to non-privileged accounts. Security Baseline: Moderate and High
E-3: The information system implements multi-factor authentication for local access to privileged accounts. Security Baseline: Moderate and High
E-4: The information system implements multi-factor authentication for local access to non-privileged accounts. Security Baseline: High
E-8: The information system implements replay-resistant authentication mechanisms for network access to privileged accounts. Security Baseline: Moderate and High
E-9: The information system implements replay-resistant authentication mechanisms for network access to non-privileged accounts. Security Baseline: High
E-11: The information system implements multi-factor authentication for remote access to privileged and non-privileged accounts such that one of the factors is provided by a device separate from the system gaining access and the device meets [Assignment: organization-defined strength of mechanism requirements]. Security Baseline: Moderate and High
E-12: The information system accepts and electronically verifies Personal Identity Verification (PIV) credentials. Security Baseline: Moderate and High

NIST SP 800-53 Control: IA-2
HUD Policy: 5.1.2 a. Program Offices/System Owners ensure that HUD information systems are capable of controlling and limiting user access based on positive user identification and authentication mechanisms accordance with FIPS 201 *Personal Identity Verification for Federal Employees and Contractors* and supporting NIST special publications. Moderate or high-impact systems employ multi-factor authentication mechanisms in accordance with Federal Directives and standards. b. Program Offices/System Owners ensure that privileged users authenticate to network accounts based on multi-factor authentication mechanisms. c. Moderate- or high-impact systems shall employ multi-factor authentication mechanisms for local access to privileged accounts. d. The CISO, in conjunction with the Deputy CIO for IOO, ensures that HUD's PKI can support the requirements for E-authentication in accordance with NIST SP-800-63, *Electronic Authentication Guideline: Recommendation of the National Institute of Standards and Technology.* e. The CISO, in conjunction with the Deputy CIO for IOO, ensures that HUD's PKI can support the requirements for personal identification verification in accordance with NIST FIPS 201, *Personal Identity Verification for Federal Employees and Contracts* and the supporting NIST Special Publications. f. The OCIO ensures that HUD information systems use replay-resistant authentication mechanisms including Kerberos for Windows, Secure Sockets Layer Version 3.0 (SSL 3.0), and/or Transport Layer Security Version 1.0 (TLS1.0) or higher for web-based authentication and terminal emulators for mainframes, for network access to privileged accounts. g. High-impact systems shall employ multi-factor authentication for network access to privileged accounts and shall use replay-resistant authentication mechanisms as defined above for network access to non-privileged accounts.

5.1.3. Device Identification and Authentication

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

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

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

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

The following policy provides guidance for ensuring that HUD information systems uniquely identify and authenticate devices that attempt to establish connections.

NIST SP 800-53 Control: IA-3
IA-3: The information system uniquely identifies and authenticates [Assignment: organization-defined specific and/or types of devices] before establishing a [Selection (one or more): local; remote; network] connection. Security Baseline: Moderate and High
HUD Policy: 5.1.3 a. Program Offices/System Owners use authentication procedures, mechanism, or protocol to secure authenticators used for application, host, or device authentication. The required strength of the selected authentication mechanism is determined by the FIPS security category of the information system. b. The OCIO assigns IDs and passwords, commonly called Machine IDs or X-IDs, to IT hardware and applications to facilitate data interfaces and data sharing. c. Machine IDs are only used in machine-to-machine communications where the machines are Departmental servers and enterprise database software.

5.1.4. Identifier Management

Managing identifiers involves maintaining a method for using credentials for the unique identification and authentication of users. The following policy provides guidance for the management of user identifiers.

NIST SP 800-53 Control: IA-4
IA-4: The organization manages information system identifiers by: a. Receiving authorization from [Assignment: organization-defined personnel or roles] to assign an individual, group, role, or device identifier; b. Selecting an identifier that identifies an individual, group, role, or device; c. Assigning the identifier to the intended individual, group, role, or device; d. Preventing reuse of identifiers for [Assignment: organization-defined time period]; and e. Disabling the identifier after [Assignment: organization-defined time period of inactivity]. Security Baseline: Low, Moderate, and High
HUD Policy: 5.1.4 a. Program Offices/System Owners ensure that user identifiers are implemented and maintained that support access control, least privilege, and system integrity in accordance with FIPS 201, *Personal Identity Verification for Federal Employees and Contractors* and supporting NIST Special Publications. b. HUD users shall not share identification or authentication materials of any kind; nor shall any HUD user allow any other person to operate any HUD system by employing the user's identity. c. HUD users and/or developers and contractors shall never use a Machine ID or X-ID as a surrogate mechanism for accessing HUD information systems. d. The system ISSO ensures that user IDs are disabled after a period of inactivity of no more than 90 days. For moderate- or high-impact systems, the system shall do this automatically.

5.1.5. Authenticator Management

The following policy provides guidance for the management of authenticators to include passwords. A password is a secret that a claimant memorizes and uses to authenticate the claimant's identity. Passwords are typically character strings. Strong passwords have a minimum

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

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

Multi-factor authentication is an authentication system or a token that uses more than one authentication factor. The three types of authentication factors are something you know, something you have, and something you are. Authentication requires that the Claimant prove, through a secure authentication protocol, that he or she controls the token. The Claimant unlocks the token with a password or biometric, or uses a secure multi-token authentication protocol to establish two-factor authentication (through proof of possession of a physical or software token in combination with some memorized secret knowledge). FIPS 201 and its attendant SP 800-73 and SP 800-76 specify a personal identity verification (PIV) card token for use in the unique identification and authentication of federal employees and contractors. In circumstances where Federal employees or contractors are not eligible or required to receive a PIV card, HUD relies on alternative multi-factor authentication mechanisms to ensure appropriate authentication strength and protection.

NIST SP 800-53 Control: IA-5
IA-5: The organization manages information system authenticators by: a. Verifying, as part of the initial authenticator distribution, the identity of the individual, group, role, or device receiving the authenticator; b. Establishing initial authenticator content for authenticators defined by the organization; c. Ensuring that authenticators have sufficient strength of mechanism for their intended use; d. Establishing and implementing administrative procedures for initial authenticator distribution, for lost/compromised or damaged authenticators, and for revoking authenticators; e. Changing default content of authenticators prior to information system installation; f. Establishing minimum and maximum lifetime restrictions and reuse conditions for authenticators; g. Changing/refreshing authenticators [Assignment: organization-defined time period by authenticator type]; h. Protecting authenticator content from unauthorized disclosure and modification; i. Requiring individuals to take, and having devices implement, specific security safeguards to protect authenticators; and j. Changing authenticators for group/role accounts when membership to those accounts changes. Security Baseline: Low, Moderate, and High

NIST SP 800-53 Control: IA-5
E-1: The information system, for password-based authentication: a. Enforces minimum password complexity of [Assignment: organization-defined requirements for case sensitivity, number of characters, mix of upper-case letters, lower-case letters, numbers, and special characters, including minimum requirements for each type]; b. Enforces at least the following number of changed characters when new passwords are created: [Assignment: organization-defined number]; c. Stores and transmits only cryptographically-protected passwords; d. Enforces password minimum and maximum lifetime restrictions of [Assignment: organization-defined numbers for lifetime minimum, lifetime maximum]; e. Prohibits password reuse for [Assignment: organization-defined number] generations; and f. Allows the use of a temporary password for system logons with an immediate change to a permanent password. Security Baseline: Low, Moderate, and High
E-2: The information system, for PKI-based authentication: a. Validates certifications by constructing and verifying a certification path to an accepted trust anchor including checking certificate status information; b. Enforces authorized access to the corresponding private key; c. Maps the authenticated identity to the account of the individual or group; and d. Implements a local cache of revocation data to support path discovery and validation in case of inability to access revocation information via the network. Security Baseline: Moderate and High
E-3: The organization requires that the registration process to receive [Assignment: organization-defined types of and/or specific authenticators] be conducted [Selection: in person; by a trusted third party] before [Assignment: organization-defined registration authority] with authorization by [Assignment: organization-defined personnel or roles]. Security Baseline: Moderate and High
E-11: The information system, for hardware token-based authentication, employs mechanisms that satisfy [Assignment: organization-defined token quality requirements]. Security Baseline: Low, Moderate, and High

NIST SP 800-53 Control: IA-5
HUD Policy: 5.1.5 a. Program Offices/System Owners ensure that authenticators are distributed to individuals and/or devices in accordance with the Department's identity, credential and access management business processes. b. The OCIO and OCHCO: • Establish and maintain administrative procedures for initial authenticator distribution including in person receipt for PIV cards, for lost/compromised or damaged authenticators, for revoking authenticators, and for refreshing authenticators. • Refresh PIV cards in accordance with Federal standards, but in no case should a PIV card be valid more than 5 years. • Establish the minimum content for authenticators based on Federal Directives and Standards including Homeland Security Presidential Directive 12(HSPD-12) and FIPS 201, *Personal Identity Verification for Federal Employees and Contractors*, and supporting NIST Special Publications. c. Program Offices/System Owners of information systems that require authentication controls over the Internet between outside parties and HUD utilize authentication mechanisms for the information system, in accordance with NIST SP 800-63, *Electronic Authentication Guide*. d. Program Offices/System Owners ensure that information systems categorized as moderate or high-impact require multi-factor authentication. To the extent information systems are integrated into the Department's Single Sign-On infrastructure, they are not required to establish system-specific authentication mechanisms. e. In those systems where user identity is authenticated by password: • The system ISSO determines and enforces appropriate measures to ensure that strong passwords are used. • The system ISSO develops and implements administrative procedures for initial password distribution, for lost/compromised passwords, and for revoking passwords. • The system ISSO determine and enforce the appropriate frequency for changing Passwords in accordance with HUD policy established under §5.2.2. • The system shall ensure that users cannot reuse a password for at least eight iterations. • The system shall ensure that passwords are not displayed when entered. • The system shall protect passwords from unauthorized disclosure and modification when stored and transmitted. • Users shall not share personal passwords. f. Users shall select strong passwords and not reuse old passwords. All passwords are required to be 8 characters in length including 1 upper case, 1 number and 1 special character (e.g., !, @, #, $). g. Use of group passwords shall be limited to situations dictated by operational necessity or those critical for mission accomplishment. Use of a Group User ID and password must be approved by the appropriate Authorizing Official.

5.1.6. Authenticator Feedback

The following policy provides guidance to ensure that authentication information is not revealed during the authentication process.

NIST SP 800-53 Control: IA-6
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. Security Baseline: Low, Moderate, and High

NIST SP 800-53 Control: IA-6
HUD Policy: 5.1.6 a. In those systems where user identity is authenticated by a password, the system shall ensure that passwords are not displayed when entered (e.g., displaying asterisks when a user types in a password). b. Information systems relying on Machine IDs shall ensure that IDs and passwords are stored in separate files, are never displayed or shared, and only accessible to authorized individuals.

5.1.7. Cryptographic Module Authentication

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

The following policy provides guidance regarding the use of encryption mechanisms on HUD information systems.

NIST SP 800-53 Control: IA-7
IA-7: The information system implements mechanisms for authentication to a cryptographic module that meet the requirements of applicable Federal laws, Executive Orders, Directives, policies, regulations, standards, and guidance for such authentication. Security Baseline: Low, Moderate, and High
HUD Policy: 5.1.7 a. Program Offices/Systems Owners identify information systems transmitting or storing sensitive information that may require protection based on a risk assessment. If encryption is required, the following methods are acceptable for encrypting sensitive information: • Products using triple Data Encryption Standard (3DES) or Advanced Encryption Standard (AES) algorithms that have been validated under FIPS 140-2 (as amended). (All new systems should use AES because it is expected that triple DES will be phased out.) • Secure Sockets Layer Version 3.0 (SSL3.0) or Transport Layer Security Version 1.0 (TLS1.0) • National Security Agency (NSA) Type 2 or Type 1 encryption b. The CISO and Deputy CIO for IOO ensure cryptographic key establishment and management is done in accordance with NIST SP 800-56, *Recommendation on Key Establishment Schemes*, and NIST SP 800-57, *Recommendation on Key Management*.

5.1.8. Identification and Authentication (Non-organizational Users)

HUD's vast community of users, well over 90%, are non-organizational users and include grantees, state and local government employees and third-party business partners. It is a broad and complex universe of information system users where confidence in virtual identities is critical to the Department's housing mission. It is critical to balance the need for confidence that the non-organizational user is the authorized entity while ensuring Departmental business processes are meeting availability requirements. The Department must ensure the secure identification of people (and processes acting on behalf of non-organizational users), while maintaining an efficient and cost-effective traffic flow.

The Federal Government has much work underway to federate identity which would allow the connection of one identity repository to another. Federation enables identity providers and relying parties to agree and to operate under compatible policies, standards, and technologies so the end-user identity information provided by identity providers can be understood and trusted such that a user does not have to manually logon to multiple systems. The ultimate goal of

identity federation is to enable users of one domain to securely access data or systems of another domain seamlessly, and without the need for completely redundant user administration.

NIST SP 800-53 Control: IA-8
IA-8: The information system uniquely identifies and authenticates non-organizational users (or processes acting on behalf of non-organizational users). Security Baseline: Low, Moderate, and High
E-1: The information system accepts and electronically verifies Personal Identity Verification (PIV) credentials from other federal agencies. Security Baseline: Low, Moderate, and High
E-2: The information system accepts only FICAM-approved third-party credentials. Security Baseline: Low, Moderate, and High
E-3: The organization employs only FICAM-approved information system components in [Assignment: organization-defined information systems] to accept third-party credentials. Security Baseline: Low, Moderate, and High
E-4: The information system conforms to FICAM-issued profiles. Security Baseline: Low, Moderate, and High
HUD Policy: 5.1.8 a. State and local governments must provide their employees that require access to HUD systems a unique nine-digit number. This number must consist of a unique departmental agency code and an employee position number. b. Program Offices/System Owners ensure information systems under their purview require authentication mechanisms that are sufficiently robust to uniquely identify non-organizational users (or processes acting on behalf) consistent with the information system's exposure to risks of authentication error as defined under NIST 800-63, *Electronic Authentication Guideline.* c. Program Offices/System Owners who elect to accept identity credentials issued by third-party identity providers shall only accept identity credentials from providers whose reliability has been established and accepted by the agency or a provider who is a member of the Federal Trust Framework and have been through the Federal Trust Framework Provider Adoption Process.

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 policies 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
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.

5.2.1. Access Control Policy and Procedures

The following policy addresses the requirement to develop policy and procedures for access control.

NIST SP 800-53 Control: AC-1
AC-1: The organization: a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]: 1. An Access Control Policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the Access Control Policy and associated access controls. b. Reviews and updates the current: 1. Access Control Policy [Assignment: organization-defined frequency]; and 2. Access control procedures [Assignment: organization-defined frequency]. Security Baseline: Low, Moderate, and High
Implementation
This control is implemented by the *Information Technology Security Policy, Handbook 2400.25 Rev. 4,* that defines HUD's formal security policies and the HUD *Information Technology Security Procedures* that defines HUD's formal security procedures. HUD reviews the policies and procedures minimally every year or when impacted by a significant change or underlying standard. The HUD security policies and procedures are disseminated via the HUD Intranet for all HUD's users to access.

5.2.2. Account Management

The following policy provides guidance for the management of accounts on HUD information systems. This includes account creation, auditing, modifying and disabling. The policy also identifies roles and responsibilities.

NIST SP 800-53 Control: AC-2
AC-2: The organization: a. Identifies and selects the following types of information system accounts to support organizational missions/business functions: [Assignment: organization-defined information system account types]; b. Assigns account managers for information system accounts; c. Establishes conditions for group and role membership; d. Specifies authorized users of the information system, group and role membership, and access authorizations (i.e., privileges) and other attributes (as required) for each account; e. Requires approvals by [Assignment: organization-defined personnel or roles] for requests to create information system accounts; f. Creates, enables, modifies, disables, and removes information system accounts in accordance with [Assignment: organization-defined procedures or conditions]; g. Monitors the use of information system accounts; h. Notifies account managers: 1. When accounts are no longer required; 2. When users are terminated or transferred; and 3. When individual information system usage or need-to-know changes. i. Authorizes access to the information system based on: 1. A valid access authorization; 2. Intended system usage; and 3. Other attributes as required by the organization or associated missions/business functions. j. Reviews accounts for compliance with account management requirements [Assignment: organization-defined frequency]; and k. Establishes a process for reissuing shared/group account credentials (if deployed) when individuals are removed from the group. Security Baseline: Low, Moderate, and High
E-1: The organization employs automated mechanisms to support the management of information system accounts. Security Baseline: Moderate and High
E-2: The information system automatically [Selection: removes; disables] temporary and emergency accounts after [Assignment: organization-defined time period for each type of account]. Security Baseline: Moderate and High
E-3: The information system automatically disables inactive accounts after [Assignment: organization-defined time period]. Security Baseline: Moderate and High
E-4: The information system automatically audits account creation, modification, enabling, disabling, and removal actions, and notifies [Assignment: organization-defined personnel or roles]. Security Baseline: Moderate and High
E-5: The organization requires that users log out when [Assignment: organization-defined time-period of expected inactivity or description of when to log out]. Security Baseline: High
E-11: The information system enforces [Assignment: organization-defined circumstances and/or usage conditions] for [Assignment: organization-defined information system accounts].

