U.S. DEPARTMENT OF HOUSING AND URBAN DEVELOPMENT

INFORMATION TECHNOLOGY SECURITY POLICY

HUD Handbook 2400.25 Rev. 5.0

8/5/2020

DOCUMENT CHANGE HISTORY

Issue	Date	Pages Affected	Description
2.0	November 2006	All	Revised to match latest draft of NIST framework and incorporate new HUD requirements.
2.1	April 2007	All	Revised to match latest draft of NIST framework and incorporate new HUD requirements.
2, CHG-2	November 2009	All	Revised to incorporate new HUD requirements.
2, CHG-2	August 2011	All	Revised to incorporate new HUD requirements.
3.0	August 2013	All	Revised to incorporate NIST SP 800-53 v3 and new HUD requirements.
4.0	March/May 2014	All	Revised to incorporate NIST SP 800-53 v4 and new HUD requirements.
4.1	March 2016	Section 3.4.4 a. Section 5.1.7 a. Section 5.4.7 a. and b	Revised the following section in response to OIG recommendations: 1) Section 3.4.4 a. 2) Section 5.1.7 a. 3) Section 5.4.7 a. and b.
4.2	November 2018	Section 3.4.2 Section 4.7.4	Revised the following section in response to Financial Statement Audit, 2018-DP-0003: 2A and 4B respectively. 1) Section 3.4.2. Security Assessments 2) Section 4.7.4 Information System Monitoring
5.0	8/5/2020	Section 1-10	Revised all sections to comply with the security and privacy requirements stated in the NIST SP 800-53, Rev. 4 publication. The handbook is revamped completely to address only policy requirements and to move all procedural details to the Security and Privacy Control Catalog.

TABLE OF CONTENTS

1. Introduction

Organizations depend on information systems to carry out their missions and business functions. The success of the missions and business functions depends on protecting the confidentiality, integrity, and availability of information processed, stored, and transmitted by those systems. The threats to information systems include equipment failure, environmental disruptions, human or machine errors, and purposeful attacks that are often sophisticated, disciplined, well-organized, and well-funded. When successful, attacks on information systems can result in serious or catastrophic damage to organizational operations and assets, individuals, other organizations, and the Nation. Therefore, it is imperative that organizations remain vigilant and that senior executives, leaders, and managers understand their responsibilities and are accountable for protecting organizational assets and for managing risk.

The E-Government Act (Public Law 107-347) in December 2002 recognized the importance of information security to the economic and national security interests of the United States. Title III of the E-Government Act, entitled the Federal Information Security Management Act (FISMA) of 2002, requires each federal agency to develop, document, and implement an agency-wide information security program to provide information security for the information and information systems that support the operations of the agency, including those provided or managed by another agency, contractor, or other source. The Federal Information Security Modernization Act (FISMA) of 2014 amended the FISMA of 2002, providing several modifications that modernize federal security and privacy practices to address evolving security concerns. One of these changes is to emphasize risk-based policy standards for federal information and information systems for cost-effective security and privacy.

The Presidential Executive Order 13800 from May 11, 2017, *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure,* also outlined actions to enhance cybersecurity across federal agencies and critical infrastructure partners, and reinforces the FISMA of 2014.

The IT Security Policy Handbook is 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 storing HUD's IT resources.

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 is referenced). 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. Guidance on HUD information security standards, methodologies, procedures, and adaptations to ongoing legislation and federal regulations and standards is expanded in the HUD *Information Technology Security Procedures Handbook 2400.25*. The procedures document provides guidance on how to implement information security and privacy policies with examples that include password enforcement mechanisms, auditing procedures, and incident-response procedures.

2. Purpose

The IT Security Policy Handbook establishes the information security policy for the Department of Housing and Urban Development (HUD). The handbook is based on federal security regulations and highlights HUD’s goals and requirements for protecting its information and information system assets. The handbook 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 handbook identifies security practices that align with HUD’s mission, provide cost-effective protection of HUD’s information and information systems, responds to security and privacy issues associated with contemporary technologies and risks, and are consistent with current applicable federal security laws, policies, and regulations.

This policy is intended to provide a set of basic protection goals and standards by providing a comprehensive view of information security and privacy considerations to all HUD components, personnel, and information systems. It addresses technical security services, as well as the management and operational requirements for information security. It identifies all relevant security and privacy 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 FISMA.

The scope of this policy handbook is as follows:

1) The policy statements in the HUD Security and Privacy Control Catalog[1] address security and privacy controls which apply solely to moderate-impact and low-impact systems.
2) The Cybersecurity Framework (CSF) Subcategories[2] (or controls) are not within the scope of this handbook. However, the CSF Subcategories are mapped to the controls within each control family in the Security and Privacy Control Catalog to provide a better overview of the control family.

3. Rescission

This policy supersedes the HUD *Information Technology Security Policy Handbook 2400.25*, Rev. 4.2, November 2018.

4. Applicability

The IT Security policy is intended to serve a diverse audience within HUD, including:

1) Individuals with system, information security, privacy, controlled unclassified information (CUI) or risk management and oversight responsibilities.
2) Employees, contractors, and service providers with system development responsibilities including, for example, system owners, program managers, systems engineers, systems security engineers, privacy engineers, software developers, systems integrators, and acquisition or procurement officials.
3) Employees, contractors, and service providers with security and privacy implementation and operations responsibilities including, for example, Program Offices, mission or business owners, system owners, information owners or stewards, system administrators, system security or privacy officers.
4) Employees, contractors, and service providers with security and privacy assessment and monitoring responsibilities including, for example, auditors, Inspectors General, system evaluators, control assessors, independent verifiers and validators, and analysts.

All IT systems owned by HUD, including IT systems operated and managed by a third-party vendor/contractor, should comply with this policy. All Program Offices shall comply with

[1] HUD Security and Privacy Control Catalog is a living document which addresses policy requirements for all twenty (20) control families listed in NIST SP 800-53, Revision 4, *Security and Privacy Controls for Information Systems and Organizations*.

[2] Cybersecurity Framework (CSF) Categories are groups of cybersecurity outcomes which can be linked to programmatic needs and associated with particular activities. Each Category contains Subcategories which make up the Cybersecurity Framework.

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 this baseline level. Additional safeguards should be based on an assessment of risk and local conditions and then implemented appropriately.

When a Program Office is unable to comply with this policy, they may request an Exception for Approval. This request is made to the Chief Information Security Officer (CISO) through the Authorizing Official (AO) and must include the operational justification, risk acceptance, and risk mitigation measures. All exception requests must be submitted in the form of a formal memorandum. Acceptable exceptions are determined by the CISO on a case-by-case basis.

5. Effective Implementation Date

The authority for the issuance of this policy rests with the Chief Information Officer (CIO) and is assigned to the Office of IT Security (OITS). The OITS serves as the central focal point for cybersecurity in HUD. This IT Security Policy Handbook is effective from the date of issuance following the clearance process.

This policy handbook will be reviewed annually from the date of issuance to assess its effectiveness and update as necessary, when implementation challenges arise, or when impacted by a significant change or underlying standard. 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 and privacy policy requirements; however, in general, the policy is free from low-level procedural and technical detail.

All updates to this policy shall be subject to the HUD-wide clearance process providing an opportunity for stakeholders to comment on the subject matter and content of the directive, such as on the implication of programmatic implementation of the proposed updates.

6. Policy

HUD information security and privacy policies are based on FISMA 2014 and the Office of Management and Budget (OMB) Circular A-130, *Managing Federal Information as a Strategic Resource*, July 28, 2016. This policy document integrates the security and privacy requirements from the Federal Information Processing Standards (FIPS) 200, *Minimum Security Requirements for Federal Information and Information Systems*, and controls that are documented in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 4, *Security and Privacy Controls for Information Systems and Organizations*, with HUD-specific requirements.

To simplify compliance with FIPS 200 and NIST SP 800-53, Rev 4, HUD policies are organized by NIST security and privacy control families. For each new control family, there is an overview and description of the family followed by high-level policy statements. Detailed policy statements for each control family are addressed in the *HUD Security and Privacy Control Catalog*.

Access Control Family

Access control is a method of guaranteeing that users are who they say they are and that they have the appropriate access to the data being sought. At a high level, access control is a selective restriction of access to data. Access control addresses user authorization to utilize an information system. It also addresses the processes and types of transactions that are allowed. Who should access HUD's data? How does HUD ensure those who attempted access have unequivocally been granted that access? Under which circumstances do you deny access to a user with access privileges?

To effectively protect its data, HUD's access control policy must address these questions. Information system access must be limited to authorized users, processes acting on behalf of authorized users, or devices (including other information systems). This promotes the least functionality paradigm by giving people, processes, or devices the most basic functionality required for completing tasks as a basic user or a privileged account holder.

HUD's access control program, at a minimum, shall:

1) Develop a policy on data exchange and interconnection security agreements (ISAs) for all HUD systems connected to external systems.
2) Ensure prevention of unauthorized access to HUD information systems and networks.
3) Employ a process to record and monitor significant changes to user accounts and groups to ensure access is not granted outside the formal HUD approval process.
4) Ensure separation of duties to prevent abuse of authorized privileges and help to reduce the risk of malevolent activity without collusion.
5) Employ least privilege for specific duties and HUD information systems to ensure that the processes operate at privilege levels no higher than necessary to accomplish required HUD missions/business functions.
6) Employ encrypted virtual private networks (VPNs) to enhance confidentiality and integrity over remote connections.

Awareness and Training Control Family

All levels of HUD management must ensure employees, contractors, vendors and other third-party entities are informed about their security responsibilities and the need to attain required continued education relevant to information security and their position within HUD and their Program Offices. Maintaining this level of due diligence ensures that key objectives of an effective Information Security Program are attained. All employees and contractors must understand their roles and responsibilities and become adequately trained to perform them, thus, ensuring the protection of the confidentiality, integrity, and availability of HUD information systems and the information they contain.

All HUD users and personnel, including contractors, with significant security responsibilities for a system must be aware of the security risks associated with their use and management of that system. This will ensure 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 by conducting Federal Workforce Assessment surveys.

HUD's awareness and training program, at a minimum, shall:

1) Ensure an up-to-date security awareness and training plan is maintained.
2) Ensure managers and users of HUD information systems are made aware of the security and privacy risks associated with their activities and of the applicable laws, Executive Orders, directives, policies, standards, instructions, regulations, and procedures related to the security of HUD information systems.
3) Ensure HUD personnel are adequately trained to carry out their assigned information security and privacy-related duties and responsibilities.
4) Ensure all employees and contractors are knowledgeable and follow best practices and protocols for managing data.
5) Ensure all employees and contractors are provided role-based security and privacy training.

Audit and Accountability Control Family

An audit is an independent review and examination of records and activities to assess the adequacy of the information system's controls, to ensure compliance with established policies and operational procedures, and to recommend necessary changes in those controls, policies, or procedures. Accountability is the principle that an individual is entrusted to safeguard and control information/data, equipment, keying material, and is accountable to management for the use/misuse or compromise of that information system or resource.