NIST SP 800-53 Control: AC-2
Security Baseline: High
E-12: The organization: (a) Monitors information system accounts for [Assignment: organization-defined atypical use]; and (b) Reports atypical usage of information system accounts to [Assignment: organization-defined personnel or roles]. Security Baseline: High
E-13: The organization disables accounts of users posing a significant risk within [Assignment: organization-defined time period] of discovery of the risk. Security Baseline: High
HUD Policy: 5.2.2 a. Program Offices/System Owners ensure that users of information systems supporting their programs have a validated requirement to access these systems. b. Program Offices/System Owners, in concert with the System Security Administrator, ensure that Access privileges which increase from greater than read only be processed through HUD's account management system. c. Program Offices/System Owners ensure that users of information systems under their purview have approved access requests prior to granting access to the systems. d. Individuals that perform duties as Administrators shall have separate administrator and non-administrator accounts. e. ISSOs ensure that emergency accounts are properly authorized and maintained. For moderate- and high-impact systems, these accounts shall be automatically disabled after 48 hours. f. ISSOs ensure that guest/anonymous accounts are not used. g. The Deputy CIO for IOO ensure that all default vendor or factory-set administrator accounts and passwords shall be changed before installation or use on all systems owned or operated on behalf of HUD. h. Program Offices/System Owners ensure that user access is reviewed once a year. i. Program Offices/System Owners ensure that their information systems implement access control measures to provide protection from unauthorized alteration, loss, unavailability, or disclosure of information. j. The ISSO ensures that user IDs are disabled after a period of inactivity of no more than 90 days. If an information system has been enabled for Single Sign-On (SSO), ISSOs may measure the 90 days of inactivity based on a user's last logon to the HUD network. Logon may include access to the HUD Local Area Network (LAN) or logon via one of HUD's remote access connections. ISSOs must ensure that the base system(s) upon which an information system relies for the 90 day inactivity trigger is identified in system documentation. For moderate- and high-impact systems, the 90 day inactivity trigger must be automated. k. Program Offices/System Owners ensure that their moderate- and high-impact systems use an automated mechanism to support management of information system accounts. For moderate- and high-impact systems, the automated mechanism shall track account creation, disabling, and termination to support audit of such actions and, as required, notify appropriate individuals.

5.2.3. Access Enforcement

The following policy provides guidance to ensure that HUD information systems include mechanisms for enforcing access control policies.

NIST SP 800-53 Control: AC-3
AC-3: The information system enforces approved authorizations for logical access to information and system resources in accordance with applicable access control policies.

NIST SP 800-53 Control: AC-3
Security Baseline: Low, Moderate, and High
HUD Policy: 5.2.3 a. The CISO along with the Deputy CIO for IOO ensures access control policies (e.g., identity-based policies, role-based policies, rule-based policies) and associated access enforcement mechanisms (e.g., access control lists, access control matrices, cryptography) are used throughout HUD to control access between users (or processes acting on behalf of users) and objects (e.g., devices, files, records, processes, programs, domains) in the information system. b. Program Offices/System Owners, and System Security Administrators grant, modify, and remove access to applications in accordance with Department and information system policies, and report evidence of unauthorized access or known security breaches. c. Access enforcement mechanisms are employed at the application level, when necessary, to provide increased information security for the organization. d. If encryption of stored information is employed as an access enforcement mechanism, the cryptography used is FIPS 140-2 (as amended) compliant.

5.2.4. Information Flow Enforcement

Information flow enforcement is the capability of a system to control the flow of information between sources and destinations both internal to the system and between interconnected systems. The mechanisms commonly used are label-based control, which relies on explicit labels on information, source and destination items and, domain-based, control which relies on protected processing domains.

The following policy addresses the requirement for HUD information systems to enforce the authorizations for governing internal flow of information.

NIST SP 800-53 Control: AC-4
AC-4: The information system enforces approved authorizations for controlling the flow of information within the system and between interconnected systems based on [Assignment: organization-defined information flow control policies]. Security Baseline: Moderate and High
HUD Policy: 5.2.4 a. Program Offices/System Owners ensure moderate- and high-impact systems within their purview are capable of enforcing flow control by using explicit labels on information internal to the system as well as between systems.

5.2.5. Separation of Duties

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

The following policy addresses the requirement for HUD systems to have the capability to enforce separation of duties through the use of unique user identifiers.

NIST SP 800-53 Control: AC-5
AC-5: The organization: a. Separates [Assignment: organization-defined duties of individuals]; b. Documents separation of duties of individuals; and c. Defines information system access authorizations to support separation of duties. Security Baseline: Moderate and High
HUD Policy: 5.2.5 a. Program Offices/System Owners divide and separate duties and responsibilities of critical information system functions among different individuals to minimize the possibility that any one individual would have the necessary authority or systems access to be able to engage in fraudulent or criminal activity. b. Program Offices/System Owners maintain documents which support the separation of duties. c. Program Offices/System Owners implement separation of duties through assigned information system access authorizations.

5.2.6. Least Privilege

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

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

The following policy provides guidance to ensure that the principle of least privilege is enforced.

NIST SP 800-53 Control: AC-6
AC-6: The organization employs the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions. Security Baseline: Moderate and High
E-1: The organization explicitly authorizes access to [Assignment: organization-defined security functions (deployed in hardware, software, and firmware) and security-relevant information]. Security Baseline: Moderate and High
E-2: The organization requires that users of information system accounts, or roles, with access to [Assignment: organization-defined security functions or security-relevant information], use non-privileged accounts or roles, when accessing nonsecurity functions. Security Baseline: Moderate and High
E-3: The organization authorizes network access to [Assignment: organization-defined privileged commands] only for [Assignment: organization-defined compelling operational needs] and documents the rationale for such access in the security plan for the information system. Security Baseline: High

NIST SP 800-53 Control: AC-6
E-5: The organization restricts privileged accounts on the information system to [Assignment: organization-defined personnel or roles]. Security Baseline: Moderate and High
E-9: The information system audits the execution of privileged functions. Security Baseline: Moderate and High
E-10: The information system prevents non-privileged users from executing privileged functions to include disabling, circumventing, or altering implemented security safeguards/countermeasures. Security Baseline: Moderate and High
HUD Policy: 5.2.6 a. Program Offices/System Owners employ the concept of least privilege, allowing only authorized accesses for users (and processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions.

5.2.7. Unsuccessful Logon Attempts

The following policy provides guidance to ensure that HUD information systems are configured to lock any user account immediately and automatically following a specified number of consecutive failed logon attempts.

NIST SP 800-53 Control: AC-7
AC-7: The information system: a. Enforces a limit of [Assignment: organization-defined number] consecutive invalid logon attempts by a user during a [Assignment: organization-defined time period]; and b. Automatically [Selection: locks the account/node for an [Assignment: organization-defined time period]; locks the account/node until released by an administrator; delays next logon prompt according to [Assignment: organization-defined delay algorithm]] when the maximum number of unsuccessful attempts is exceeded. Security Baseline: Low, Moderate, and High
HUD Policy: 5.2.7 a. Program Offices/System Owners ensure that their information systems implement and enforce an Account Lockout Policy that limits the number of consecutive failed logon attempts to three within a thirty-minute period. b. The account remains locked until the user unlocks the account using the self-service account management functionality managed by the OCIO or the manual intervention by an appropriate Security Administrator. Users who have not registered with the Department's self-service account management functionality will be requested by the Security Administrator to register immediately upon being restored access. Account lock-out occurs regardless of whether the login is via a local or network connection.

5.2.8. System Use Notification

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

system, informing users that equipment is the property of the government, that the use of government property is for the conduct of government business only, and that the use of government equipment is subject to monitoring.

The following policy provides guidance to ensure that all HUD systems display a standard notification message and the appropriate warnings to users of those systems.

NIST SP 800-53 Control: AC-8
AC-8: The information system: a. Displays to users an CISO-approved system use notification message or banner before granting access to the system that provides privacy and security notices consistent with applicable Federal laws, Executive Orders, Directives, policies, regulations, standards, and guidance and states that: 1. Users are accessing a U.S. Government information system; 2. Information system usage may be monitored, recorded, and subject to audit; 3. Unauthorized use of the information system is prohibited and subject to criminal and civil penalties; and 4. Use of the information system indicates consent to monitoring and recording. b. Retains the notification message or banner on the screen until users acknowledge the usage conditions and take explicit actions to log on to or further access the information system; and c. For publicly accessible systems: 1. Displays a CISO-approved system use information, before granting further access; 2. Displays references, if any, to monitoring, recording, or auditing that are consistent with privacy accommodations for such systems that generally prohibit those activities; and 3. Includes a description of the authorized uses of the system. Security Baseline: Low, Moderate, and High
HUD Policy: 5.2.8 a. The CISO, as approved by the HUD's Office of General Counsel, provides a standard notification message for HUD systems that warns unauthorized users that they have accessed a U.S. Government system and can be punished. The wording shall also warn authorized users that they are subject to monitoring and recording and that use of the system indicates consent to such monitoring and recording. b. Information systems internal to the HUD network shall display a warning banner stipulated by the HUD CISO and the Privacy Officer, and approved by the HUD's Office of General Counsel, when applicable. The warning banner shall require users to click through, indicating acknowledgment, prior to granting access to the system. c. Information systems accessible to the public shall provide both a security and privacy statement approved by the CISO and the Privacy Officer at every entry point. The statement shall include a description of the authorized uses of the system.

5.2.9. Concurrent Session Control

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

The following policy provides guidance to ensure that high-impact HUD systems limit the number of concurrent sessions.

NIST SP 800-53 Control: AC-10
AC-10: The information system limits the number of concurrent sessions for each [Assignment: organization-defined account and/or account type] to [Assignment: organization-defined number]. Security Baseline: High

NIST SP 800-53 Control: AC-10
HUD Policy: 5.2.9 a. For high-impact systems, the Program Offices/System Owners ensure that the system does not allow concurrent sessions.

5.2.10. Session Lock

The following policy provides guidance to ensure that HUD information systems are configured to deactivate any user session immediately and automatically following a specified period of inactivity, in such a way that will require the user to re-authenticate the user's identity before resuming interaction with the system.

NIST SP 800-53 Control: AC-11
AC-11: The information system: a. Prevents further access to the system by initiating a session lock after [Assignment: organization-defined time period] of inactivity or upon receiving a request from a user; and b. Retains the session lock until the user re-establishes access using established identification and authentication procedures. Security Baseline: Moderate and High
E-1: The information system conceals, via the session lock, information previously visible on the display with a publicly viewable image. Security Baseline: Moderate and High
HUD Policy: 5.2.10 a. All users shall ensure that their unattended workstations are either logged off or locked, or that a password-protected screensaver is used. b. The Deputy CIO for IOO ensures HUD (owned or leased) workstations are configured to automatically lock after a minimum of 15 minutes but in no circumstances exceeding 30 minutes of inactivity. c. Program Offices/System Owners of moderate- or high-impact systems shall ensure that applications are configured to automatically lock after a minimum of 15 minutes but in no circumstances exceeding 30 minutes of inactivity. If an information system has been enabled for Single Sign-On, session lock-out may rely on the session lock out parameters set for the workstation or logon method used such as remote access. d. Program Offices/System Owners of moderate- or high- impact systems shall ensure that applications are configured to terminate user-initiated logical sessions after a period of 8 hours. Logical sessions are initiated whenever a user accesses an organizational system; session termination terminates all processes associated with a user's logical session except those processes that are specifically created by the user (i.e., session owner) to continue after the session is terminated. Session termination requires users to re-authenticate to the application.

5.2.11. Session Termination

The following policy provides guidance to ensure that HUD information systems are configured to terminate any remote user session immediately and automatically following a specified period of inactivity.

NIST SP 800-53 Control: AC-12
AC-12: The information system automatically terminates a user session after [*Assignment: organization-defined conditions or trigger events requiring session disconnect*]. Security Baseline: Moderate and High
HUD Policy: 5.2.11 a. Program Offices/System Owners ensure information systems automatically terminate a user session after user exits or disconnects from session or within 30 minutes of inactivity.

5.2.12. Permitted Actions without Identification or Authentication

The following policy provides guidance for identifying user actions that can be performed on HUD's publicly available information systems.

NIST SP 800-53 Control: AC-14
AC-14: The organization: a. Identifies [Assignment: organization-defined user actions] that can be performed on the information system without identification or authentication consistent with organizational missions/business functions; and b. Documents and provides supporting rationale in the Security Plan for the information system, user actions not requiring identification or authentication. Security Baseline: Low, Moderate, and High
HUD Policy: 5.2.12 a. Program Offices/System Owners identify and document specific user actions that can be performed on public websites or other publicly available information systems without identification and authentication. b. For moderate- or high-impact systems, actions to be performed without identification and authentication will be permitted only to the extent necessary to accomplish mission objectives. Permitted actions shall be documented in security plans.

5.2.13. Remote Access

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

The following policy provides guidance for the implementation and monitoring of remote access capabilities.

NIST SP 800-53 Control: AC-17
AC-17: The organization: a. Establishes and documents usage restrictions, configuration/connection requirements, and implementation guidance for each type of remote access allowed; and b. Authorizes remote access to the information system prior to allowing such connections. Security Baseline: Low, Moderate, and High

NIST SP 800-53 Control: AC-17
E-1: The information system monitors and controls remote access methods. Security Baseline: Moderate and High
E-2: The information system implements cryptographic mechanisms to protect the confidentiality and integrity of remote access sessions. Security Baseline: Moderate and High
E-3: The information system routes all remote accesses through [Assignment: organization-defined number] managed network access control points. Security Baseline: Moderate and High
E-4: The organization: (a) Authorizes the execution of privileged commands and access to security-relevant information via remote access only for [Assignment: organization-defined needs]; and (b) Documents the rationale for such access in the security plan for the information system. Security Baseline: Moderate and High
HUD Policy: 5.2.13 a. The Deputy CIO for IOO provides remote access mechanisms that are centrally managed, monitored, and protected by strong authentication. The mechanisms shall have the capability to provide strong cryptographic mechanisms for authentication and protection of sensitive information during transmission. For access to moderate- or high-impact systems, the session shall be encrypted and access shall be managed through a limited number of managed access control point. b. Program Offices/System Owners authorize and approve remote access methods for systems under their purview. The remote access methods shall only use mechanisms authorized by the Deputy CIO for IOO. c. Remote access is limited to official use by individuals authorized by HUD management to work at home, or other non-HUD worksite, (e.g., maintenance ports, system and device administration) only for compelling operational needs and during emergencies. d. ISSOs authorize (in writing) users requiring remote access including remote access for privileged functions, and documents the rationale for such access in the Security Plan. e. Program Offices/Systems Owners of moderate- or high-impact systems shall use encryption to implement the following controls: • Remote access; • Wireless access; • Cryptographic module authentication; and • Transmission integrity and confidentiality. f. Program Offices/System Owners prohibit users from copying HUD-related documents to the hard/floppy drives of personally- or privately-owned computers. During the time a user is on the HUD telecommuting website, he or she is strictly prohibited from having an open peer-to-peer software connection (e.g., LimeWire, Napster) that enables internet file sharing (commonly used in the sharing of music files, with the Internet community at large).

5.2.14. Wireless Access Restrictions

Wireless communications technologies include the following:

- Wireless systems (e.g., wireless local area networks (WLAN), wireless wide area networks (WWAN), wireless personal area networks (WPAN), peer-to-peer wireless networks, IT systems that leverage commercial wireless services). Wireless systems include the

transmission medium, stationary integrated devices, firmware, supporting services, and protocols.

- Wireless portable electronic devices (PED) capable of storing, processing, or transmitting sensitive information (e.g., wireless-capable laptop computers, personal digital assistants (PDA), tablets, smart telephones, two-way pagers, handheld radios, cellular telephones, personal communications services (PCS) devices, multifunctional wireless devices, portable audio/video recording devices with wireless capability, scanning devices, and messaging devices (including Blackberry devices))
- Wireless tactical systems, including mission-critical communication systems and devices (e.g., include Land Mobile Radio (LMR) subscriber devices and infrastructure equipment, remote sensors, and technical investigative communications systems)

Wireless communications are inherently insecure. The following policy provides guidance to ensure that the transmission and storage of sensitive information using wireless technologies are protected from compromise.

NIST SP 800-53 Control: AC-18
AC-18: The organization: a. Establishes usage restrictions, configuration/connection requirements, and implementation guidance for wireless access; and b. Authorizes wireless access to the information system prior to allowing such connections. Security Baseline: Low, Moderate, and High
E-1: The information system protects wireless access to the system using authentication of [Selection (one or more): users; devices] and encryption. Security Baseline: High
E-4: The organization identifies and explicitly authorizes users allowed to independently configure wireless networking capabilities. Security Baseline: High
E-5: The organization selects radio antennas and calibrates transmission power levels to reduce the probability that usable signals can be received outside of organization-controlled boundaries. Security Baseline: High
HUD Policy: 5.2.14 a. The Deputy CIO for IOO approves the implementation and use of all Wireless Local Area Networks (WLAN) and wireless access points, including international requests at a specified risk level and only after they have been certified and accredited. b. The Deputy CIO for IOO ensures that all WLANs and wireless fidelity (Wi-Fi) Access Protection have been configured in accordance with NIST SP 800-48, Wireless Network Security and NIST SP 800-97, *Guide to IEEE 802.11: Establishing Robust Security Networks.* c. The Deputy CIO for IOO implements encryption and strong identification and authentication (e.g., Extensible Authentication Protocol with WAP or Institute of Electrical and Electronics Engineers (IEEE) 802.11i) on moderate- or high-impact WLANs and access points. d. The Deputy CIO for IOO and CISO shall scan for rogue access points on HUD's high-impact systems annually.

5.2.15. Access Control for Mobile Devices

The following policy provides guidance regarding the access control for portable and mobile devices connecting to HUD networks.

NIST SP 800-53 Control: AC-19
AC-19: The organization: a. Establishes usage restrictions, configuration requirements, connection requirements, and implementation guidance for organization-controlled mobile devices; and b. Authorizes the connection of mobile devices to organizational information systems. Security Baseline: Low, Moderate and High
E-5: The organization employs [Selection: full-device encryption; container encryption] to protect the confidentiality and integrity of information on [Assignment: organization-defined mobile devices]. Security Baseline: Moderate and High
HUD Policy: 5.2.15 a. The Deputy CIO for IOO establishes connection criteria for allowing portable or mobile devices access to HUD's networks. b. The Deputy CIO for IOO establishes and maintains a Mobile Device Management (MDM) Program which: • Ensures implementation of the connection criteria for all mobile devices connecting to the HUD network following the Mobile Device Management Policy procedures. • Develops and maintains security control standards for all HUD-owned mobile IT devices that create, access, process or store Agency information, and the information created, collected, and processed on behalf of HUD on these devices. • Monitors the HUD network for compliance with the MDM Program requirements. c. Program Offices/System Owners and Users shall ensure moderate- or high-impact information residing on portable or mobile systems use FIPS 140-2-approved (as amended) encryption to protect the information.