The audit and accountability control family address 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 family also serves as an insurance policy, ensuring that there are mechanisms in place to track and associate user, process, and system activity to events. Whenever there is a deviation from the prescribed mode of operation, an examination of the audit and accountability controls can serve as a launch point to determine factors that may have caused this deviation or failure.

HUD’s audit and accountability program, at a minimum, shall:

1) Develop, adopt, and adhere to a formal documented program for the monitoring, management, and review of system, application, network, and user activity.
2) Develop standards and procedures to guide the implementation and management of audit controls and records.
3) 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.
4) 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) Provide audit record generation capability for auditable events identified by HUD.

Assessment, Authorization, and Monitoring Control Family

The assessment and authorization (A&A) process is implemented to ensure compliance with federal laws and regulations and is critical to minimizing the threat of breaches. Security and privacy assessments are conducted 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 and privacy requirements for the information system. Authorization is the process of accepting the residual risks associated with the continued operation of HUD systems and granting approval to operate for a specified span of time. The Information Security Continuous Monitoring (ISCM) process is established to maintain an ongoing awareness of information security, vulnerabilities, and threats to support HUD risk management decisions.

HUD’s assessment, authorization, and monitoring program, at a minimum, shall:

1) Categorize information sensitivity in compliance with FIPS 199 as the basis for HUD’s categorization process.
2) Ensure that only authorized systems including workstations, servers, cloud computing applications, software applications, mobile devices, networks, and

data repositories have an authorization to operate (ATO) in accordance with HUD's business needs.

3) Periodically assess security and privacy controls in HUD information systems to determine if the controls are effective in their application.
4) Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in HUD information systems.
5) Authorize the operation of HUD information systems and any associated information system connections.
6) Monitor security and privacy controls on an ongoing basis to ensure the continued effectiveness of the controls.

Configuration Management Control Family

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.

The configuration of a HUD system and its components has a direct impact on the security posture of that system. Changes to the configuration of HUD systems are often needed to stay up to date with changing business functions and services, and information security needs. However, changes can adversely impact the previously established security posture; therefore, effective configuration management is vital to the establishment and maintenance of security of information and systems. The HUD security-focused configuration management process is critical to maintaining a secure state under normal operations, contingency recovery operations, and reconstitution to normal operations.

To effectively execute its configuration management policies and program, HUD, at a minimum, shall:

1) Establish and maintain baseline configurations and inventories of HUD information systems.
2) Document, implement, and maintain configuration and change management processes.
3) Establish and enforce security configuration settings for HUD IT products employed in HUD information systems.
4) Monitor and control changes to the baseline configurations and to the constituent components of HUD information systems (including the installation of patches, hardware, software, firmware, and documentation) throughout the system's development life cycles.

5) Have effective plans and be adequately staffed to ensure the ability to reverse or undo any deployment or implementation that has negatively impacted the working environment.

Contingency Planning Control Family

Contingency planning refers to interim measures to recover information systems after a disruption. Interim measures may include relocation of information systems and operations to an alternate site, recovery of information system functions using alternate equipment, or performance of information system functions using manual methods. The main goal of contingency planning is the restoration to normal modes of operation while mitigating against loss of data with minimum cost and disruption to normal business activities after an unanticipated event.

HUD must develop contingency planning processes to prepare for, detect, react to, and recover from events that threaten the security of HUD information system resources and assets. The appropriate level of IT business continuity management must be in place to sustain the operation of HUD's critical IT services to support the continuity of vital business functions and the timely delivery of critical automated business services. Appropriate planning and testing processes must be in place to ensure that, in the event of a significant business interruption, critical production environments can be recovered and sustained to meet HUD's business requirements. This policy covers mainframe, distributed environments, and cloud-hosted environments.

HUD's contingency planning program, at a minimum, shall:

1) Identify HUD's essential missions and business functions and associated contingency requirements.
2) Establish, maintain, and effectively implement plans for emergency response, backup operations, and post-disaster recovery for HUD information systems to ensure the availability of critical information resources and continuity of operations in emergency situations.
3) Test the contingency plan for all HUD systems to determine the effectiveness of the contingency plan and to identify potential weaknesses in the plans.
4) Provide contingency planning training to all system users.
5) Establish an alternate storage site to permit the storage and retrieval of HUD system backup information.

Identification and Authentication Control Family

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, public key infrastructure (PKI) certificates, key cards, biometrics, or in the case of multifactor authentication, some combination therein. The identification and authentication controls provide HUD security policy requirements for the management of user identification and authentication, which is required to safeguard access to information systems and critical business processes/resources. HUD users include employees or individuals that HUD considers having the equivalent status of employees, including contractors and third-party entities or business partners. This policy shall be implemented for identification and authentication devices requiring unique device-to-device identification and authentication.

HUD's identification and authentication program, at a minimum, shall:

1) Identify information system users, processes acting on behalf of users, or devices, and authenticate the identities of those users, processes, or devices, as a prerequisite to allowing access to HUD information systems.
2) Uniquely identify and authenticate HUD devices before establishing a remote or network connection.
3) Manage system identifiers by receiving authorization from HUD to assign an individual, group, role, or device identifier.
4) Implement mechanisms for authentication to a cryptographic module that meet the requirements of applicable laws, Executive Orders, directives, policies, regulations, standards, and guidelines for such authentication.
5) Uniquely identify and authenticate non-HUD users or processes acting on behalf of non-HUD users.

Individual Participation Control Family

The purpose of the Privacy Act of 1974 is to balance the government's need to maintain information about individuals with the rights of individuals to be protected against unwarranted invasions of their privacy stemming from federal agencies' collection, maintenance, use, and disclosure of personal information about them. Individuals are active participants in the decision-making process regarding the collection and use of their

Personally Identifiable Information (PII). The controls in this family enhance HUD’s ability to comply with the Privacy Act and the public confidence in HUD decisions made based on the PII. Each HUD user has a right to decide when and whether to share personal information, how much information to share, and the circumstances under which that information can be shared.

HUD’s privacy program, at a minimum, shall:

1) Require users to consent to the processing of their PII prior to its collection.
2) Provide mechanisms for users to redress the use of their PII residing in HUD systems.
3) Make privacy notices available to users to help them understand how their information is being processed.
4) Make available Privacy Act Statements to HUD users, including notice of the authority of HUD offices or systems to collect their PII.
5) Provide users the ability to access their PII information maintained in HUD systems of records.

Incident Response Control Family

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, HUD is required to implement and maintain a security incident reporting and handling capability.

Quickly responding to incidents provides a mechanism for controlling the impact of the incident on HUD information systems; therefore, all HUD users must understand their incident response responsibilities and the actions they should take if an incident is suspected or has occurred. To accomplish this, users require training in incident detection and response.

HUD’s incident response program managed by OITS, at a minimum, shall:

1) Establish an operational incident handling capability for HUD information systems that includes adequate preparation, detection, analysis, containment, recovery, and user response activities.
2) Track, document, and report incidents to appropriate HUD officials and authorities.

3) Conduct tests and exercises in a controlled environment to determine the effectiveness and weaknesses of HUD's incident response capability and to improve on that capability.
4) Report PII data breach(s) to the Cybersecurity and Infrastructure Security Agency (CISA) promptly.

Maintenance Control Family

Regular maintenance of information systems mitigates some of the threats to the system. The maintenance control family address policies to ensure that the systems and services used by HUD are maintained and repaired properly. Maintenance requirements apply to all types of maintenance to any system component (hardware, firmware, operating system, and applications). System maintenance also includes components not directly associated with information processing or retention, such as scanners, copiers, and printers. 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, contractors, or other federal agencies.

HUD's system maintenance program, at a minimum, shall:

1) Perform periodic and timely maintenance on HUD information systems.
2) Provide effective controls on the tools, techniques, mechanisms, and personnel used to conduct information system maintenance.
3) Schedule, document, and review records of maintenance, repair, or replacement on system components in accordance with manufacturer or vendor specifications and/or HUD requirements.
4) Employ effective maintenance tools, such as hardware/software diagnostic test equipment and hardware and software packet sniffers.
5) Establish a process for maintenance of personnel authorization and supervise the maintenance activities of personnel who do not possess the required access authorizations.
6) Obtain maintenance support and spare parts for critical systems, to support HUD-defined recovery time objectives.

Media Protection Control Family

Information resides in many forms and can be stored in different ways. Media controls are protective measures specifically designed to safeguard electronic data, the physical media they are stored on (tape, disk, flash-memory, etc.) and hardcopy information (paper, microfilm, etc.). This policy addresses the protection, marking, sanitization, production input/output, and disposal of media containing sensitive information. All levels of HUD management must ensure that employees, contractors, vendors, and other third-party entities protect information system media, both paper and digital; limit access to information on information system media to authorized users; and sanitize or destroy information system media before disposal or release for reuse.

HUD's media protection program, at a minimum, shall:

1) Limit access to information system media to authorized users.
2) Protect information system media and sanitize or destroy information system media before disposal or release for reuse.
3) Mark system media indicating the distribution limitations, handling caveats, and applicable security markings (if any) of the information.
4) Store media securely based on the information's required level of protection to prevent improper access.

Privacy Authorization Control Family

HUD's privacy program is a foundation of information security. Privacy is more than security and includes the principles of transparency, notice, and choice. The privacy authorization controls focus on ensuring that HUD managers and systems have proper authority and authorization to collect, store, and make use of privacy-related information.

HUD's privacy program, at a minimum, shall:

1) Determine and document the legal authority that permits the collection, use, maintenance, and sharing of PII in support of a specific HUD program or system need.
2) Identify and document the purpose for which PII is collected, used, maintained, and shared in its privacy notices.
3) Develop and disseminate guidelines for the sharing of PII externally.

Physical and Environmental Protection Control Family

Physical and environmental protection controls provide measures for HUD's system operational environment so that HUD systems are physically protected from threats and that an appropriate operating environment is provided. The broad scope of requirements includes physical access authorizations and access control of HUD's users and visitors, access control of communications and output devices (monitors, printers), and monitoring of access. Protections of the operating environment include protection of power equipment and power cabling, maintenance and repair, and management of emergency power, lighting, fire protection, temperature and humidity, water damage protection, and alternate worksites.

HUD's physical and environmental protection program, at a minimum, shall:

1) Limit physical access to information systems, equipment, and the respective operating environments to authorized users.
2) Protect the physical plant and support infrastructure for information systems.
3) Provide supporting utilities for information systems.
4) Protect information systems against environmental hazards.
5) Provide appropriate environmental controls in HUD facilities containing information systems.