5.2.16. Use of External Information Systems

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

NIST SP 800-53 Control: AC-20
AC-20: The organization establishes terms and conditions, consistent with any trust relationships established with other organizations owning, operating, and/or maintaining external information systems, allowing authorized individuals to: a. Access the information system from external information systems; and b. Process, store, or transmit organization-controlled information using external information systems. Security Baseline: Low, Moderate, and High
E-1: The organization permits authorized individuals to use an external information system to access the information system or to process, store, or transmit organization-controlled information only when the organization:

NIST SP 800-53 Control: AC-20
(a) Verifies the implementation of required security controls on the external system as specified in the organization's Information Security Policy and Security Plan; or (b) Retains approved information system connection or processing agreements with the organizational entity hosting the external information system. Security Baseline: Moderate, and High
E-2: The organization [Selection: restricts; prohibits] the use of organization-controlled portable storage devices by authorized individuals on external information systems. Security Baseline: Moderate and High
HUD Policy: 5.2.16 a. Program Offices/System Owners prohibit users from using personally- or privately-owned equipment and software (e.g., laptop computers, Blackberries, Universal Serial Bus (USB) flash drives, external drives, diskettes, removable media, or personal digital devices) to process, access, or store information for HUD-related work except through approved remote access (e.g., Telework Agreements), or email without prior written approval from the Program Offices/System Owner. b. Employees and contractors shall not directly connect equipment not owned or leased by HUD to HUD equipment or networks without prior written approval from the CISO. The written approval shall include a terms and conditions statement that addresses at a minimum: (i) the types of applications that can be accessed from personally-owned information systems; (ii) the maximum FIPS 199 security category of information that can be processed, stored, and transmitted; (iii) how other users of the personally-owned information system will be prevented from accessing federal information; (iv) the use of virtual private network (VPN) and firewall technologies; (v) the use of and protection against the vulnerabilities of wireless technologies; (vi) the maintenance of adequate physical security controls; (vii) the use of virus and spyware protection software; and (viii) how often the security capabilities of installed software are to be updated (e.g., operating system and other software security patches, virus definitions, firewall version updates, and spyware definitions). c. HUD employees or contractors shall not transmit sensitive HUD information to any personal email account that is not authorized to receive it. d. Program Offices/System Owners prohibit users from downloading HUD-related work onto any external media from their HUD computer for the purpose of working on those documents or tasks on any personally- or privately-owned computer equipment.

5.2.17. Information Sharing

The following policy addresses the personal use of government office equipment and HUD information systems. Policies governing personal use may be contained in several HUD management directives.

NIST SP 800-53 Control: AC-21
AC-21: The organization: a. Facilitates information sharing by enabling authorized users to determine whether access authorizations assigned to the sharing partner match the access restrictions on the information for [Assignment: organization-defined information sharing circumstances where user discretion is required]; and b. Employs [Assignment: organization-defined automated mechanisms or manual processes] to assist users in making information sharing/collaboration decisions. Security Baseline: Moderate and High

NIST SP 800-53 Control: AC-21
HUD Policy: 5.2.17 The CISO must: a. Facilitate information sharing by enabling ***authorized*** users to determine whether access authorizations assigned to the sharing partner match the access restrictions on the information for information sharing circumstances where user discretion is required]; and b. Employ an automated mechanisms or manual processes to assist users in making information sharing/collaboration decisions.

5.2.18. Publicly Accessible Content

NIST SP 800-53 Control: AC-22
AC-22: The organization: a. Designates individuals authorized to post information onto a publicly accessible information system; b. Trains authorized individuals to ensure that publicly accessible information does not contain nonpublic information; c. Reviews the proposed content of information prior to posting onto the publicly accessible information system to ensure that nonpublic information is not included; and d. Reviews the content on the publicly accessible information system for nonpublic information [Assignment: organization-defined frequency] and removes such information, if discovered. Security Baseline: Low, Moderate, and High
HUD Policy HUD:22
HUD Policy: 5.2.18 The CIO must: a. Designate individuals authorized to post information onto a publicly accessible information system; b. Train authorized individuals to ensure that publicly accessible information does not contain nonpublic information; c. Review the proposed content of information prior to posting onto the publicly accessible information system to ensure that nonpublic information is not included; and d. Review the content on the publicly accessible information system for nonpublic information quarterly and remove such information, if discovered.

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
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.

5.3.1. Audit and Accountability Policy and Procedures

The following policy addresses the requirement to develop and maintain audit and accountability policy and procedures.

NIST SP 800-53 Control: AU-1
AU-1: The organization: a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]: 1. An Audit and Accountability Policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the audit and accountability policy and associated audit and accountability controls; and b. Reviews and updates the current: 1. Audit and Accountability Policy [Assignment: organization-defined frequency]; and 2. Audit and accountability procedures [Assignment: organization-defined frequency]. Security Baseline: Low, Moderate, and High
Implementation
This control is implemented by the *Information Technology Security Policy, Handbook 2400.25 Rev. 4,* that defines HUD's formal security policies and the HUD *Information Technology Security Procedures* that defines HUD's formal security procedures. HUD reviews the policies and procedures minimally every year or when impacted by a significant change or underlying standard. The HUD security policies and procedures are disseminated via the HUD Intranet for all HUD's users to access.

5.3.2. Audit Events

Audit events are those activities that can be tracked that provide information regarding system resource usage. The following policy addresses the requirement for HUD information systems to generate records for identified auditable events.

NIST SP 800-53 Control: AU-2
AU-2: The organization: a. Determines that the information system is capable of auditing the following events: [Assignment: organization-defined auditable events]; b. Coordinates the security audit function with other organizational entities requiring audit-related information to enhance mutual support and to help guide the selection of auditable events; c. Provides a rationale for why the auditable events are deemed to be adequate to support after-the-fact investigations of security incidents; and d. Determines that the following events are to be audited within the information system: [Assignment: organization-defined audited events (the subset of the auditable events defined in AU-2 a.) along with the frequency of (or situation requiring) auditing for each identified event]. Security Baseline: Low, Moderate, and High
E-3: The organization reviews and updates the audited events [Assignment: organization-defined frequency]. Security Baseline: High
HUD Policy: 5.3.2 a. HUD information systems must be capable of auditing the following events: (i.e., event type; account logon events, account management; object access; policy change; privilege use; process tracking; system events). CA eTrust Audit captures the following: (i) date and time of event; (ii) the component of the information system

NIST SP 800-53 Control: AU-2
where the event occurred; (iii) type of event; (iv) user/subject identity; and (v) the outcome (failure) of the event; (vi) session, connection, transaction, and activity duration; (vii) source and destination addresses) b. Unauthorized access, unauthorized system or data modification, system outages or performance interruptions, system performance malfunctions, data leakage, or unauthorized data extraction/removal. c. Program Offices/System Owners shall identify for each system under their purview, the minimum events requiring auditing on a continuous basis and which events require auditing in response to specific situations based on an assessment of risk and documented in the System Security Plan. The auditing frequency shall be specified in System Security Plans. d. Program Offices/System Owners review and update, as needed, the list of auditable events for systems under their purview. At a minimum, the auditable events shall be adequate to support after-the-fact investigations of security incidents.

5.3.3. Content of Audit Records

The following policy provides guidance to ensure that the information that is included in audit records is sufficient to determine system activity.

NIST SP 800-53 Control: AU-3
AU-3: The information system generates audit records containing information that establishes what type of event occurred, when the event occurred, where the event occurred, the source of the event, the outcome of the event, and the identity of any individuals or subjects associated with the event. Security Baseline: Low, Moderate, and High
E-1: The information system generates audit records containing the following additional information: [Assignment: organization-defined additional, more detailed information]. Security Baseline: Moderate and High
E-2: The information system provides centralized management and configuration of the content to be captured in audit records generated by [Assignment: organization-defined information system components]. Security Baseline: High
HUD Policy: 5.3.3 a. Program Offices/System Owners ensure that audit trails are sufficient in detail to facilitate the reconstruction of events if a system is compromised or if a malfunction occurs or is suspected. The audit trail shall contain, at a minimum, the following information: • Time and date of the event; • The component of the information system (e.g., software component and hardware component); • Where the event occurred; • Type of event; • User/Subject identity; • Outcome (success or failure) of the event; and • Additional items as defined in the Security Plan. b. For moderate- to high-impact systems, the audit function shall have the capability of providing more detailed information for audit events identified by type, location, or subject. For high-impact systems, the system shall provide the capability for centralized management of audit records.

5.3.4. Audit Storage Capacity

The following policy provides guidance to ensure that audit record storage capacity is sufficient.

NIST SP 800-53 Control: AU-4
AU-4: The organization allocates audit record storage capacity in accordance with [*Assignment: organization-defined audit record storage requirements*]. Security Baseline: Low, Moderate, and High
HUD Policy: 5.3.4 a. Program Offices/System Owners shall ensure that the system allocates sufficient audit record storage capacity and configures auditing to reduce the likelihood of such capacity being exceeded.

5.3.5. Response to Audit Processing Failures

The following policy provides guidance to ensure that HUD information systems are capable of alerting personnel in the event of an audit processing failure.

NIST SP 800-53 Control: AU-5
AU-5: The information system: a. Alerts [Assignment: organization-defined personnel or roles] in the event of an audit processing failure; and b. Makes the following additional actions: [Assignment: organization-defined actions to be taken (e.g., shut down information system, overwrite oldest audit records, stop generating audit records)]. Security Baseline: Low, Moderate, and High
E-1: The information system provides a warning to [Assignment: organization-defined personnel, roles, and/or locations] within [Assignment: organization-defined time period] when allocated audit record storage volume reaches [Assignment: organization-defined percentage] of repository maximum audit record storage capacity. Security Baseline: High
E-2: The information system provides an alert in [Assignment: organization-defined real-time period] to [Assignment: organization-defined personnel, roles, and/or locations] when the following audit failure events occur: [Assignment: organization-defined audit failure events requiring real-time alerts]. Security Baseline: High
HUD Policy: 5.3.5 a. Program Offices/System Owners ensure that the system alerts the appropriate officials in the event of an audit failure or when the audit capacity is close to being reached. b. For high-impact systems, the appropriate officials are alerted when the storage volume reaches 80%. c. For high-impact systems, appropriate officials are alerted in real-time when audit capabilities are disabled. d. Program Offices/System Owners shall make a risk-based decision on which one of the following actions the system should take in the event of an audit failure or when the audit capacity is being reached: • Shut down the system; • Overwrite the oldest audit records; or • Stop generating audit records.

5.3.6. Audit Review, Analysis, and Reporting

The following policy provides guidance to ensure that processes are developed for reviewing, analyzing and reporting audit records.

NIST SP 800-53 Control: AU-6
AU-6: The organization: a. Reviews and analyzes information system audit records [Assignment: organization-defined frequency] for indications of [Assignment: organization-defined inappropriate or unusual activity]; and b. Reports findings to [Assignment: organization-defined personnel or roles]. Security Baseline: Moderate and High
E-1: The organization employs automated mechanisms to integrate audit review, analysis, and reporting processes to support organizational processes for investigation and response to suspicious activities. Security Baseline: Moderate and High
E-3: The organization analyzes and correlates audit records across different repositories to gain organization-wide situational awareness. Security Baseline: Moderate and High
E-5: The organization integrates analysis of audit records with analysis of [Selection (one or more): vulnerability scanning information; performance data; information system monitoring information; [Assignment: organization-defined data/information collected from other sources] to further enhance the ability to identify inappropriate or unusual activity. Security Baseline: High
E-6: The organization correlates information from audit records with information obtained from monitoring physical access to further enhance the ability to identify suspicious, inappropriate, unusual, or malevolent activity. Security Baseline: High
HUD Policy: 5.3.6 a. Program Offices/System Owners review and analyze information system audit records frequently for indications of inappropriate or unusual activity, and report findings to designated organizational officials; and b. Program Offices/System Owners adjust the level of audit review, analysis, and reporting within the information system when there is a change in risk to organizational operations, organizational assets, individuals, other organizations, or the Nation based on law enforcement information, intelligence information, or other credible sources of information.

5.3.7. Audit Reduction and Report Generation

The following policy provides guidance to ensure that HUD information systems are capable of processing audit records.

NIST SP 800-53 Control: AU-7
AU-7: The information system provides an audit reduction and report generation capability that: a. Supports on-demand audit review, analysis, and reporting requirements and after-the-fact investigations of security incidents; and b. Does not alter the original content or time ordering of audit records. Security Baseline: Moderate and High

NIST SP 800-53 Control: AU-7
E-1: The information system provides the capability to process audit records for events of interest based on [Assignment: organization-defined audit fields within audit records]. Security Baseline: Moderate and High
HUD Policy: 5.3.7 a. Program Offices/System Owners of moderate- or high-impact systems shall utilize audit reduction, review, and reporting techniques, while ensuring that original audit records needed to support after-the-fact investigations are not altered or compromised in such a manner as to reduce their utility and reliability in after-the-fact investigations. b. Program Offices/System Owners of moderate- and high-impact systems shall ensure the system provides the capability to automatically process audit records for events of interest based upon selectable, event criteria.

5.3.8. Time Stamps

The following policy provides guidance to ensure that HUD information systems provide time stamps for use in audit record generation.

NIST SP 800-53 Control: AU-8
AU-8: The information system: a. Uses internal system clocks to generate time stamps for audit records; and b. Records time stamps for audit records that can be mapped to Coordinated Universal Time (UTC) or Greenwich Mean Time (GMT) and meets [Assignment: organization-defined granularity of time measurement]. Security Baseline: Low, Moderate, and High
E-1: The information system: (a) Compares the internal information system clocks [Assignment: organization-defined frequency] with [Assignment: organization-defined authoritative time source]; and (b) Synchronizes the internal system clocks to the authoritative time source when the time difference is greater than [Assignment: organization-defined time period]. Security Baseline: Moderate and High
HUD Policy: 5.3.8 a. Program Offices/System Owners ensure that information systems under their purview provide time stamps for use in audit record generation. The time stamps shall be generated using internal information system clocks that are synchronized twice daily system-wide.

5.3.9. Protection of Audit Information

The following policy provides guidance to ensure that audit information is protected.

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

NIST SP 800-53 Control: AU-9
E-2: The information system backs up audit records [Assignment: organization-defined frequency] onto a physically different system or system component than the system or component being audited. Security Baseline: High
E-3: The information system implements cryptographic mechanisms to protect the integrity of audit information and audit tools. Security Baseline: High
E-4: The organization authorizes access to management of audit functionality to only [Assignment: organization-defined subset of privileged users]. Security Baseline: Moderate and High
HUD Policy: 5.3.9 a. Program Offices/System Owners ensure that their audit trails and audit logs are protected from unauthorized modification, access, or destruction while online and during offline storage.

5.3.10. Non-Repudiation

Non-repudiation protects users from being falsely accused of not completing an activity such as sending an email message or not signing an electronic document. Digital Signatures are one mechanism for insuring non-repudiation.

A digital signature is an electronic analogue of a written signature. The digital signature can be used to prove to a recipient or third-party that the originator did in fact sign the message (i.e., the message originators cannot repudiate the message).

NIST SP 800-53 Control: AU-10
AU-10: The information system protects against an individual (or process acting on behalf of an individual) falsely denying having performed [*Assignment: organization-defined actions to be covered by non-repudiation*]. Security Baseline: High
HUD Policy: 5.3.10 a. System Owners must ensure the information system protects against an individual falsely denying having performed a particular action.

5.3.11. Audit Record Retention

The following policy provides guidance to ensure that audit logs are retained in accordance with HUD records retention policies.

NIST SP 800-53 Control: AU-11
AU-11: The organization retains audit records for [Assignment: organization-defined time period consistent with records retention policy] 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
HUD Policy: 5.3.11

NIST SP 800-53 Control: AU-11
a. Program Offices/System Owners ensure that audit logs are recorded and retained in accordance with HUD's records retention policies, but in no case shall the retention frequency be less than one year for moderate- or high-impact systems.

5.3.12. Audit Generation

NIST SP 800-53 Control: AU-12
AU-12: The information system: a. Provides audit record generation capability for the auditable events defined in AU-2a at [Assignment: organization-defined information system components]; b. Allows [Assignment: organization-defined personnel or roles] to select which auditable events are to be audited by specific components of the information system; and c. Generates audit records for the events defined in AU-2 d. with the content defined in AU-3. Security Baseline: Low, Moderate, and High
E-1: The information system compiles audit records from [Assignment: organization-defined information system components] into a system-wide (logical or physical) audit trail that is time-correlated to within [Assignment: organization-defined level of tolerance for relationship between time stamps of individual records in the audit trail]. Security Baseline: High
E-3: The information system provides the capability for [Assignment: organization-defined individuals or roles] to change the auditing to be performed on [Assignment: organization-defined information system components] based on [Assignment: organization-defined selectable event criteria] within [Assignment: organization-defined time thresholds]. Security Baseline: High
HUD Policy: 5.3.12 a. Program Offices/System Owners retain recorded system audit records in accordance with HUD's record retention policies, but for no less than one year. b. Program Offices/System Owners allow designated organizational personnel to select which auditable events are to be audited by specific components of the system. c. Program Offices/System Owners shall generate audit records, at a minimum, for the list of auditable events in AU-2 at an information system level, (i.e., covering all the components that exist within an information system's defined system boundaries). At a minimum, the audit records shall provide documentation details specified in AU-3 of this policy. d. Program Offices/System Owners shall specify in their System Security Plans which information system components shall generate auditable event records.

5.4. System and Communications Protection

System 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 policies 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 Protection Policy and Procedures

The following policy provides guidance to ensure that system and communications (network) protection policy and procedures are developed.

NIST SP 800-53 Control: SC-1
SC-1: The organization: b. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]: 1. A System and Communications Protection Policy that addresses the purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the System and Communications Protection Policy and associated system and communications protection controls; and c. Reviews and updates the current: 1. System and Communications Protection Policy [Assignment: organization-defined frequency]; and 2. System and communications protection procedures [Assignment: organization-defined frequency]. Security Baseline: Low, Moderate, and High
Implementation
This control is implemented by the *Information Technology Security Policy, Handbook 2400.25 Rev. 4,* that defines HUD's formal security policies and the HUD *Information Technology Security Procedures* that defines HUD's formal security procedures. HUD reviews the policies and procedures minimally every year or when impacted by a significant change or underlying standard. The HUD security policies and procedures are disseminated via the HUD Intranet for all HUD's users to access.

5.4.2. Application Partitioning

The following policy provides guidance to ensure that HUD information systems are capable of separating user functionality from system management functionality.

NIST SP 800-53 Control: SC-2
SC-2: The information system separates user functionality (including user interface services) from information system management functionality. Security Baseline: Moderate and High

NIST SP 800-53 Control: SC-2
HUD Policy: 5.4.2 a. Program Offices/System Owners ensure that moderate- or high-impact systems physically or logically separate user interface services (e.g., public web pages) from information storage and management services (e.g., database management). Separation may be accomplished using different computers, different central processing units, different instances of the operating system, different network addresses, combinations of these methods, or other methods as appropriate.

5.4.3. Security Function Isolation

The following policy provides guidance to ensure that HUD information systems are capable of separating security functions from non-security functions.

NIST SP 800-53 Control: SC-3
SC-3: The information system isolates security functions from nonsecurity functions. Security Baseline: High
HUD Policy: 5.4.3 a. Program Offices/System Owners ensure high-impact systems under their purview isolates security functions from non-security functions (i.e., by means of partitions, domains) including access to and integrity of the hardware, software, and firmware that perform these functions. Maintain a separate execution domain (e.g., address space) for each executing process.

5.4.4. Information in Shared Resources

An information remnant is a small part or trace of information remaining after an information transfer. Therefore, it is important to 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. The following policy provides guidance to ensure that HUD information systems are capable of preventing unauthorized and unintended transfer of information through shared system resources.

NIST SP 800-53 Control: SC-4
SC-4: The information system prevents unauthorized and unintended information transfer via shared system resources. Security Baseline: Moderate and High
HUD Policy: 5.4.4 a. Program Offices/System Owners shall ensure that moderate- and high-impact systems within their purview prevent information, including encrypted representations of information, produced by the actions of a prior user/role (or the actions of a process acting on behalf of a prior user/role), from being available to any current user/role (or current process) that obtains access to a shared system resource (e.g., registers, main memory, secondary storage) after that resource has been released back to the information system.

5.4.5. Denial of Service Protection

Since the Internet is an open network available to everyone, including hackers and attackers, HUD must strike a balance that provides Internet connectivity to its constituents while

maintaining an appropriate level of security. The following policy provides guidance to ensure that HUD networks are protected against denial of service attacks.

NIST SP 800-53 Control: SC-5
SC-5: The information system protects against or limits the effects of the following types of denial of service attacks: [*Assignment: organization-defined types of denial of service attacks or reference to source for such information*] by employing [*Assignment: organization-defined security safeguards*]. Security Baseline: Low, Moderate, and High
HUD Policy: 5.4.5 a. The Deputy CIO for IOO ensures that controlled interfaces protecting the boundary filter certain types of packets to protect devices on HUD's internal network from being directly affected by denial of service attacks.

5.4.6. Boundary Protection

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

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

NIST SP 800-53 Control: SC-7
SC-7: The information system: a. Monitors and controls communications at the external boundary of the system and at key internal boundaries within the system; b. Implements subnetworks for publicly accessible system components that are [Selection: physically; logically] separated from internal organizational networks; and c. Connects to external networks or information systems only through managed interfaces consisting of boundary protection devices arranged in accordance with organizational security architecture. Security Baseline: Low, Moderate, and High
E-3: The organization limits the number of external network connections to the information system. Security Baseline: Moderate and High
E-4: The organization: a. Implements a managed interface for each external telecommunication service; b. Establishes a traffic flow policy for each managed interface; c. Protects the confidentiality and integrity of the information being transmitted across each interface; d. Documents each exception to the traffic flow policy with a supporting mission/business need and duration of that need; and e. Reviews exceptions to the traffic flow policy [Assignment: organization-defined frequency] and removes exceptions that are no longer supported by an explicit mission/business need. Security Baseline: Moderate and High

NIST SP 800-53 Control: SC-7
E-5: The information system at managed interfaces denies network communications traffic by default and allows network communications traffic by exception (i.e., deny all, permit by exception). Security Baseline: Moderate and High
E-7: The information system, in conjunction with a remote device, prevents the device from simultaneously establishing non-remote connections with the system and communicating via some other connection to resources in external networks. Security Baseline: Moderate and High
E-8: The information system routes [Assignment: organization-defined internal communications traffic] to [Assignment: organization-defined external networks] through authenticated proxy servers at managed interfaces. Security Baseline: High
E-18: The information system fails securely in the event of an operational failure of a boundary protection device. Security Baseline: High
E-19: The information system blocks both inbound and outbound communications traffic between [Assignment: organization-defined communication clients] that are independently configured by end users and external service providers. Security Baseline: High
HUD Policy: 5.4.6 a. Program Offices/System Owners ensure that interconnections between sensitive information systems under their purview and information systems not controlled by HUD are established only through controlled interfaces. The controlled interfaces shall be accredited at the highest security level of information on the network. b. The Deputy CIO for IT Operations ensures that a failure of the controlled interfaces does not result in any unauthorized release of information outside the information system boundary. c. The Deputy CIO for IOO ensures that there is no public access to HUD's internal networks except as appropriately mediated through a proxy server. d. The Deputy CIO for IOO ensures that alternate processing sites provide the same level of protection for network connections as the primary site. e. The Deputy CIO for IOO ensures that any direct connection of HUD networks to the Internet or to Extranets occurs through controlled interfaces that have been certified and accredited. f. The Deputy CIO for IT Operations ensures that publicly accessible information system components (e.g., public web servers) reside on separate sub-networks with separate physical network interfaces. g. Program Offices/System Owners, working with the Deputy CIO for IOO, shall 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.

5.4.7. Transmission Confidentiality and Integrity

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

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

The following policy provides guidance to ensure that HUD information systems are capable of protecting the integrity of information during transmission.

Additionally, the following policy provides guidance to ensure that HUD information systems are capable of protecting the confidentiality of information during transmission. NIST SP 800-52 and SP 800-77 provide guidance for protecting transmission confidentiality.

NIST SP 800-53 Control: SC-8
SC-8: The information system protects the [Selection (one or more): confidentiality; integrity] of transmitted information. Security Baseline: Moderate and High
E-1: The information system implements cryptographic mechanisms to [Selection (one or more): prevent unauthorized disclosure of information; detect changes to information] during transmission unless otherwise protected by [Assignment: organization-defined alternative physical safeguards]. Security Baseline: High
HUD Policy: 5.4.7 a. Program Offices/System Owners ensure that the integrity of the information in systems under their purview is protected during transmission. For high-impact systems, the system shall employ cryptographic mechanisms to ensure recognition of changes to information during transmission, unless adequately protected by alternate physical measures (e.g., protective distribution systems). b. Program Offices/System Owners ensure that the confidentiality of the information in systems under their purview is protected during transmission. For high-impact systems, the system shall employ cryptographic mechanisms to prevent unauthorized disclosure of information during transmission, unless otherwise protected by adequate physical measures (e.g., protective distribution systems).

5.4.8. Network Disconnect

The following policy provides guidance to ensure that HUD information systems are configured to terminate a network connection immediately and automatically following a specified period of inactivity.

NIST SP 800-53 Control: SC-10
SC-10: The information system terminates the network connection associated with a communications session at the end of the session or after [*Assignment: organization-defined time period*] of inactivity. Security Baseline: Moderate and High
HUD Policy: 5.4.8 a. The Deputy CIO for IT Operations ensures that the network connections associated with communications sessions are terminated within 10 minutes after the communication session ends or after a period of inactivity of 10 minutes. Program Offices/System Owners may request a waiver from the CISO due to documented operating requirements.

5.4.9. Cryptographic Key Establishment and Management

The following policy addresses the requirement for organizations to implement mechanisms and procedures for establishing and managing cryptographic keys.

NIST SP 800-53 Control: SC-12
SC-12: The organization establishes and manages cryptographic keys for required cryptography employed within the information system in accordance with [*Assignment: organization-defined requirements for key generation, distribution, storage, access, and destruction*]. Security Baseline: Moderate and High
E-1: The organization maintains availability of information in the event of the loss of cryptographic keys by users. Security Baseline: High
HUD Policy: 5.4.9 a. The CISO and Deputy CIO for IOO ensures cryptographic key establishment and management is done in accordance with NIST SP 800-56, *Recommendation on Key Establishment Schemes,* and NIST SP 800-57, *Recommendation on Key Management*.

5.4.10. Cryptographic Protection

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

- Secret Key Systems—also called symmetric systems; and
- Public Key Systems—also called asymmetric systems.

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

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

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

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

- Encrypt data while in storage (e.g., hard drives, diskettes, and tapes);
- Encrypt data while in transmission;
- Encrypt individual files for transmission over an unsecured medium;
- Encrypt email messages;
- Guarantee the integrity of a file or message, and detect any modifications;

- Provide the legally binding equivalent of a hand signature in digital form;
- Support non-repudiation;
- Support authentication, including strong authentication;
- Support electronic financial transactions, including electronic funds transfers, automated teller machine transactions, cash cards, gift cards, and credit cards; and
- Provide copyright protection (e.g., for DVDs).

The following policy provides guidance to ensure that HUD information systems that store sensitive information are capable of implementing a method for encrypting that information.

NIST SP 800-53 Control: SC-13
SC-13: The information system implements [Assignment: organization-defined cryptographic uses and type of cryptography required for each use] in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards. Security Baseline: Low, Moderate, and High
HUD Policy: 5.4.10 a. Program Offices/System Owners identify IT systems transmitting or storing sensitive information that may require protection based on a risk assessment. If encryption is required, the following methods are acceptable for encrypting sensitive information: • Products using triple Data Encryption Standard (3DES) or Advanced Encryption Standard (AES) algorithms that have been validated under FIPS 140-1 or FIPS 140-2 (as amended). (All new systems should use AES because it is expected that triple DES will be phased out). • Secure Sockets Layer Version 3.0 (SSL3.0) or Transport Layer Security Version 1.0 (TLS1.0). • National Security Agency (NSA) Type 2 or Type 1 encryption.

5.4.11. Collaborative Computing

The following policy provides guidance regarding the use of collaborative computing resources such as audio and video conferencing.

NIST SP 800-53 Control: SC-15
SC-15: The information system: a. Prohibits remote activation of collaborative computing devices with the following exceptions: 1. [Assignment: organization-defined exceptions where remote activation is to be allowed]; and 2. Provides an explicit indication of use to users physically present at the devices. Security Baseline: Low, Moderate, and High
E-1: The information system provides physical disconnect of camera and microphone in a manner that supports ease of use. Security Baseline: N/A
HUD Policy: 5.4.11 a. Program Offices/System Owners of moderate- or high-impact systems that use collaborative computing resources, like audio and video conferencing and electronic white boards, shall ensure that the collaborative computing resources cannot be activated remotely and provide explicit indication of use to the local user.

5.4.12. Public Key Infrastructure Certificates

A public key infrastructure (PKI) is an architecture that provides the means to bind public keys to their owners and helps in the distribution of reliable public keys in large heterogeneous networks. Public keys are bound to their owners by public key certificates. These certificates, which contain information such as the owner's name and the associated public key, are issued by a reliable certification authority (CA). A public key/private key pair is generated using the PKI. The user retains the private key. The issuing CA signs the public key, creating a public key certificate. These certificates are used by the PKI to validate a public key. Public key/private keys can be used in a public key cryptographic system to encrypt data. They also can be used to create digital signatures.

The following policy provides guidance for the selection and implementation of a PKI architecture within the HUD enterprise.

NIST SP 800-53 Control: SC-17
SC-17: The organization issues public key certificates under an [Assignment: organization-defined certificate policy] or obtains public key certificates from an approved service provider. Security Baseline: Moderate and High
HUD Policy: 5.4.12 a. The CISO, in conjunction with the Deputy CIO for IOO, selects and implements a PKI for HUD in accordance with NIST SP 800-32, *Introduction to Public Key Technology and the Federal PKI Infrastructure*. b. The CISO, in conjunction with the Deputy CIO for IOO, establishes HUD's root CA and operates under an approved Certificate Policy and Certificate Practice Statement. Any additional CAs within HUD must be subordinate to the HUD root. c. Program Offices wishing to establish their own CA shall request approval from the CISO, be a subordinate to the HUD root, and operate under an approved Certificate Policy and Certificate Practice Statement. d. The CISO shall cross-certify the HUD root CA with the Federal Bridge. The certificate policies and practice statements of CAs subordinate to the HUD root must comply with the Federal Bridge Certificate Policy. e. The CISO performs a yearly compliance audit of the root CA and all subordinate CAs. f. The CISO, in conjunction with the Deputy CIO for IOO, ensures separate public/private key pairs are used for encryption and digital signature. g. Users shall not disclose or allow the use of their private keys. If a user shares his or her private key, the user is accountable for all transactions signed with the user's private key. h. Users shall be responsible for the security of their private keys.

5.4.13. Mobile Code

Mobile (downloadable) code is software that is transmitted from a remote source across a network to a local system and then executed on that local system (e.g., personal computer, PDA, mobile phone, Internet appliance). Examples include ActiveX controls, Java applets, script run within the browser, and HTML e-mail. Although mobile code is a legitimate method for distributing application software, it is most frequently associated with "malicious mobile code" (e.g., viruses, worms, Trojan horses) that executes without the permission of or any explicit action by the local system's owner/user.

The following policy provides guidance for the use of mobile code on HUD information systems.

NIST SP 800-53 Control: SC-18
SC-18: The organization: a. Defines acceptable and unacceptable mobile code and mobile code technologies; b. Establishes usage restrictions and implementation guidance for acceptable mobile code and mobile code technologies; and c. Authorizes, monitors, and controls the use of mobile code within the information system. Security Baseline: Moderate and High
HUD Policy: 5.4.13 a. HUD employees or contractors shall not download or install mobile code (e.g., ActiveX or JavaScript) that has not been approved by the CISO.

5.4.14. Voice Over Internet Protocol

Voice over Internet Protocol (VoIP) and similar technologies move voice over digital networks using protocols that may have been originally designed for data networking rather than voice.

The following policy provides guidance for the secure implementation of Voice over Internet Protocol (VoIP) technologies in the HUD enterprise.

NIST SP 800-53 Control: SC-19
SC-19: The organization: a. 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 b. Authorizes, monitors, and controls the use of VoIP within the information system. Security Baseline: Moderate and High
HUD Policy: 5.4.14 a. Program Offices/System Owners wishing to use VoIP in information systems under their purview must obtain approval from the CISO and Deputy CIO for IOO and follow the guidance in NIST SP 800-58, *Security Considerations for VoIP Systems*.

5.4.15. Secure Name/Address Resolution Service (Authoritative Source)

The following policy provides guidance to ensure that name and address resolution services is capable of providing additional data origin and integrity artifacts.

NIST SP 800-53 Control: SC-20
SC-20: The information system: a. Provides additional data origin authentication and integrity verification artifacts along with the authoritative name resolution data the system returns in response to external name/address resolution queries; and b. Provides the means to indicate the security status of child zones and (if the child supports secure resolution services) to enable verification of a chain of trust among parent and child domains, when operating as part of a distributed, hierarchical name space. Security Baseline: Low, Moderate, and High

NIST SP 800-53 Control: SC-20
HUD Policy: 5.4.15 a. Program Offices/System Owners ensure that moderate- and high-impact systems under their purview enables remote clients to obtain origin authentication and integrity verification assurances for the name/address resolution information obtained through the service following the guidance in NIST SP 800-81, *Security Domain Name Deployment Guide*.

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

The following policy provides guidance to ensure that name and address resolution services are protected through the use of client level data authentication and integrity verification.

NIST SP 800-53 Control: SC-21
SC-21: The information system requests and performs data origin authentication and data integrity verification on the name/address resolution responses the system receives from authoritative sources. Security Baseline: Low, Moderate, and High
HUD Policy: 5.4.16 a. Program Offices/System Owners ensure that high-impact systems under their purview that provide name/address resolution service for local clients perform data origin authentication and data integrity verification on the resolution responses it receives from authoritative source when requested by client systems following the guidance in NIST SP 800-81, *Security Domain Name Deployment Guide*.

5.4.17. Architecture and Provisioning for Name/Address Resolution Service

The following policy provides guidance to ensure that name and address resolution services are protected through the use of role separation.

NIST SP 800-53 Control: SC-22
SC-22: The information systems that collectively provide name/address resolution service for an organization are fault-tolerant and implement internal/external role separation. Security Baseline: Low, Moderate, and High
HUD Policy: 5.4.17 a. Each DNS server shall have a duplicate server, one configured as primary and the other as secondary. The two servers must be located in two different network subnets and geographically separated (i.e., not located in the same physical facility). If organizational information technology resources are divided into those resources belonging to internal networks and external networks, authoritative DNS servers with two roles (internal and external) are established. The list of clients who can access the authoritative DNS server of a particular role is also specified. Follow the guidance in NIST SP 800-81, *Secure Domain Name System (DNS) Deployment Guide*.