Planning Control Family

The objective of system security planning is to improve protection of information system resources. All HUD systems have some level of sensitivity and require protection as part of good security management practice. The protection of a system must be documented in a security and privacy plan. The purpose of the security and the privacy plan is to provide an overview of the security and privacy requirements of the system and describe the controls in place or planned for meeting those requirements. The security and privacy plan also delineate responsibilities and expected behavior of all users who access HUD systems. Since the security and privacy plan establishes and documents the security and privacy controls, it should form the basis for the authorization, supplemented by the assessment report and the plan of action and milestones (POA&Ms).

HUD’s planning policy, at a minimum, shall:

1) Develop, document, periodically update, and implement security plans for HUD information systems that describe the security controls in place or planned for the information systems.
2) Develop, document, and periodically update the rules of behavior (to include data handling rules for both PII and non-PII data) for HUD users requiring access to HUD information systems.
3) Develop security and privacy architecture for HUD information systems and strategically allocate security safeguards (procedural, technical, or both) in the architecture so that adversaries must overcome multiple safeguards to achieve their objective.
4) Select control baselines for each HUD system and tailor them by applying specified tailoring actions.

Program Management Control Family

The program management policy specifies the development, implementation, assessment, authorization, and monitoring of the IT security program management. The successful implementation of security controls for HUD's data and information systems depends on the successful implementation of HUD's program management controls. As a result, the program management controls are essential for managing the IT security program.

HUD's IT security and privacy program management, at a minimum, shall:

1) Develop a comprehensive strategy to manage security risk to HUD operations and assets, individuals, other organizations, and the Nation associated with the operation and use of HUD systems.
2) Manage the security and privacy state of HUD systems and the environments in which those systems operate through authorization processes.
3) Implement an insider threat program that includes a cross-discipline insider threat incident handling team.
4) Develop, monitor, and report on the results of information security and privacy measures of performance.
5) Implement a process to ensure that POA&Ms for the security and privacy programs and associated HUD systems are developed and maintained.
6) Implement a process for ensuring that vulnerabilities are properly identified, document remediation actions and track vulnerabilities to mitigate risk to operations, assets, individuals.
7) Develop and maintain an inventory of HUD systems.

Personnel Security Control Family

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.

HUD's personnel security program, at a minimum, shall:

1) Ensure that individuals occupying positions of responsibility within HUD (including third-party service providers) are trustworthy and meet established security criteria for those positions.

2) Ensure that HUD's information and information systems are protected during and after personnel actions such as terminations and transfers.
3) Employ formal sanctions for personnel failing to comply with HUD security policies and procedures.
4) Assign position risk categorizations or designations to all personnel positions held within HUD.
5) Screen users prior to authorizing access to HUD systems.

Risk Assessment Control Family

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. This process 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. Assessing the risks to HUD's 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 risk assessment control policies ensure that there are mechanisms in place to address the identification, assessment, and mitigation of risks to information assets.

HUD's risk assessment program, at a minimum, shall:

1) Periodically assess the risk to HUD operations (including mission, functions, image, or reputation), HUD assets, and individuals, resulting from the operation of HUD information systems and the associated processing, storage, or transmission of HUD information.
2) Conduct periodic vulnerability assessments of HUD information systems to determine security risks that should be mitigated.
3) Conduct regular risk assessments of HUD information systems.
4) Conducting periodic e-authentication risk assessments.

System and Services Acquisition Control Family

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, and maintenance of HUD facilities, equipment, software, and related services or those operated by external providers of information system services on behalf of HUD.

HUD’s system and services acquisition management, at a minimum, shall:

1) Allocate resources to protect HUD information systems.
2) Employ Software Development Life Cycle (SDLC) processes that incorporate information security considerations.
3) Not use live data in any environment other than in production and disaster recovery (DR) environments nor use live data in development, testing or staging environments.
4) Employ software usage and installation restrictions.
4) Ensure that third-party providers employ adequate security measures to protect information, applications, and/or services outsourced by HUD.
5) Develop information system documentation to support the configuration baseline of HUD systems.
6) Require providers of external system services to comply with HUD’s security and privacy requirements.
7) Employ HUD’s supply chain safeguards to protect against supply chain risks to the system, system component, or system service and to limit the harm or consequences from supply chain-related events.

System and Communication Protection Control Family

System and communications protection controls ensure that system and communications protection policies and procedures are implemented to address the protection of information transmitted or received by HUD information systems. The system and communication protection control policies address implementing appropriate protection for systems and communications to include separation of functions, cryptographic key management, denial of service, and boundary protection.

HUD's system and communication protection management shall:

1) Monitor, control, and protect HUD communications (i.e., information transmitted or received by HUD information systems) at the external boundaries and key internal boundaries of the information systems.
2) Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within HUD information systems.
3) Separate user functionality, including user interface, from system management functionality.
4) Prevent unauthorized and unintended information transfer via shared system resources.

5) Monitor and control communications at the external boundary of HUD systems and at key internal boundaries within the system.

6) Provide authentication, data integrity, data confidentiality, and non-repudiation services through cryptographic key establishment and cryptographic protection.

System and Information Integrity Control Family

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.

The system and information integrity controls also refer 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. Flaws in information systems provide an opportunity for systems to be compromised. Therefore, weaknesses, particularly those related to security, must be remediated through the configuration management process.

Software is vulnerable to malicious code; it is essential that HUD provide protection against malicious code and ensure mechanisms and tools are in place to assist in this protection. Too often, vulnerabilities may be embedded in 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 system security functions are essential in the protection of HUD information assets, as it is important that these functions execute appropriately and, thus, should be verified during system startup. Information system outputs (i.e., reports, files) could be used to compromise the system or expose information that should be protected. HUD 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. External security alerts and advisories provide information to personnel prior to an incident, providing a possible opportunity to correct system vulnerabilities that might potentially compromise a system.