5.4.18. Session Authenticity

The following policy provides guidance to ensure that session level protection is implemented.

NIST SP 800-53 Control: SC-23
SC-23: The information system protects the authenticity of communications sessions. Security Baseline: Moderate and High
HUD Policy: 5.4.18 a. The Deputy CIO for IOO ensures that session-level protection is implemented following the guidance in NIST SP 800-52, *Guidelines for the Selection and Use of Transport Layer Security (TLS) Implementations*, and NIST SP 800-77, *Guide to IPsec VPNs*, where needed (e.g., for service-oriented architectures providing web-based services).

5.4.19. Fail in Known State

The following policy provides guidance to ensure that session level protection is implemented.

NIST SP 800-53 Control: SC-24
SC-24: The information system fails to a [Assignment: organization-defined known-state] for [Assignment: organization-defined types of failures] preserving [Assignment: organization-defined system state information] in failure. Security Baseline: High
HUD Policy: 5.4.19 b. The Deputy CIO for IOO ensures that session-level protection is implemented following the guidance in NIST SP 800-52, *Guidelines for the Selection and Use of Transport Layer Security (TLS) Implementations*, and NIST SP 800-77, *Guide to IPsec VPNs*, where needed (e.g., for service oriented architectures providing web-based services). For high-impact systems, implement session-level protection using FIPS 140-2 (as amended) approved cryptographic modules.

5.4.20. Protection of Information at Rest

The following policy provides guidance to ensure that session level protection is implemented.

NIST SP 800-53 Control: SC-28
SC-28: The information system protects the [Selection (one or more): confidentiality; integrity] of [Assignment: organization-defined information at rest]. Security Baseline: Moderate and High
HUD Policy: 5.4.20 c. The Deputy CIO for IOO ensures that session-level protection is implemented following the guidance in NIST SP 800-52, *Guidelines for the Selection and Use of Transport Layer Security (TLS) Implementations*, and NIST SP 800-77, *Guide to IPsec VPNs*, where needed (e.g., for service oriented architectures providing web-based services). For high-impact systems, implement session-level protection using FIPS 140-2 (as amended) approved cryptographic modules.

6.0 PROGRAM MANAGEMENT

The information security program management (PM) controls complement the security controls and focus on the HUD-wide information security requirements that are independent of any particular information system and are essential for managing information security programs. HUD must document the program management controls in the *Information Security Program Plan (ISPP).* The HUD-wide Information Security Program Plan supplements the individual security plans developed for each information system. Together, the security plans for the individual information systems and the information security program cover the totality of security controls employed by the HUD organization.

6.1. Information Security Program Plan

HUD will define an organization-wide program management plan that documents the organization-wide program management controls and organization-defined common controls.

NIST SP 800-53 Control: PM-1
PM-1: The organization: a. Develops and disseminates an organization-wide Information Security Program Plan that: 1. Provides an overview of the requirements for the security program and a description of the security program management controls and common controls in place or planned for meeting those requirements; 2. Includes the identification and assignment of roles, responsibilities, management commitment, coordination among organizational entities, and compliance; 3. Reflects coordination among organizational entities responsible for the different aspects of information security (i.e., technical, physical, personnel, cyber-physical); and 4. Is approved by a senior official with responsibility and accountability for the risk being incurred to organizational operations (including mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the Nation. b. Reviews the organization-wide Information Security Program Plan [Assignment: organization-defined frequency]; c. Updates the Plan to address organizational changes and problems identified during plan implementation or security control assessments; and d. Protects the Information Security Program Plan from unauthorized disclosure and modification. Security Baseline: N/A

NIST SP 800-53 Control: PM-1
HUD Policy: 6.1.1 a. The OCIO develops, disseminates, and reviews annually a department Information Security Program Plan that: • Provides an overview of the requirements for the security program and a description of the security program management controls and common controls in place or planned for meeting those requirements. • Provides sufficient information about the program management controls and common controls (including specification of parameters for any assignment and selection operations either explicitly or by reference) to enable an implementation that is unambiguously compliant with the intent of the Plan and a determination of the risk to be incurred if the Plan is implemented as intended. • Includes roles, responsibilities, management commitment, coordination among organizational entities, and compliance. • Is approved by a senior official with responsibility and accountability for the risk being incurred to organizational operations (including mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the Nation; b. The OCIO revises the Plan to address organizational changes and problems identified during plan implementation or security control assessments.

6.2. Senior Management Security Officer

HUD will appoint a senior information security officer with the mission and resources to coordinate, develop, implement and maintain an organization-wide information security program.

NIST SP 800-53 Control: PM-2
PM-2: The organization appoints a senior information security officer with the mission and resources to coordinate, develop, implement, and maintain an organization-wide Information Security Program. Security Baseline: N/A
HUD Policy: 6.2 a. The OCIO appoints a Chief Information Security Officer (CISO) who will have the mission and resources to coordinate, develop, implement, and maintain an organization-wide Information Security Program.

6.3. Information Security Recourses

Organizations may designate and empower an Investment Review Board (or similar group) to manage and provide oversight for the information security-related aspects of the capital planning and investment control process.

NIST SP 800-53 Control: PM-3
PM-3: The organization: a. Ensures that all capital planning and investment requests include the resources needed to implement the Information Security Program and documents all exceptions to this requirement; b. Employs a Business Case/Exhibit 300/Exhibit 53 to record the resources required; and c. Ensures that information security resources are available for expenditure as planned. Security Baseline: N/A

NIST SP 800-53 Control: PM-3
HUD Policy: 6.3 a. The OCIO ensures that each capital planning and investment request includes the resources needed to implement the Information security Program and documents all exceptions to this requirement. b. The OCIO employs a Business Case (e.g., Exhibit 300, Exhibit 53) to record the resources required. c. The OCIO ensures that information security resources are available for expenditure as planned.

6.4. Plan of Action and Milestones Process

The Plan of Action and Milestones (POA&Ms) are a key document in the security authorization package and are subject to federal reporting requirements established by the Office of Management and Budget (OMB). POA&Ms updates are based on the findings from security control assessments, security impact analyses, and continuous monitoring activities. OMB FISMA reporting guidance contains instructions regarding organizational plans of action and milestones.

A Plan of Action and Milestone (POA&M) is a tool that identifies tasks that need to be accomplished to correct an identified weakness in an IT System or IT Program. It details resources required to accomplish the elements of the plan, the steps or milestones needed to accomplish the task, and the schedule for completing the milestones.

NIST SP 800-53 Control: PM-4
PM-4: The organization: a. Implements a process for ensuring that Plans of Action and Milestones for the Security Program and associated organizational information systems: 1. Are developed and maintained; 2. Document the remedial information security actions to adequately respond to risks on the organizational operations and assets, individuals, other organizations, and the Nation; and 3. Are reported in accordance with OMB FISMA reporting requirements. b. Reviews Plans of Action and Milestones for consistency with the organizational risk management strategy and organization-wide priorities for risk response actions. Security Baseline: N/A
HUD Policy 6.4 a. The OITS develops, implements, and manages a process for ensuring that Plans of Action and Milestones (POA&Ms) for the Security Program and the associated HUD information systems are maintained, and document the remedial information security actions to mitigate risk to organizational operations and assets, individuals, other organizations, and the Nation.

6.5. Information System Inventory

The organization develops and maintains an inventory of its information systems. This control addresses the inventory requirements in FISMA. OMB provides guidance on developing information systems inventories and associated reporting requirements.

NIST SP 800-53 Control: PM-5
PM-5: The organization develops and maintains an inventory of its information systems. Security Baseline: N/A

NIST SP 800-53 Control: PM-5
HUD Policy 6.5 a. The OCIO develops and maintains a comprehensive inventory of information systems and relevant security information for those systems. The authoritative inventory is HUD's Inventory of Automated Systems (IAS) and is the central reporting of information on applications (or systems) which supports business areas within the Department. The authoritative source for detailed security information is CSAM.

6.6. Information Security Measures of Performance

The organization measures the effectiveness or efficiency of the information security program and the security controls employed in support of the program.

NIST SP 800-53 Control: PM-6
PM-6: The organization develops, monitors, and reports on the results of information security measure of performance. Security Baseline: N/A
HUD Policy 6.6 a. The OCIO develops, defines, monitors, and reports on the results of information security measures of performance, which are the outcome-based metrics to measure/evaluate the effectiveness or efficiency of the Information Security Program and the security controls employed in support of the program.

6.7. Enterprise Architecture

To ensure that security is appropriately addressed throughout business activities, HUD developed a business-driven, risk-aware, Enterprise Security Architecture (ESA) that identifies the major security processes that support implementation of sound security practices and the components that are affected by these processes. The basic framework for the ESA covers external security drivers, security governance, security strategy and risk management, security operations, periodic reviews and continuous monitoring.

NIST SP 800-53 Control: PM-7
PM-7: The organization develops an enterprise architecture with consideration for information security and the resulting risk to organizational operations, organizational assets, individuals, other organizations, and the Nation. Security Baseline: N/A
HUD Policy 6.7 a. The OCIO develops an enterprise architecture with consideration for information security and the resulting risk to organizational operations, organizational assets, individuals, other organizations. b. The OITS maintains the Network Security Architecture in coordination with the Deputy CIO for IOO.

6.8. Critical Infrastructure Plan

The organization defines critical infrastructure and key resources that are outlined in a critical infrastructure plan.

NIST SP 800-53 Control: PM-8
PM-8: The organization addresses information security issues in the development, documentation, and updating of a critical infrastructure and key resources protection plan. Security Baseline: N/A
HUD Policy 6.8 a. The OCIO addresses information security issues in the development, documentation, and updating of a Critical Infrastructure and Key Resources Protection Plan. b. The Critical Infrastructure and Key Resources Protection Plan shall be consistent with applicable Federal laws, Executive Orders, Directives, policies, regulations, standards, and guidance.

6.9. Risk Management Strategy

The organization develops a Risk Management Strategy that includes an unambiguous expression of the risk tolerance for the organization, acceptable risk assessment methodologies, risk mitigation strategies, a process for consistently evaluating risk across the organization with respect to the organization's risk tolerance, and approaches for monitoring risk over time.

NIST SP 800-53 Control: PM-9
PM-9: The organization: a. Develops a comprehensive strategy to manage risk to organizational operations and assets, individuals, other organizations, and the Nation associated with the operation and use of information systems; b. Implements the Risk Management Strategy consistently across the organization; and c. Reviews and updates the Risk Management Strategy [Assignment: organization-defined frequency] or as required, to address organizational changes. Security Baseline: N/A
HUD Policy 6.9 a. The OCIO develops a comprehensive strategy to manage risk to organizational operations and assets, individuals, other organizations, and the Nation associated with the operation and use of information systems. b. The OCIO implements the Risk Management Strategy consistently across the organization. The Risk Management Strategy shall include, but not be limited to the following: • An unambiguous expression of the risk tolerance for the organization; • Acceptable risk assessment methodologies; • Risk mitigation strategies; • A process for consistently evaluating risk across the organization with respect to the organization's risk tolerance; and • Approaches for monitoring risk over time.

6.10. Security Authorization Process

The security authorization process for information systems requires the implementation of the Risk Management Framework (RMF) and the employment of associated security standards and guidelines. Specific roles within the Risk Management Process include a designated authorizing official for each organizational information system.

NIST SP 800-53 Control: PM-10
PM-10: The organization: a. Manages (i.e., documents, tracks, and reports) the security state of organizational information systems and the environments in which those systems operate through security authorization processes; b. Designates individuals to fulfill specific roles and responsibilities within the organizational risk management process; and c. Fully integrates the security authorization processes into an organization-wide risk management program. Security Baseline: N/A
HUD Policy: 6.10 a. Program Offices/System Owners manage (i.e., documents, tracks, and reports) the security state of organizational information systems through security authorization processes. b. Program Offices/System Owners designate individuals to fulfill specific roles and responsibilities within the organizational risk management process; and c. The OCIO fully integrates the security authorization processes into an organization-wide Risk Management Program.

6.11. Mission/Business Process Definition

NIST SP 800-53 Control: PM-11
PM-11: The organization: a. Defines mission/business processes with consideration for information security and the resulting risk to organizational operations, organizational assets, individuals, other organizations, and the Nation; and b. Determines information protection needs arising from the defined mission/business processes and revises the processes as necessary, until achievable protection needs are obtained. Security Baseline: N/A
HUD Policy 6.11 a. HUD defines mission/business processes with consideration for information security and the resulting risk to organizational operations, organizational assets, individuals, other organizations, and the Nation. b. HUD determines information protection needs arising from the defined mission/business processes and revises the processes as necessary, until an achievable set of protection needs is obtained.

6.12. Insider Threat Program

NIST SP 800-53 Control: PM-12
PM-12: The organization implements an insider threat program that includes a cross-discipline insider threat incident handling team. Security Baseline: N/A
HUD Policy 6.12 a. The OCIO ensures that the HUD-CIRT implements an insider threat program that includes a cross-discipline insider threat incident handling team.

6.13. Information Security Workforce

NIST SP 800-53 Control: PM-13
PM-13: The organization establishes an information security workforce development and improvement program. Security Baseline: N/A
HUD Policy 6.13 a. The Office of Information Security establishes an information security workforce development and improvement program for the HUD organization.

6.14. Testing, Training, and Monitoring

NIST SP 800-53 Control: PM-14
PM-14: The organization: a. Implements a process for ensuring that organizational plans for conducting security testing, training, and monitoring activities associated with organizational information systems: 1. Are developed and maintained; and 2. Continue to be executed in a timely manner; b. Reviews testing, training, and monitoring plans for consistency with the organizational risk management strategy and organization-wide priorities for risk response actions. Security Baseline: N/A
HUD Policy 6.14 The CISO ensures that the Office of Information Security: a. Implements a process for ensuring that HUD plans for conducting security testing, training, and monitoring activities associated with HUD information systems: 1. Are developed and maintained; and 2. Continue to be executed in a timely manner; b. Reviews testing, training, and monitoring plans for consistency with the HUD organization risk management strategy and HUD-wide priorities for risk response actions.

7.0 PRIVACY CONTROLS

The HUD organization cannot have effective privacy without a basic foundation of information security. Privacy is more than security and includes the principles of transparency, notice, and choice.

This section provides a structured set of controls for protecting privacy and serves as a roadmap for the HUD organization to use in identifying and implementing privacy controls concerning the entire life cycle of Personally Identifiable Information (PII), whether in paper or electronic form. The security controls focus on information privacy as a value distinct from, but highly interrelated with, information security. Privacy controls are the administrative, technical, and physical safeguards employed within organizations to protect and ensure the proper handling of PII.

7.1. Authority and Purpose

7.1.1. Authority to Collect

NIST SP 800-53 Control: AP-1
AP-1: The organization determines and documents the legal authority that permits the collection, use, maintenance, and sharing of personally identifiable information (PII), either generally or in support of a specific program or information system need. Security Baseline: N/A
HUD Policy 7.1.1 a. The HUD Chief Privacy Officer must determine and document the legal authority that permits the collection, use, maintenance, and sharing of personally identifiable information (PII) for each information system.

7.1.2. Purpose Specification

NIST SP 800-53 Control: AP-2
AP-2: The organization describes the purpose(s) for which personally identifiable information (PII) is collected, used, maintained, and shared in its privacy notices. Security Baseline: N/A
HUD Policy 7.1.2 b. The Chief Privacy Officer must document the purpose(s) for which personally identifiable information (PII) is collected, used, maintained, and shared in its privacy notices.

7.2. Accountability, Audit, and Risk Management

7.2.1. Governance and Privacy Program

NIST SP 800-53 Control: AR-1
AR-1: The organization: a. Appoints a Senior Agency Official for Privacy (SAOP)/Chief Privacy Officer (CPO) accountable for developing, implementing, and maintaining an organization-wide Governance and Privacy Program to ensure compliance with all applicable laws and regulations regarding the collection, use, maintenance, sharing, and disposal of personally identifiable information (PII) by programs and information systems; b. Monitors federal privacy laws and policy for changes that affect the Privacy Program; c. Allocates [Assignment: organization-defined allocation of budget and staffing] sufficient resources to implement and operate the organization-wide Privacy Program; d. Develops a strategic organizational Privacy Plan for implementing applicable privacy controls, policies, and procedures; e. Develops, disseminates, and implements operational privacy policies and procedures that govern the appropriate privacy and security controls for programs, information systems, or technologies involving PII; and f. Updates the Privacy Plan, policies, and procedures [Assignment: organization-defined frequency, at least biennially]. Security Baseline: N/A
HUD Policy 7.2.1 a. The HUD CIO appoints a Senior Agency Official for Privacy (SAOP)/Chief Privacy Officer (CPO) accountable for developing, implementing, and maintaining an HUD-wide Governance and Privacy Program to ensure compliance with all applicable laws and regulations regarding the collection, use, maintenance, sharing, and disposal of personally identifiable information (PII) by programs and information systems. The Chief Privacy Officer monitors Federal privacy laws and policy for changes that affect the privacy program. c. The HUD CIO allocates sufficient resources to implement and operate the HUD-wide Privacy Program. d. The Chief Privacy Officer develops a strategic HUD-wide Privacy Plan for implementing applicable privacy controls, policies, and procedures. e. The Chief Privacy Officer develops, disseminates, and implements operational privacy policies and procedures that govern the appropriate privacy and security controls for programs, information systems, or technologies involving PII. f. The Chief Privacy Officer updates the Privacy Plan, policies, and procedures *at* least biennially.

7.3. Privacy Impact and Risk Assessment

NIST SP 800-53 Control: AR-2
AR-2: The organization: a. Documents and implements a privacy risk management process that assesses privacy risk to individuals resulting from the collection, sharing, storing, transmitting, use, and disposal of personally identifiable information (PII); and b. Conducts Privacy Impact Assessments (PIAs) for information systems, programs, or other activities that pose a privacy risk in accordance with applicable law, OMB policy, or any existing organizational policies and procedures. Security Baseline: N/A

NIST SP 800-53 Control: AR-2
HUD Policy 7.3 a. The Chief Privacy Officer documents and implements a privacy risk management process that assesses privacy risk to individuals resulting from the collection, sharing, storing, transmitting, use, and disposal of personally identifiable information (PII). b. The Chief Privacy Officer and/or ISSO conducts Privacy Impact Assessments (PIAs) for information systems, programs, or other activities that pose a privacy risk in accordance with applicable Federal law, OMB policy, or any existing HUD policies and procedures.

7.4. Privacy Requirements for Contractors and Service Providers

NIST SP 800-53 Control: AR-3
AR-3: The organization: a. Establishes privacy roles, responsibilities, and access requirements for contractors and service providers; and b. Includes privacy requirements in contracts and other acquisition-related documents. Security Baseline: N/A
HUD Policy 7.4 The HUD Chief Privacy Officer : b. Establishes privacy roles, responsibilities, and access requirements for contractors and service providers. b. Includes privacy requirements in contracts and other acquisition-related documents.

7.5. Privacy Monitoring and Auditing

NIST SP 800-53 Control: AR-4
AR-4: The organization monitors and audits privacy controls and internal privacy policy [*Assignment: organization-defined frequency*] to ensure effective implementation. Security Baseline: N/A
HUD Policy 7.5 c. The HUD Chief Privacy Officer monitors and audits privacy controls and internal privacy policy on an annual basis to ensure effective implementation.

7.6. Privacy Awareness and Training

NIST SP 800-53 Control: AR-5
AR-5: The organization: a. Develops, implements, and updates a comprehensive training and awareness strategy aimed at ensuring that personnel understand privacy responsibilities and procedures; b. Administers basic privacy training [*Assignment: organization-defined frequency, at least annually*] and targeted, role-based privacy training for personnel having responsibility for personally identifiable information (PII) or for activities that involve PII [*Assignment: organization-defined frequency, at least annually*]; and c. Ensures that personnel certify (manually or electronically) acceptance of responsibilities for privacy requirements [*Assignment: organization-defined frequency, at least annually*]. Security Baseline: N/A

NIST SP 800-53 Control: AR-5
HUD Policy 7.6 The HUD Chief Privacy Officer: a. Develops, implements, and updates a comprehensive training and awareness strategy aimed at ensuring that personnel understand privacy responsibilities and procedures. b. Administers basic privacy training on an annual basis and targeted, role-based privacy training for personnel having responsibility for personally identifiable information (PII) or for activities that involve PII on an annual basis. c. Ensures that personnel certify (manually or electronically) acceptance of responsibilities for privacy requirements *at least annually*.

7.7. Privacy Reporting

NIST SP 800-53 Control: AR-6
AR-6: The organization develops, disseminates, and updates reports to the Office of Management and Budget (OMB), Congress, and other oversight bodies, as appropriate, to demonstrate accountability with specific statutory and regulatory privacy program mandates, and to senior management and other personnel with responsibility for monitoring Privacy Program progress and compliance. Security Baseline: N/A
HUD Policy 7.7 a. The HUD Chief Privacy Officer develops, disseminates, and updates reports to the Office of Management and Budget (OMB), Congress, and other oversight bodies, as appropriate, to demonstrate accountability with specific statutory and regulatory privacy program mandates, and to senior management and other personnel with responsibility for monitoring the Privacy Program progress and compliance.

7.8. Privacy-Enhanced System Design and Development

NIST SP 800-53 Control: AR-7
AR-7: The organization designs information systems to support privacy by automating privacy controls. Security Baseline: N/A
HUD Policy 7.8 a. The HUD CISO, in conjunction with the HUD Chief Privacy Officer, ensures that information systems are designed to support privacy by automating privacy controls.

7.9. Accounting of Disclosures

NIST SP 800-53 Control: AR-8
AR-8: The organization: a. Keeps an accurate accounting of disclosures of information held in each system of records under its control, including: 1. Date, nature, and purpose of each disclosure of a record; and 2. Name and address of the person or agency to which the disclosure was made. b. Retains the accounting of disclosures for the life of the record or 5 years after the disclosure is made, whichever is longer; and c. Makes the accounting of disclosures available to the person named in the record upon request. Security Baseline: N/A
HUD Policy 7.9 The HUD Chief Privacy Officer: a. Keeps an accurate accounting of disclosures of information held in each system of records under its control, including: • Date, nature, and purpose of each disclosure of a record; and • Name and address of the person or agency to which the disclosure was made. b. Retains the accounting of disclosures for the life of the record or 5 years after the disclosure is made, whichever is longer. c. Makes the accounting of disclosures available to the person named in the record upon request.

7.10. Data Quality and Integrity

7.10.1. Data Quality

NIST SP 800-53 Control: DI-1
DI-1: The organization: a. Confirms to the greatest extent practicable upon collection or creation of personally identifiable information (PII), the accuracy, relevance, timeliness, and completeness of that information; b. Collects PII directly from the individual to the greatest extent practicable; c. Checks for, and corrects as necessary, any inaccurate or outdated PII used by its programs or systems [*Assignment: organization-defined frequency*]; and d. Issues guidelines ensuring and maximizing the quality, utility, objectivity, and integrity of disseminated information. Security Baseline: N/A
E-1: The organization requests that the individual or individual's authorized representative validate PII during the collection process. Security Baseline: N/A
E-2: The organization requests that the individual or individual's authorized representative revalidate that PII collected is still accurate [*Assignment: organization-defined frequency*]. Security Baseline: N/A

NIST SP 800-53 Control: DI-1
HUD Policy 7.10.1 The HUD Chief Privacy Officer: a. Confirms to the greatest extent practicable upon collection or creation of personally identifiable information (PII), the accuracy, relevance, timeliness, and completeness of that information. b. Collects PII directly from the individual to the greatest extent practicable. c. Checks for and corrects, as necessary, any inaccurate or outdated PII used by its Programs or systems annually. d. Issues guidelines ensuring and maximizing the quality, utility, objectivity, and integrity of disseminated information.

7.10.2. Data Integrity and Data Integrity Board

NIST SP 800-53 Control: DI-2
DI-2: The organization: a. Documents processes to ensure the integrity of personally identifiable information (PII) through existing security controls; and b. Establishes a Data Integrity Board when appropriate to oversee organizational Computer Matching Agreements123 and to ensure that those agreements comply with the computer matching provisions of the Privacy Act. Security Baseline: N/A
E-1: The organization publishes Computer Matching Agreements on its public website. Security Baseline: N/A
HUD Policy 7.10.2 The HUD Chief Privacy Officer: a. Documents processes to ensure the integrity of personally identifiable information (PII) through existing security controls. b. Establishes a *Data Integrity Board* when appropriate to oversee organizational *Computer Matching Agreements* and to ensure that those agreements comply with the computer matching provisions of the Privacy Act.

7.11. Data Minimization and Retention

7.11.1. Minimization of Personally Identifiable Information

NIST SP 800-53 Control: DM-1
DM-1: The organization: a. Identifies the minimum personally identifiable information (PII) elements that are relevant and necessary to accomplish the legally authorized purpose of collection; b. Limits the collection and retention of PII to the minimum elements identified for the purposes described in the notice and for which the individual has provided consent; and c. Conducts an initial evaluation of PII holdings and establishes and follows a schedule for regularly reviewing those holdings at least annually to ensure that only PII identified in the notice is collected and retained, and that the PII continues to be necessary to accomplish the legally authorized purpose. Security Baseline: N/A

NIST SP 800-53 Control: DM-1
E-1: The organization, where feasible and within the limits of technology, locates and removes/redacts specified PII and/or uses anonymization and de-identification techniques to permit use of the retained information while reducing its sensitivity and reducing the risk resulting from disclosure. Security Baseline: N/A
HUD Policy 7.11.1 The HUD Chief Privacy Officer: a. Identifies the minimum personally identifiable information (PII) elements that are relevant and necessary to accomplish the legally authorized purpose of collection. b. Limits the collection and retention of PII to the minimum elements identified for the purposes described in the notice and for which the individual has provided consent. c. Conducts an initial evaluation of PII holdings and establishes and follows a schedule for regularly reviewing those holdings on an annual basis to ensure that only PII identified in the notice is collected and retained, and that the PII continues to be necessary to accomplish the legally authorized purpose.

7.11.2. Data Retention and Disposal

NIST SP 800-53 Control: DM-2
DM-2: The organization: a. Retains each collection of personally identifiable information (PII) for [*Assignment: organization-defined time period*] to fulfill the purpose(s) identified in the notice or as required by law; b. Disposes of, destroys, erases, and/or anonymizes the PII, regardless of the method of storage, in accordance with a NARA-approved record retention schedule and in a manner that prevents loss, theft, misuse, or unauthorized access; and c. Uses [*Assignment: organization-defined techniques or methods*] to ensure secure deletion or destruction of PII (including originals, copies, and archived records). Security Baseline: N/A
E-1: The organization, where feasible, configures its information systems to record the date PII is collected, created, or updated and when PII is to be deleted or archived under an approved record retention schedule. Security Baseline: N/A
HUD Policy 7.11.2 The HUD Chief Privacy Officer: a. Retains each collection of personally identifiable information (PII) to fulfill the purpose(s) identified in the notice or as required by law. b. Disposes of, destroys, erases, and/or anonymizes the PII, regardless of the method of storage, in accordance with a NARA-approved record retention schedule and in a manner that prevents loss, theft, misuse, or unauthorized access. c. Uses HUD-approved sanitization mechanisms to ensure secure deletion or destruction of PII (including originals, copies, and archived records).

7.11.3. Minimization of PII Used in Testing, Training, and Research

NIST SP 800-53 Control: DM-3
DM-3: The organization: a. Develops policies and procedures that minimize the use of personally identifiable information (PII) for testing, training, and research; and b. Implements controls to protect PII used for testing, training, and research. Security Baseline: N/A
E-1: The organization, where feasible, uses techniques to minimize the risk to privacy of using PII for research, testing, or training. Security Baseline: N/A
HUD Policy 7.11.3 The HUD Chief Privacy Officer: a. Develops policies and procedures that minimize the use of personally identifiable information (PII) for testing, training, and research. b. Implements controls to protect PII used for testing, training, and research.

7.12. Individual Participation and Redress

7.12.1. Consent

NIST SP 800-53 Control: IP-1
IP-1: The organization: a. Provides means, where feasible and appropriate, for individuals to authorize the collection, use, maintaining, and sharing of personally identifiable information (PII) prior to its collection; b. Provides appropriate means for individuals to understand the consequences of decisions to approve or decline the authorization of the collection, use, dissemination, and retention of PII; c. Obtains consent, where feasible and appropriate, from individuals prior to any new uses or disclosure of previously collected PII; and d. Ensures that individuals are aware of and, where feasible, consent to all uses of PII not initially described in the public notice that was in effect at the time the organization collected the PII. Security Baseline: N/A
E-1: The organization implements mechanisms to support itemized or tiered consent for specific uses of data. Security Baseline: N/A
HUD Policy 7.12.1 The HUD Chief Privacy Officer: a. Provides means, where feasible and appropriate, for individuals to authorize the collection, use, maintaining, and sharing of personally identifiable information (PII) prior to its collection. b. Provides appropriate means for individuals to understand the consequences of decisions to approve or decline the authorization of the collection, use, dissemination, and retention of PII. c. Obtains consent, where feasible and appropriate, from individuals prior to any new uses or disclosure of previously collected PII. d. Ensures that individuals are aware of and, where feasible, consent to all uses of PII not initially described in the public notice that was in effect at the time the organization collected the PII.

7.12.2. Individual Access

NIST SP 800-53 Control: IP-2
IP-2: The organization: a. Provides individuals the ability to have access to their personally identifiable information (PII) maintained in its system(s) of records; b. Publishes rules and regulations governing how individuals may request access to records maintained in a Privacy Act System of Records; c. Publishes access procedures in System of Records Notices (SORNs); and d. Adheres to Privacy Act requirements and OMB policies and guidance for the proper processing of Privacy Act requests. Security Baseline: N/A
HUD Policy 7.12.2 The HUD Chief Privacy Officer: a. Provides individuals the ability to have access to their personally identifiable information (PII) maintained in its system(s) of records. b. Publishes rules and regulations governing how individuals may request access to records maintained in a Privacy Act System of Records. c. Publishes access procedures in System of Records Notices (SORNs). d. Adheres to Privacy Act requirements and OMB policies and guidance for the proper processing of Privacy Act requests.

7.12.3. Redress

NIST SP 800-53 Control: IP-3
IP-3: The organization: a. Provides a process for individuals to have inaccurate personally identifiable information (PII) maintained by the organization corrected or amended, as appropriate; and b. Establishes a process for disseminating corrections or amendments of the PII to other authorized users of the PII, such as external information-sharing partners and, where feasible and appropriate, notifies affected individuals that their information has been corrected or amended. Security Baseline: N/A
HUD Policy 7.12.3 The HUD Chief Privacy Officer: a. Provides a process for individuals to have inaccurate personally identifiable information (PII) maintained by the organization corrected or amended, as appropriate. b. Establishes a process for disseminating corrections or amendments of the PII to other authorized users of the PII, such as external information-sharing partners and, where feasible and appropriate, notifies affected individuals that their information has been corrected or amended.

7.12.4. Complaint Management

NIST SP 800-53 Control: IP-4
IP-4: The organization implements a process for receiving and responding to complaints, concerns, or questions from individuals about the organizational privacy practices. Security Baseline: N/A

NIST SP 800-53 Control: IP-4
E-1: The organization responds to complaints, concerns, or questions from individuals within [*Assignment: organization-defined time period*]. Security Baseline: N/A
HUD Policy 7.12.4 The HUD Chief Privacy Officer implements a process for receiving and responding to complaints, concerns, or questions from individuals about the HUD privacy practices.

7.13. Security

7.13.1. Inventory of Personally Identifiable Information

NIST SP 800-53 Control: SE-1
SE-1: The organization: a. Establishes, maintains, and updates [*Assignment: organization-defined frequency*] an inventory that contains a listing of all programs and information systems identified as collecting, using, maintaining, or sharing personally identifiable information (PII); and b. Provides each update of the PII inventory to the CIO or information security official [*Assignment: organization-defined frequency*] to support the establishment of information security requirements for all new or modified information systems containing PII. Security Baseline: N/A
HUD Policy 7.13.1 The HUD Chief Privacy Officer: a. Establishes, maintains, and updates annually an inventory that contains a listing of all Programs and information systems identified as collecting, using, maintaining, or sharing personally identifiable information (PII). b. Provides each update of the PII inventory to the CIO or information security official annually to support the establishment of information security requirements for all new or modified information systems containing PII.

7.13.2. Privacy Incident Response

NIST SP 800-53 Control: SE-2
SE-2: The organization: a. Develops and implements a Privacy Incident Response Plan; and b. Provides an organized and effective response to privacy incidents in accordance with the organizational Privacy Incident Response Plan. Security Baseline: N/A
HUD Policy 7.13.2 The HUD Chief Privacy Officer: a. Develops and implements a HUD Privacy Incident Response Plan. b. Provides an organized and effective response to privacy incidents in accordance with the HUD Privacy Incident Response Plan.

7.14. Transparency

7.14.1. Privacy Notice

NIST SP 800-53 Control: TR-1
TR-1: The organization: a. Provides effective Notice to the public and to individuals regarding: (i) its activities that impact privacy, including its collection, use, sharing, safeguarding, maintenance, and disposal of personally identifiable information (PII); (ii) authority for collecting PII; (iii) the choices, if any, individuals may have regarding how the organization uses PII and the consequences of exercising or not exercising those choices; and (iv) the ability to access and have PII amended or corrected if necessary; b. Describes: (i) the PII the organization collects and the purpose(s) for which it collects that information; (ii) how the organization uses PII internally; (iii) whether the organization shares PII with external entities, the categories of those entities, and the purposes for such sharing; (iv) whether individuals have the ability to consent to specific uses or sharing of PII and how to exercise any such consent; (v) how individuals may obtain access to PII; and (vi) how the PII will be protected; and c. Revises its public notices to reflect changes in practice or policy that affects PII or changes in its activities that impact privacy, before or as soon as practicable after the change. Security Baseline: N/A
E-1: The organization provides real-time and/or layered notice when it collects PII. Security Baseline: N/A
HUD Policy 7.14.1 The HUD Chief Privacy Officer: a. Provides effective Notice to the public and to individuals regarding: (i) its activities that impact privacy, including its collection, use, sharing, safeguarding, maintenance, and disposal of personally identifiable information (PII); (ii) authority for collecting PII; (iii) the choices, if any, individuals may have regarding how the organization uses PII and the consequences of exercising or not exercising those choices; and (iv) the ability to access and have PII amended or corrected if necessary. b. Describes: (i) the PII the HUD organization collects and the purpose(s) for which it collects that information; (ii) how the organization uses PII internally; (iii) whether the organization shares PII with external entities, the categories of those entities, and the purposes for such sharing; (iv) whether individuals have the ability to consent to specific uses or sharing of PII and how to exercise any such consent; (v) how individuals may obtain access to PII; and (vi) how the PII will be protected. c. Revises its public notices to reflect changes in practice or policy that affects PII or changes in its activities that impact privacy, before or as soon as practicable after the change.

7.14.2. System of Records Notices and Privacy Act Statements

NIST SP 800-53 Control: TR-2
TR-2: The organization: a. Publishes System of Records Notices (SORNs) in the Federal Register, subject to required oversight processes, for systems containing personally identifiable information (PII); b. Keeps SORNs current; and c. Includes Privacy Act Statements on its forms that collect PII, or on separate forms that can be retained by individuals, to provide additional formal notice to individuals from whom the information is being collected. Security Baseline: N/A
E-1: The organization publishes SORNs on its public website. Security Baseline: N/A

NIST SP 800-53 Control: TR-2
HUD Policy 7.14.2 The HUD Chief Privacy Officer: a. Publishes System of Records Notices (SORNs) in the Federal Register, subject to required oversight processes, for systems containing personally identifiable information (PII). b. Keeps SORNs current and publishes SORNs on the HUD public website. c. Includes Privacy Act Statements on its forms that collect PII, or on separate forms that can be retained by individuals, to provide additional formal notice to individuals from whom the information is being collected.