HUD's system and information integrity program, at a minimum, shall:

1) Identify, report, and correct information and information system flaws in a timely manner.
2) Provide protection from malicious code at appropriate locations within HUD information systems.
3) Monitor information system security alerts and advisories and take appropriate actions in response.

7. Roles and Responsibilities

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, 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 and privacy 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.

Chief Information Officer (CIO)

The CIO is responsible for the implementation of applicable IT security policies. The CIO reviews and evaluates the HUD information security program at least annually.

Authorizing Official (AO)

The AO is a senior government management official with the authority to formally assume responsibility for operating an information system at an acceptable level of risk. AOs control personnel, operations, maintenance, and budgets for their systems or field sites. Therefore, to control the resources necessary to mitigate risks for their information systems, an AO must be an Assistant Secretary, Deputy Assistant Secretary, or equivalent Senior Leader. AOs may designate, in writing, 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 security assessment and authorization (SA&A) documentation, and the determination of risk to agency operations, agency assets, and individuals. The AO cannot delegate the security accreditation decision and signing of the associated accreditation decision letter.

Chief Information Security Officer (CISO)

The CISO is responsible for the management and oversight of the HUD's information security program. The CISO, with the support of the IT security staff, establishes a strong foundation for HUD security by maintaining the HUD's information security program. The CISO interacts with internal and external resources, sponsors an information system security forum for Information System Security Officers (ISSOs), and coordinates security compliance across HUD's Program Offices. The CISO serves as the CIO's primary liaison with AOs, system owners, and ISSOs.

Chief Privacy Officer

The Privacy Officer is responsible for the development and maintenance of Privacy Act policies, procedures, and guidance essential to safeguarding the collection, access, use, dissemination, and storage of PII and Privacy Act information in accordance with the Privacy Act of 1974, the E-Government Act of 2002, the FISMA of 2014, and policy and guidance issued by the President and OMB. The Chief Privacy Officer works closely with the HUD Computer Incident Response Team (CIRT) and the General Counsel when addressing and handling incidents and data breaches involving PII. The Chief Privacy Officer also coordinates with the Office of Infrastructure and Operations (IOO) and OITS for data protection privacy issues affecting IT systems.

Information System Security Officer (ISSO)

The ISSO is responsible for ensuring that security and privacy controls are in place and effective for securing HUD system(s) belonging to the Program Office. The ISSO is the principal point of contact (POC) for the security of the designated information systems and actively participates in the information security system forum. The ISSO is responsible for all security aspects of his or her assigned systems from inception through disposal, as well as for ensuring system availability. An ISSO must be designated for every information system to serve as the POC for all security matters related to that information system.

System Owners

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 and privacy controls to ensure that they are effective in protecting the information and information systems under their purview. Moreover, system owners of major and minor applications are responsible for coordinating 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. Additionally, system owners must ensure that:

1) An ISSO is designated (in writing) for each information system under their purview.
2) Completing SA&A and continuous monitoring activities.
3) Maintaining and reporting POA&Ms.

Program Offices' Senior Executive

Each Program Office performs a specific role aimed at delivering on HUD's mission to create strong, sustainable, inclusive communities and quality affordable homes for all. Notwithstanding the specific role and services each Program Office delivers, its tasks are guided by and implemented with the use of IT; however, some offices have more security-specific and relevant roles and responsibilities from an IT perspective that must be addressed as part of a due diligent and proactive IT security policy as spearheaded by the CIO. Each Program Office is, therefore, responsible for:

1) Adhering to HUD's IT security and privacy policies and procedures.
2) Ensuring that system authorization to operate (ATO) is conducted every three years or when there is a significant change to the system.
3) Conducting risk assessments annually to identify and determine the likelihood of occurrence and the potential impact on mission success.
4) Ensuring that the security and privacy plan for each system is reviewed and updated annually and uploaded to Cybersecurity Assessment and Management (CSAM) tool.
5) Coordinating with IOO to ensure the implementation of security components to secure the shared information system assets.
6) Working closely with the Office Technical Coordinator (OTC) to address and resolve any IT requests.
7) Working closely with OITS on information security-related programs and issues.

8. Definitions

This section includes definitions associated with the terms within this policy.

WORD	DEFINITIONS
Agency	Any executive agency or department, military department, Federal Government corporation, Federal Government-controlled corporation, or other establishment in the Executive Branch of the Federal Government, or any independent regulatory agency.
Assessment	The testing or evaluation of security or privacy controls 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 an information system or organization.
Availability	Ensuring timely and reliable access to and use of information.
Confidentiality	Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.
Configuration Management	A collection of activities focused on establishing and maintaining the integrity of information technology products and systems, through control of processes for initializing, changing, and monitoring the configurations of those products and systems throughout the system development life cycle.
Controlled Unclassified Information	Controlled Unclassified Information (CUI) is information that requires safeguarding or dissemination controls pursuant to and consistent with applicable law, regulations, and government -wide policies that adhere to Executive Order 13556 which establishes a program for managing CUI across the Executive branch to ensure compliance of CUI implementation.
External System Service	A system service that is implemented outside of the authorization boundary of the organizational system (i.e., a service that is used by, but not a part of, the organizational system) and for which the organization typically has no direct control over the application of required security and privacy controls or the assessment of security and privacy control effectiveness.
Information System	A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.
Incident	An occurrence that actually or imminently jeopardizes, without lawful authority, the confidentiality, integrity, or availability of information or an information system; or constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies.