7.14.3. Dissemination of Privacy Program Information

NIST SP 800-53 Control: TR-3
TR-3: The organization: a. Ensures that the public has access to information about its privacy activities and is able to communicate with its Senior Agency Official for Privacy (SAOP)/Chief Privacy Officer (CPO); and b. Ensures that its privacy practices are publicly available through organizational websites or otherwise. Security Baseline: N/A
HUD Policy 7.14.3 The CIO: a. Ensures that the public has access to information about its privacy activities and is able to communicate with its HUD Chief Privacy Officer. b. Ensures that its privacy practices are publicly available through organizational websites or otherwise.

7.15. Use Limitation

7.15.1. Internal Use

NIST SP 800-53 Control: UL-1
UL-1: The organization uses personally identifiable information (PII) internally only for the authorized purpose(s) identified in the Privacy Act and/or in public notices. Security Baseline: N/A
HUD Policy 7.15.1 a. HUD only uses personally identifiable information (PII) internally only for the authorized purpose(s) identified in the Privacy Act and/or in public notices.

7.15.2. Information Sharing with Third Parties

NIST SP 800-53 Control: UL-2
UL-2: The organization: a. Shares personally identifiable information (PII) externally, only for the authorized purposes identified in the Privacy Act and/or described in its notice(s) or for a purpose that is compatible with those purposes; b. Where appropriate, enters into Memoranda of Understanding, Memoranda of Agreement, Letters of Intent, Computer Matching Agreements, or similar agreements, with third parties that specifically describe the PII covered and specifically enumerate the purposes for which the PII may be used; c. Monitors, audits, and trains its staff on the authorized sharing of PII with third parties and on the consequences of unauthorized use or sharing of PII; and d. Evaluates any proposed new instances of sharing PII with third parties to assess whether the sharing is authorized and whether additional or new public notice is required. Security Baseline: N/A
HUD Policy 7.15.2 The HUD Chief Privacy Officer: a. Shares personally identifiable information (PII) externally, only for the authorized purposes identified in the Privacy Act and/or described in its notice(s) or for a purpose that is compatible with those purposes. b. Where appropriate, enters into Memoranda of Understanding, Memoranda of Agreement, Letters of Intent, Computer Matching Agreements, or similar agreements, with third parties that specifically describe the PII covered and specifically enumerate the purposes for which the PII may be used. c. Monitors, audits, and trains its staff on the authorized sharing of PII with third parties and on the consequences of unauthorized use or sharing of PII. d. Evaluates any proposed new instances of sharing PII with third parties to assess whether the sharing is authorized and whether additional or new public notice is required.

APPENDIX A. SECURITY CONTROL MAPPINGS

Relationship of Security Controls to Other Standards and Control Sets

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

MAPPING NIST SP 800-53 TO ISO/IEC 27001

NIST SP 800-53 CONTROLS		ISO/IEC 27001 CONTROLS	HUD Policy
AC-1	Access Control Policy and Procedures	A.5.1.1, A.5.1.2, A.6.1.1, A.6.1.2, A.6.1.3, A.8.1.1, A.10.1.1, A.10.8.1, A.11.1.1, A.11.3.3, A.11.4.1, A.11.6.1, A.11.7.1, A.11.7.2, A.12.3.2, A.15.1.1, A.15.2.1	5.2.1
AC-2	Account Management	A.8.3.3, A.11.2.1, A.11.2.2, A.11.2.4, A.11.5.2, A.11.5.5, A.11.5.6	5.2.2
AC-3	Access Enforcement	A.7.2.2, A.10.6.1, A.10.7.3, A.10.7.4, A.10.8.1 A.10.9.1, A.10.9.2, A.10.9.3, A.11.2.2, A.11.5.4, A.11.6.1, A.12.4.3, A.15.1.3	5.2.3
AC-4	Information Flow Enforcement	A.7.2.2, A.10.7.3, A.10.8.1, A.11.4.5, A.11.4.7, A.12.5.4	5.2.4
AC-5	Separation of Duties	A.10.1.3	5.2.5
AC-6	Least Privilege	A.11.2.2, A.11.4.1, A.11.4.4, A.11.5.4, A.11.6.1, A.12.4.3	5.2.6
AC-7	Unsuccessful Logon Attempts	A.11.5.1	5.2.7
AC-8	System Use Notification	A.6.2.2, A.11.5.1, A.15.1.5	5.2.8
AC-9	Previous Logon (Access) Notification	A.11.5.1	n/a
AC-10	Concurrent Session Control	None	5.2.9
AC-11	Session Lock	A.11.3.2, A.11.3.3, A.11.5.5	5.2.10
AC-12	Session Termination	A.11.5.5	5.2.11
AC-13	**Withdrawn**	---	n/a

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

NIST SP 800-53 CONTROLS		ISO/IEC 27001 CONTROLS	HUD Policy
AC-14	Permitted Actions without Identification or Authentication	None	5.2.12
AC-15	**Withdrawn**	---	n/a
AC-16	Security Attributes	A.7.2.2, A.10.7.3	n/a
AC-17	Remote Access	A.10.6.1, A.10.8.1, A.10.8.5, A.11.4.1, A.11.4.2, A.11.4.6, A.11.7.1, A.11.7.2	5.2.13
AC-18	Wireless Access	A.10.6.1, A.10.8.1, A.11.4.1, A.11.4.2, A.11.4.6, A.11.7.1	5.2.14
AC-19	Access Control for Mobile Devices	A.9.2.5, A.10.4.1, A.10.7.3, A.11.4.3, A.11.4.6, A.11.7.1	5.2.15
AC-20	Use of External Information Systems	A.6.2.1, A.7.1.3, A.9.2.5, A.10.6.1, A.10.8.1, A.11.4.1, A.11.4.2, A.11.4.6	5.2.16
AC-21	Information Sharing	None	5.2.17
AC-22	Publicly Accessible Content	A.10.9.3, A.11.6.1	5.2.18
AC-23	Data Mining Protection	None	n/a
AC-24	Access Control Decisions	A.11.6.1	n/a
AC-25	Reference Monitor	None	n/a
AT-1	Security Awareness and Training Policy and Procedures	A.5.1.1, A.5.1.2, A.6.1.1, A.6.1.2, A.6.1.3, A.8.1.1, A.10.1.1, A.15.1.1, A.15.2.1	4.10.1
AT-2	Security Awareness Training	A.6.2.2, A.8.2.2, A.10.4.1	4.10.2
AT-3	Role-Based Security Training	A.6.2.2, A.8.2.2, A.10.4.1	4.10.3
AT-4	Security Training Records	None	4.10.4
AT-5	**Withdrawn**	---	n/a
AU-1	Audit and Accountability Policy and Procedures	A.5.1.1, A.5.1.2, A.6.1.1, A.6.1.2, A.6.1.3, A.8.1.1, A.10.1.1, A.15.1.1, A.15.2.1, A.15.3.1	5.3.1
AU-2	Audit Events	A.10.10.1, A.10.10.2, A.10.10.4, A.10.10.5, A.11.5.4, A.15.3.1	5.3.2
AU-3	Content of Audit Records	A.10.10.1, A.10.10.2, A.10.10.4	5.3.3
AU-4	Audit Storage Capacity	A.10.3.1, A.10.10.3	5.3.4
AU-5	Response to Audit Processing Failures	A.10.3.1, A.10.10.3	5.3.5
AU-6	Audit Review, Analysis, and Reporting	A.10.10.2, A.10.10.5, A.13.1.1, A.15.1.5	5.3.6
AU-7	Audit Reduction and Report Generation	A.10.10.2, A.13.2.3	5.3.7
AU-8	Time Stamps	A.10.10.1, A.10.10.6, A.13.2.3	5.3.8
AU-9	Protection of Audit Information	A.10.10.3, A.13.2.3, A.15.1.3, A.15.3.2	5.3.9
AU-10	Non-repudiation	A.10.8.4, A.10.9.1, A.10.9.2, A.12.2.3	5.3.10
AU-11	Audit Record Retention	A.10.10.1, A.13.2.3, A.15.1.3	5.3.11
AU-12	Audit Generation	A.10.10.1, A.10.10.2, A.10.10.4, A.10.10.5	5.3.12
AU-13	Monitoring for Information Disclosure	A.12.5.4	n/a
AU-14	Session Audit	A.10.10.1	n/a
AU-15	Alternate Audit Capability	None	n/a
AU-16	Cross-Organizational Auditing	None	n/a
CA-1	Security Assessment and Authorization Policies and Procedures	A.5.1.1, A.5.1.2, A.6.1.1, A.6.1.2, A.6.1.3 A.6.1.4, A.6.1.8, A.8.1.1, A.10.1.1, A.15.1.1, A.15.2.1	3.4.1
CA-2	Security Assessments	A.6.1.8, A.6.2.2, A.10.3.2, A.13.1.2, A.15.2.1, A.15.2.2	3.4.2
CA-3	System Interconnections	A.6.2.1, A.6.2.2, A.6.2.3, A.10.6.1, A.10.6.2, A.10.8.1, A.10.8.2, A.10.8.5, A.11.4.2	3.4.3
CA-4	**Withdrawn**	---	n/a
CA-5	Plan of Action and Milestones	None	3.4.4
CA-6	Security Authorization	A.6.1.4, A.10.3.2	3.4.5

NIST SP 800-53 CONTROLS		ISO/IEC 27001 CONTROLS	HUD Policy
CA-7	Continuous Monitoring	A.6.1.8, A.12.6.1, A.13.1.2, A.15.2.1, A.15.2.2	3.4.6
CA-8	Penetration Testing	None	3.4.7
CA-9	Internal System Connections	None	3.4.8
CM-1	Configuration Management Policy and Procedures	A.5.1.1, A.5.1.2, A.6.1.1, A.6.1.2, A.6.1.3, A.8.1.1, A.10.1.1, A.12.4.1, A.12.5.1, A.15.1.1, A.15.2.1	4.5.1
CM-2	Baseline Configuration	A.10.1.2, A.10.1.4, A.12.4.1	4.5.2
CM-3	Configuration Change Control	A.10.1.2, A.10.3.2, A.12.4.1, A.12.5.1, A.12.5.2, A.12.5.3	4.5.3
CM-4	Security Impact Analysis	A.10.1.2, A.10.1.4, A.10.3.2, A.12.4.1, A.12.5.2, A.12.5.3	4.5.4
CM-5	Access Restrictions for Change	A.10.1.2, A.12.4.1, A.12.4.3, A.12.5.3	4.5.5
CM-6	Configuration Settings	A.10.10.2	4.5.6
CM-7	Least Functionality	A.11.4.1, A.11.4.4, A.11.4.6, A.12.4.1	4.5.7
CM-8	Information System Component Inventory	A.7.1.1, A.7.1.2	4.5.8
CM-9	Configuration Management Plan	A.6.1.3. A.7.1.1, A.7.1.2, A.10.1.2, A.10.1.4, A.10.3.2, A.12.4.1, A.12.4.3, A.12.5.1, A.12.5.2, A.12.5.3	4.5.9
CM-10	Software Usage Restrictions	A.12.4.1, A.15.1.2	4.5.10
CM-11	User-Installed Software	A.10.4.1, A.10.10.2, A.12.4.1, A.15.1.5	4.5.11
CP-1	Contingency Planning Policy and Procedures	A.5.1.1, A.5.1.2, A.6.1.1, A.6.1.2, A.6.1.3, A.8.1.1, A.10.1.1, A.14.1.1, A.14.1.3, A.15.1.1, A.15.2.1	4.4.1
CP-2	Contingency Plan	A.6.1.2, A.6.1.3, A.9.1.4, A.10.3.1, A.14.1.1, A.14.1.2, A.14.1.3, A.14.1.4, A.14.1.5	4.4.2
CP-3	Contingency Training	A.8.2.2	4.4.3
CP-4	Contingency Plan Testing	A.6.1.2, A.14.1.4, A.14.1.5	4.4.4
CP-5	**Withdrawn**	---	n/a
CP-6	Alternate Storage Site	A.9.1.4, A.14.1.3	4.4.5
CP-7	Alternate Processing Site	A.9.1.4, A.14.1.3	4.4.6
CP-8	Telecommunications Services	A.9.2.2, A.14.1.3	4.4.7
CP-9	Information System Backup	A.10.5.1, A.14.1.3, A.15.1.3	4.4.8
CP-10	Information System Recovery and Reconstitution	A.14.1.3	4.4.9
CP-11	Alternate Communications Protocols	A.14.1.3	n/a
CP-12	Safe Mode	None	n/a
CP-13	Alternative Security Mechanisms	A.14.1.3	n/a
IA-1	Identification and Authentication Policy and Procedures	A.5.1.1, A.5.1.2, A.6.1.1, A.6.1.2, A.6.1.3, A.8.1.1, A.10.1.1, A.15.1.1, A.15.2.1	5.1.1
IA-2	Identification and Authentication (Organizational Users)	A.10.9.1, A.10.9.2, A.11.4.2, A.11.5.1, A.11.5.2	5.1.2
IA-3	Device Identification and Authentication	A.11.4.2, A.11.4.3	5.1.3
IA-4	Identifier Management	A.11.2.1, A.11.5.2	5.1.4
IA-5	Authenticator Management	A.11.2.1, A.11.2.3, A.11.3.1, A.11.5.1, A.11.5.2, A.11.5.3	5.1.5
IA-6	Authenticator Feedback	A.11.5.1, A.11.5.3	5.1.6
IA-7	Cryptographic Module Authentication	A.15.1.6	5.1.7
IA-8	Identification and Authentication (Non-Organizational Users)	A.10.9.1, A.10.9.2, A.11.4.2, A.11.5.1, A.11.5.2	5.1.8

NIST SP 800-53 CONTROLS		ISO/IEC 27001 CONTROLS	HUD Policy
IA-9	Service Identification and Authentication	None	n/a
IA-10	Adaptive Identification and Authentication	None	n/a
IA-11	Re-authentication	A.11.5.6	n/a
IR-1	Incident Response Policy and Procedures	A.5.1.1, A.5.1.2, A.6.1.1, A.6.1.2, A.6.1.3, A.8.1.1, A.10.1.1, A.13.1.1, A.13.2.1, A.15.1.1, A.15.2.1	4.9.1
IR-2	Incident Response Training	A.8.2.2, A.10.4.1	4.9.2
IR-3	Incident Response Testing	None	4.9.3
IR-4	Incident Handling	A.6.1.2, A.6.1.6, A.13.2.1, A.13.2.2, A.13.2.3	4.9.4
IR-5	Incident Monitoring	None	4.9.5
IR-6	Incident Reporting	A.6.1.6, A.13.1.1	4.9.6
IR-7	Incident Response Assistance	A.6.1.6	4.9.7
IR-8	Incident Response Plan	A.10.4.1	4.9.8
IR-9	Information Spillage Response	None	n/a
IR-10	Integrated Information Security Analysis Team	A.13.2.2	n/a
MA-1	System Maintenance Policy and Procedures	A.5.1.1, A.5.1.2, A.6.1.1, A.6.1.2, A.6.1.3, A.8.1.1, A.10.1.1, A.15.1.1, A.15.2.1	4.6.1
MA-2	Controlled Maintenance	A.9.2.4, A.9.2.7, A.11.4.4	4.6.2
MA-3	Maintenance Tools	A.9.2.4, A.10.4.1	4.6.3
MA-4	Nonlocal Maintenance	A.9.2.4, A.11.4.4	4.6.4
MA-5	Maintenance Personnel	A.9.1.1, A.9.2.4, A.12.4.3	4.6.5
MA-6	Timely Maintenance	A.9.2.4	4.6.6
MP-1	Media Protection Policy and Procedures	A.5.1.1, A.5.1.2, A.6.1.1, A.6.1.2, A.6.1.3, A.8.1.1, A.10.1.1, A.10.7.1, A.11.1.1, A.11.3.3, A.12.3.1, A.15.1.1, A.15.1.3, A.15.2.1	4.8.1
MP-2	Media Access	A.7.2.2, A.10.7.3, A.11.3.3	4.8.2
MP-3	Media Marking	A.7.2.2, A.10.7.3, A.10.7.4	4.8.3
MP-4	Media Storage	A.10.7.1, A.10.7.4, A.11.3.3, A.15.1.3	4.8.4
MP-5	Media Transport	A.9.2.5, A.9.2.7, A.10.7.1, A.10.8.3	4.8.5
MP-6	Media Sanitization	A.9.2.6, A.10.7.1, A.10.7.2	4.8.6
MP-7	Media Use	A.10.4.1, A.10.7.1	4.8.7
MP-8	Media Downgrading	None	n/a
PE-1	Physical and Environmental Protection Policy and Procedures	A.5.1.1, A.5.1.2, A.6.1.1, A.6.1.2, A.6.1.3, A.8.1.1, A.9.1.4, A.9.1.5, A.10.1.1, A.15.1.1, A.15.2.1	4.2.1
PE-2	Physical Access Authorizations	A.8.3.3, A.9.1.2	4.2.2
PE-3	Physical Access Control	A.9.1.1, A.9.1.2, A.9.1.3, A.9.1.6, A.11.4.4	4.2.3
PE-4	Access Control for Transmission Medium	A.9.1.1, A.9.1.2, A.9.1.3, A.9.2.3	4.2.4
PE-5	Access Control for Output Devices	A.9.1.1, A.9.1.2, A.9.1.3	4.2.5
PE-6	Monitoring Physical Access	A.9.1.2, A.10.10.2	4.2.6
PE-7	**Withdrawn**	---	n/a
PE-8	Visitor Access Records	A.9.1.2, A.10.10.2	4.2.7
PE-9	Power Equipment and Cabling	A.9.1.4, A.9.2.2, A.9.2.3	4.2.8
PE-10	Emergency Shutoff	A.9.2.2	4.3
PE-11	Emergency Power	A.9.2.2	4.3.1
PE-12	Emergency Lighting	A.9.2.2	4.3.2
PE-13	Fire Protection	A.6.1.6, A.9.1.4, A.9.2.1	4.3.3
PE-14	Temperature and Humidity Controls	A.9.2.1, A.9.2.2	4.3.4
PE-15	Water Damage Protection	A.9.1.4, A.9.2.1	4.3.5