WORD	DEFINITIONS
Information	Information is stimuli that has meaning in some context for its receiver. Information is created when data are processed, interpreted, organized, structured, or presented so as to make them meaningful or useful. Information provides context for data.
Information Security	The protection of information and systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability.
Information Technology	Any services, equipment, or interconnected system(s) or subsystem(s) of equipment, that are used in the automatic acquisition, storage, analysis, evaluation, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the agency.
Integrity	Guarding against improper information modification or destruction and ensuring information non-repudiation and authenticity.
Least Privilege	The principle that a security architecture is designed so that each entity is granted the minimum system resources and authorizations that the entity needs to perform its function.
Malicious Code	Software or firmware intended to perform an unauthorized process that will have adverse impact on the confidentiality, integrity, or availability of a system. Examples include: a virus, worm, Trojan horse, or other code-based entity that infects a host. Spyware and some forms of adware are also examples of malicious code.
Network	A system implemented with a collection of interconnected components. Such components may include routers, hubs, cabling, telecommunications controllers, key distribution centers, and technical control devices.
Personally Identifiable Information	Information that can be used to distinguish or trace an individual’s identity, either alone or when combined with other information that is linked or linkable to a specific individual.
Privacy Control	The administrative, technical, and physical safeguards employed within an agency to ensure compliance with applicable privacy requirements and manage privacy risks.
Privacy Plan	A formal document that details the privacy controls selected for an information system or environment of operation that are in place or planned for meeting applicable privacy requirements and managing privacy risks, details how the controls have been implemented, and describes the methodologies and metrics that will be used to assess the controls.

WORD	DEFINITIONS
Risk	A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically is a function of: (i) the adverse impact, or magnitude of harm, that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence.
Risk Assessment	The process of identifying risks to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation, resulting from the operation of a system. Part of risk management incorporates threat and vulnerability analyses and analyses of privacy-related problems arising from information processing and considers mitigations provided by security and privacy controls planned or in place.
Risk Management	The program and supporting processes to manage risk to agency operations (including mission, functions, image, reputation), agency assets, individuals, other organizations, and the Nation, and includes establishing the context for risk-related activities; assessing risk; responding to risk once determined; and monitoring risk over time.
Security Control	The safeguards or countermeasures prescribed for an information system or an organization to protect the confidentiality, integrity, and availability of the system and its information.
Security Policy	A set of criteria for the provision of security services.
Sensitive Information	Sensitive information is data that must be protected from unauthorized access to safeguard the privacy and security of an individual or organization. Sensitive information could be Sensitive Personally Identified Information (PII) data that can be traced back to an individual and that, if disclosed, could result in harm to that person. Such information includes biometric data, medical information, personally identifiable financial information (PIFI) and unique identifiers such as passport or Social Security numbers. Another type of sensitive information could be business information that includes anything that poses a risk to the organization in question if discovered by a competitor or the general public. Such information includes trade secrets, acquisition plans, financial data and supplier and customer information, among other possibilities. The last type of sensitive information is classified information that pertains to a government body and is restricted according to level of sensitivity (for example, restricted, confidential, secret, and top secret). Information is generally classified to protect security.

WORD	DEFINITIONS
Software	Computer programs and associated data that may be dynamically written or modified during execution.
Spam	The abuse of electronic messaging systems to indiscriminately send unsolicited bulk messages.
Supply Chain	Linked set of resources and processes between multiple tiers of developers that begins with the sourcing of products and services and extends through the design, development, manufacturing, processing, handling, and delivery of products and services to the acquirer.
System	Any organized assembly of resources and procedures united and regulated by interaction or interdependence to accomplish a set of specific functions.
System Component	A discrete identifiable information technology asset that represents a building block of a system and may include hardware, software, and firmware.
Threat	Any circumstance or event with the potential to adversely impact organizational operations, organizational assets, individuals, other organizations, or the Nation through a system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service.
User	Individual, or (system) process acting on behalf of an individual, authorized to access a system.
Vulnerability Assessment	Systematic examination of an information system or product to determine the adequacy of security measures, identify security deficiencies, provide data from which to predict the effectiveness of proposed security measures, and confirm the adequacy of such measures after implementation.

9. Authorities and References

HUD established a department-wide information security policy based on the following Executive Orders, public laws and regulations, and national policies: (latest version published is referenced).

- Section 508 of the Rehabilitation Act of 1973.
- Privacy Act, Public Law 93-579, December 1974.
- Paperwork Reduction Act, Public Law 104-13, May 1995.
- Clinger-Cohen Act, Public Law 104–106, February 1996.
- Health Insurance Portability and Accountability Act (HIPAA), Public Law 104-191, August 21, 1996.
- Executive Order 13556, *Controlled Unclassified Information*.
- Government Paperwork Elimination Act, Public Law 105-277, October 1998.
- Electronic Signatures in Global and National Commerce Act (P.L. 106-229), June 2000.
- U.S. Patriot Act, Public Law 107-56, October 26, 2001.