NIST SP 800-53 CONTROLS		ISO/IEC 27001 CONTROLS	HUD Policy
PE-16	Delivery and Removal	A.9.1.6, A.9.2.7	4.3.6
PE-17	Alternate Work Site	A.9.2.5, A.11.7.2	4.3.7
PE-18	Location of Information System Components	A.9.1.4, A.9.2.1	4.3.8
PE-19	Information Leakage	A.9.1.4, A.9.2.1, A.12.5.4	n/a
PE-20	Asset Monitoring and Tracking	None	n/a
PL-1	Security Planning Policy and Procedures	A.5.1.1, A.5.1.2, A.6.1.1, A.6.1.2, A.6.1.3, A.8.1.1, A.10.1.1, A.15.1.1, A.15.2.1	3.2.1
PL-2	System Security Plan	A.6.1.2	3.2.2
PL-3	**Withdrawn**	---	n/a
PL-4	Rules of Behavior	A.6.1.5, A.6.2.2, A.6.2.3, A.7.1.3. A.8.1.1, A.8.1.3, A.8.2.1, A.10.8.1, A.11.7.1, A.11.7.2, A.13.1.2, A.15.1.5	3.2.3
PL-5	**Withdrawn**	---	n/a
PL-6	**Withdrawn**	---	n/a
PL-7	Security Concept of Operations	A.12.1.1	n/a
PL-8	Information Security Architecture	A.12.1.1	3.2.4
PL-9	Central Management	None	n/a
PS-1	Personnel Security Policy and Procedures	A.5.1.1, A.5.1.2, A.6.1.1, A.6.1.2, A.6.1.3, A.8.1.1, A.10.1.1, A.15.1.1, A.15.2.1	4.1.1
PS-2	Position Risk Designation	A.8.1.1	4.1.2
PS-3	Personnel Screening	A.8.1.2	4.1.3
PS-4	Personnel Termination	A.8.3.1, A.8.3.2, A.8.3.3	4.1.4
PS-5	Personnel Transfer	A.8.3.1, A.8.3.2, A.8.3.3	4.1.5
PS-6	Access Agreements	A.6.1.5, A.6.2.3, A.7.1.3, A.8.1.1, A.8.1.3, A.8.2.1, A.10.8.1, A.11.7.1, A.11.7.2, A.15.1.5	4.1.6
PS-7	Third-Party Personnel Security	A.6.1.3, A.6.2.3, A.8.1.1, A.8.2.1	4.1.7
PS-8	Personnel Sanctions	A.8.2.3, A.15.1.5	4.1.8
RA-1	Risk Assessment Policy and Procedures	A.5.1.1, A.5.1.2, A.6.1.1, A.6.1.2, A.6.1.3, A.8.1.1, A.10.1.1, A.15.1.1, A.15.2.1	3.1.1
RA-2	Security Categorization	A.7.2.1, A.12.1.1	3.1.2
RA-3	Risk Assessment	A.6.2.1, A.12.6.1, A.14.1.2	3.1.3
RA-4	**Withdrawn**	---	n/a
RA-5	Vulnerability Scanning	A.12.6.1, A.15.2.2	3.1.4
RA-6	Technical Surveillance Countermeasures Survey	None	n/a
SA-1	System and Services Acquisition Policy and Procedures	A.5.1.1, A.5.1.2, A.6.1.1, A.6.1.2, A.6.1.3, A.8.1.1, A.10.1.1, A.12.5.5, A.15.1.1, A.15.2.1	3.3.1
SA-2	Allocation of Resources	A.6.1.2, A.10.3.1	3.3.2
SA-3	System Development Life Cycle	A.6.1.3, A.12.1.1	3.3.3
SA-4	Acquisition Process	A.10.3.2, A.12.1.1, A.12.5.5	3.3.4
SA-5	Information System Documentation	A.10.1.1, A.10.7.4, A.13.1.2, A.15.1.3	3.3.5
SA-6	**Withdrawn**	---	n/a
SA-7	**Withdrawn**	---	n/a
SA-8	Security Engineering Principles	A.10.4.2, A.12.1.1	3.3.6
SA-9	External Information System Services	A.6.1.3, A.6.1.5, A.6.2.1, A.6.2.2, A.6.2.3, A.8.2.1, A.10.2.1, A.10.2.2, A.10.2.3, A.10.6.2, A.10.8.2, A.12.5.5	3.3.7
SA-10	Developer Configuration Management	A.10.1.2, A.10.1.4, A.10.2.3, A.10.3.2, A.12.4.3, A.12.5.1, A.12.5.3, A.12.5.5	3.3.8

NIST SP 800-53 CONTROLS		ISO/IEC 27001 CONTROLS	HUD Policy
SA-11	Developer Security Testing and Evaluation	A.6.1.8, A.10.3.2, A.12.5.5, A.13.1.2	3.3.9
SA-12	Supply Chain Protections	A.12.5.5	3.3.10
SA-13	Trustworthiness	A.12.5.5	n/a
SA-14	Criticality Analysis	None	n/a
SA-15	Development Process, Standards, and Tools	A.12.4.2, A.12.5.5	3.3.11
SA-16	Developer-Provided Training	A.8.2.2	3.3.12
SA-17	Developer Security Architecture and Design	None	3.3.13
SA-18	Tamper Resistance and Detection	None	n/a
SA-19	Component Authenticity	None	n/a
SA-20	Customized Development of Critical Components	None	n/a
SA-21	Developer Screening	A.8.1.2	n/a
SA-22	Unsupported System Components	None	n/a
SC-1	System and Communications Protection Policy and Procedures	A.5.1.1, A.5.1.2, A.6.1.1, A.6.1.2, A.6.1.3, A.8.1.1, A.10.1.1, A.10.8.1, A.11.4.1, A.12.3.1, A.15.1.1, A.15.2.1	5.4.1
SC-2	Application Partitioning	A.10.4.2, A.10.9.2, A.11.4.5, A.11.5.4	5.4.2
SC-3	Security Function Isolation	A.10.4.2, A.10.9.2	5.4.3
SC-4	Information In Shared Resources	None	5.4.4
SC-5	Denial of Service Protection	A.10.3.1, A.10.6.1	5.4.5
SC-6	Resource Availability	None	n/a
SC-7	Boundary Protection	A.10.4.1, A.10.4.2, A.10.6.1, A.10.8.1, A.10.8.4, A.10.9.1, A.10.9.2, A.10.10.2, A.11.4.1, A.11.4.5, A.11.4.6, A.11.4.7, A.11.6.2	5.4.6
SC-8	Transmission Confidentiality and Integrity	A.10.6.1, A.10.8.1, A.10.8.4, A.10.9.1, A.10.9.2, A.12.2.3	5.4.7
SC-9	**Withdrawn**	---	n/a
SC-10	Network Disconnect	A.10.6.1, A.11.3.2, A.11.5.5	5.4.8
SC-11	Trusted Path	None	n/a
SC-12	Cryptographic Key Establishment and Management	A.12.3.2	5.4.9
SC-13	Cryptographic Protection	A.10.9.1, A.10.9.2, A.15.1.6	5.4.10
SC-14	**Withdrawn**	---	n/a
SC-15	Collaborative Computing Devices	A.10.8.1	5.4.11
SC-16	Transmission of Security Attributes	A.7.2.2	n/a
SC-17	Public Key Infrastructure Certificates	A.12.3.2	5.4.12
SC-18	Mobile Code	A.10.4.2, A.12.4.1	5.4.13
SC-19	Voice Over Internet Protocol	None	5.4.14
SC-20	Secure Name/Address Resolution Service (Authoritative Source)	A.10.6.1	5.4.15
SC-21	Secure Name/Address Resolution Service (Recursive or Caching Resolver)	A.10.6.1	5.4.16

NIST SP 800-53 CONTROLS		ISO/IEC 27001 CONTROLS	HUD Policy
SC-22	Architecture and Provisioning for Name/Address Resolution Service	A.10.6.1	5.4.17
SC-23	Session Authenticity	None	5.4.18
SC-24	Fail in Known State	None	5.4.19
SC-25	Thin Nodes	None	n/a
SC-26	Honeypots	None	n/a
SC-27	Platform-Independent Applications	None	n/a
SC-28	Protection of Information at Rest	None	5.4.20
SC-29	Heterogeneity	None	n/a
SC-30	Concealment and Misdirection	None	n/a
SC-31	Covert Channel Analysis	A.12.5.4	n/a
SC-32	Information System Partitioning	A.11.6.2	n/a
SC-33	**Withdrawn**	---	n/a
SC-34	Non-Modifiable Executable Programs	None	n/a
SC-35	Honeyclients	None	n/a
SC-36	Distributed Processing and Storage	None	n/a
SC-37	Out-of-Band Channels	None	n/a
SC-38	Operations Security	A.12.5.4	n/a
SC-39	Process Isolation	None	n/a
SC-40	Wireless Link Protection	None	n/a
SC-41	Port and I/O Device Access	None	n/a
SC-42	Sensor Capability and Data	A.10.4.1	n/a
SC-43	Usage Restrictions	A.11.5.6	n/a
SC-44	Detonation Chambers	A.10.8.4	n/a
SI-1	System and Information Integrity Policy and Procedures	A.5.1.1, A.5.1.2, A.6.1.1, A.6.1.2, A.6.1.3, A.8.1.1, A.10.1.1, A.10.4.1, A.15.1.1, A.15.2.1	4.7.1
SI-2	Flaw Remediation	A.12.6.1, A.13.1.2	4.7.2
SI-3	Malicious Code Protection	A.10.4.1, A.10.9.3	4.7.3
SI-4	Information System Monitoring	A.10.9.3, A.10.10.2, A.10.10.3, A.15.3.1	4.7.4
SI-5	Security Alerts, Advisories, and Directives	A.6.1.6, A.6.1.7, A.10.4.1, A.10.9.3, A.12.6.1, A.13.1.2	4.7.5
SI-6	Security Function Verification	A.10.10.2, A.10.10.6, A.12.2.2	4.7.6
SI-7	Software, Firmware, and Information Integrity	A.10.4.1, A.10.9.3, A.10.10.2, A.12.2.2, A.12.2.3, A.12.4.1	4.7.7
SI-8	Spam Protection	None	4.7.8
SI-9	**Withdrawn**	---	n/a
SI-10	Information Input Validation	A.10.7.3, A.10.9.3, A.12.2.1, A.12.2.2	4.7.9
SI-11	Error Handling	None	4.7.10
SI-12	Information Handling and Retention	A.10.7.3, A.15.1.3, A.15.1.4	4.7.11
SI-13	Predictable Failure Prevention	None	n/a
SI-14	Non-Persistence	None	n/a
SI-15	Information Output Filtering	A.12.2.4	n/a
SI-16	Memory Protection	None	n/a
SI-17	Fail-Safe Procedures	None	n/a
PM-1	Information Security Program Plan	A.5.1.1, A.5.1.2, A.6.1.1, A.6.1.2, A.6.1.3	6.1.1
PM-2	Senior Information Security Officer	A.6.1.1, A.6.1.2, A.6.1.3	6.2

NIST SP 800-53 CONTROLS		ISO/IEC 27001 CONTROLS	HUD Policy
PM-3	Information Security Resources	A.6.1.1	6.3
PM-4	Plan of Action and Milestones Process	None	6.4
PM-5	Information System Inventory	A.7.1.1, A.7.1.2	6.5
PM-6	Information Security Measures of Performance	None	6.6
PM-7	Enterprise Architecture	None	6.7
PM-8	Critical Infrastructure Plan	None	6.8
PM-9	Risk Management Strategy	A.6.1.8, A.6.2.1, A.14.1.2	6.9
PM-10	Security Authorization Process	A.6.1.3, A.6.1.4	6.10
PM-11	Mission/Business Process Definition	None	6.11
PM-12	Insider Threat Program	None	6.12
PM-13	Information Security Workforce	A.8.2.2	6.13
PM-14	Testing, Training, and Monitoring	A.8.2.2	6.14
PM-15	Contacts with Security Groups and Associations	A.6.1.7	n/a
PM-16	Threat Awareness Program	None.	n/a

APPENDIX B. Acronyms

3DES	Triple Data Encryption Standard
AC	Access Control Family
AES	Advanced Encryption Standard
ASHRAE	American Society of Heating, Refrigerating and Air-Conditioning Engineers
AT	Awareness and Training Family
ATO	Authority To Operate
AU	Audit and Accountability Family
BIA	Business Impact Analysis
CA	Certification, Accreditation, and Security Assessment Family
CAD	Computer-aided Design
CCMB	Configuration Control Management Board
CFR	Code of Federal Regulations
CIP	Critical Infrastructure Protection
CISO	Chief Information Security Officer
CM	Configuration Management Family
CMP	Configuration Management Plan
CO	Contracting Officer
COOP	Continuity of Operations
COTS	Commercial Off-the-Shelf
CP	Contingency Planning Family
CPIC	Capital Planning and Investment Control
CPO	Chief Privacy Officer
CSAM	Cyber Security Assessment and Management
DES	Data Encryption Standard
DHCP	Dynamic Host Conference Protocol
DISA	Defense Information Systems Agency
DNS	Domain Name System
EA	Enterprise Architecture
EAP	Extensible Authentication Protocol
EO	Executive Order
ESIGN	Electronic Signature in Global National Commerce Act
FAR	Federal Acquisition Regulation
FICAM	Federal Identity, Credential, and Access Management
FIPS	Federal Information Processing Standard
FISMA	Federal Information Security Management Act
GMT	Greenwich Mean Time
GPEA	Government Paperwork Elimination Act
GSS	General Support System
COR	Contracting Officer Representative
HSPD	Homeland Security Presidential Directive
HUDAR	HUD Acquisition Regulation
HUD	Department of Housing and Urban Development
HUD-CIRT	HUD Computer Incident Response Team

IA	Identification and Authentication Family
IAS	Inventory of Automated Systems
ID	Identification
IDS	Intrusion Detection System
IEEE	Institute of Electrical and Electronics Engineers
IG	Inspector General
IOO	Infrastructure and Operations Office
IR	Incident Response Family
ISA	Interconnection Security Agreement
ISPP	Information Security Program Plan
ISSO	Information System Security Officer
IT	Information Technology
LAN	Local Area Network
LMR	Land Mobile Radio
MA	Maintenance Family
MAC	Media Access Control
MBI	Minimum Background Investigations
MDM	Mobile Device Management
MOA/U	Memorandum of Agreement/Understanding
MP	Media Protection Family
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
OAMS	Office of Administration and Management Services
OCHCO	Office of the Chief Human Capital Officer
OCIO	Office of the Chief Information Officer
OGC	Office of General Counsel
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
OCRPM	Office of Customer Relations and Performance Management
OPM	Office of Personnel Management
PCS	Personal Communications Services
PDA	Personal Digital Assistant
PDS	Protective Distribution Services
PE	Physical and Environmental Protection Family
PED	Portable Electronic Devices
PIA	Privacy Impact Assessment
PII	Personally Identifiable Information
PIV	Personal Identity Verification
PKI	Public Key Infrastructure

PL	Planning Family
POA&M	Plan Of Action & Milestones
PM	Program Management, Program Plan
PS	Personnel Security Family
PTA	Privacy Threshold Analysis
RA	Risk Assessment Family
SA	System and Services Acquisition Family
SC	Systems and Communications Protection Family
SCCB	Software Configuration Control Board
SCM	Software Configuration Management
SCMP	Software Configuration Management Plan
SDM	System Development Methodology
SI	System and Information Integrity Family
SORN	System of Record Notice
SOW	Statement of Work
SP	Special Publication
SA&A	Security Assessment & Authorization
SAOP	Senior Agency Official for Privacy
SSL3.0	Secure Sockets Layer Version 3.0
SSO	Single Sign-On
SSP	System Security Plan
ST&E	Security Test & Evaluation
TCP/IP	Transmission Control Protocol/Internet Protocol
TLS1.0	Transport Layer Security Version 1.0
TRM	Technical Reference Model
TSP	Telecommunications Service Priority
UPS	Uninterrupted Power Supply
USB	Universal Serial Bus
US-CERT	United States Computer Emergency Readiness Team
USGCB	United States Government Configuration Baseline
UTC	Universal Time Coordinated
VoIP	Voice over Internet Protocol
VPN	Virtual Private Network
WAN	Wide Area Network
Wi-Fi	Wireless Fidelity
WLAN	Wireless Local Area Networks
WPAN	Wireless Personal Area Networks

APPENDIX C. Definitions

The following definitions are applicable to HUD policies and procedures.

Sensitive Information

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

FIPS 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 *low*, *moderate*, and *high* sensitivity categories and deals explicitly with integrity, availability, and confidentiality as security goals. Categories correspond to the different degrees of potential impact a security incident may have on a department's mission, assets, legal responsibilities, functions, or individuals.

Personally Identifiable Information

Personally Identifiable Information (PII) is any item, collection, or grouping of information about an individual that is maintained by an agency, including identifying information, education, financial transactions, medical history, Social Security Numbers, and criminal or employment history.

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 System	A HUD information 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	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 IOO are the System Owner for such systems.
Major Applications	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.
Minor Applications	A minor application is an information system that generally operates on an accredited general support system 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).
Mission Critical Information System	Mission-critical information systems are systems that an organization designates as critical to fulfilling its mission, including certain administrative systems.