- Electronic Government Act, Public Law 107-347, December 2002.
- Federal Information Security Modernization Act (FISMA) of 2014.
- Executive Order 13800, *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure,* May 11, 2017.
- Federal Cybersecurity Workforce Assessment Act, PL 114-113, Title III & IV, December 18, 2015.
- Office of Management and Budget (OMB), Circular A-130, *Managing Information as a Strategic Resource*, July 28, 2016.
- Office of Management and Budget (OMB), 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 (OMB), Memorandum M-04-04, *E-Authentication Guidance for Federal Agencies*, December 2003.
- Office of Management and Budget (OMB), 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 (OMB), Memorandum M-17-12, *Preparing for and Responding to a Breach of Personally Identifiable Information*, January 3, 2017.
- Office of Management and Budget (OMB), Memorandum M-17-25, *Reporting Guidance for Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*, May 19, 2017.
- Office of Management and Budget (OMB), Memorandum M-18-16, *Appendix A to OMB Circular No. A-123, Management of Reporting and Data Integrity Risk*, June 6, 2018.
- Office of Management and Budget (OMB), Memorandum M-19-03, *Strengthening the Cybersecurity of Federal Agencies by enhancing the High Value Asset Program*, December 10, 2019.
- Office of Management and Budget (OMB), Memorandum M-19-17, *Enabling Mission Delivery through Improved Identity, Credential, and Access Management*, May 21, 2019.
- Office of Management and Budget (OMB), Memorandum M-20-04, *Fiscal Year 2019-2020 Guidance on Federal Information Security and Privacy Management Requirements*, November 19, 2019.
- General Accounting Office (GAO), *Federal Information Systems Controls Audit Manual* (FISCAM), January 1999.
- National Institute of Standards and Technology (NIST), Version 1.1, *Framework for Improving Critical Infrastructure Cybersecurity*, April 16, 2018.
- National Institute of Standards and Technology (NIST) Special Publication (SP), 800-18 Revision 1, *Guide for Developing Security Plans for Federal Information Systems*, February 2006.
- National Institute of Standards and Technology (NIST) Special Publication (SP), 800-34 Revision 1, *Contingency Planning Guide for Federal Information Systems*, May 2010.
- National Institute of Standards and Technology (NIST) Special Publication (SP), 800-37 Revision 2, *Risk Management Framework for Information Systems and Organizations*, December 2018.

- National Institute of Standards and Technology (NIST) Special Publication (SP), 800-39, *Managing Information Security Risk: Organization, Mission, and Information System View*, March 2011.
- National Institute of Standards and Technology (NIST) Special Publication (SP), 800-50, *Building an Information Technology Security Awareness and Training Program*, October 2003.
- National Institute of Standards and Technology (NIST) Special Publication (SP), 800-53, Revision 4, *Security and Privacy Controls for Information Systems and Organizations*, April 2013.
- National Institute of Standards and Technology (NIST) Special Publication (SP), 800-53A, Revision 4, *Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Assessment Plans*, December 2014.
- National Institute of Standards and Technology (NIST) Special Publication (SP), 800-61, Revision 1, *Computer Security Incident Handling Guide*, August 2012.
- National Institute of Standards and Technology (NIST) Special Publication (SP), 800-84, *Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities*, September 2006.
- National Institute of Standards and Technology (NIST) Special Publication (SP), 800-100, *Information Security Handbook: A Guide to Managers*, October 2006.
- National Institute of Standards and Technology (NIST) Special Publication (SP), 800-116, Revision 1, *Guidelines for the Use of PIV Credentials in Facility Access,* June 2018.
- National Institute of Standards and Technology (NIST) Special Publication (SP), 800-122, *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)*, April 2010.
- National Institute of Standards and Technology (NIST) Special Publication (SP), 800-128, *Guide for Security-Focused Configuration Management of Information Systems*, August 2011.
- National Institute of Standards and Technology (NIST) Special Publication (SP), 800-137, *Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations*, September 2011.
- National Institute of Standards and Technology (NIST) Special Publication (SP), 800-160, *Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems*, November 2016.
- National Institute of Standards and Technology (NIST) Special Publication (SP), 800-161, *Supply Chain Risk Management Practices for Federal Information Systems and Organizations*, April 2015.
- National Institute of Standards and Technology (NIST) Special Publication (SP), 800-171, Revision 1, *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations*, December 2016.
- National Institute of Standards and Technology (NIST) Special Publication (SP), 800-181, *NICE Cybersecurity Workforce Framework (NCWF)*, August 2017.

- National Institute of Standards and Technology (NIST) Special Publication (SP), 800-184, *Guide for Cybersecurity Event Recovery*, December 2016.
- National Institute of Standards and Technology (NIST) Special Publication (SP), 800-192, *Verification and Test Methods for Access Control Policies/Models*, June 2017.
- Federal Information Processing Standards (FIPS) 140–3*, Security Requirements for Cryptographic Modules*, March 2019.
- Federal Information Processing Standards (FIPS) 199, *Standards for Security Categorization of Federal Information and Information Systems,* February 2004.
- Federal Information Processing Standards (FIPS) 200, *Minimum Security Requirements for Federal Information and Information Systems*, March 2006.
- Federal Information Processing Standards (FIPS) 201-1, *Personal Identity Verification for Federal Employees and Contractors*, March 2006.
- Department of Homeland Security (DHS) Presidential Directive 12, *Policy for a Common Identification Standard for Federal Employees and Contractors*, August 27, 2004.
- Department of Housing and Urban Development (HUD) Policy on *Section 508 of the Rehabilitation Act and Accessible Technology*, January 19, 2017.

10. Glossary – Abbreviations and Acronyms

This section lists abbreviations and acronyms as annotated in the policy.

ACRONYM	DEFINITION
A&A	Assessment and Authorization
AO	Authorizing Official
ATO	Authorization to Operate
CCMB	Configuration Control Management Board
CIO	Chief Information Officer
CIRT	Computer Incident Response Team
CISA	Cybersecurity and Infrastructure Security Agency
CISO	Chief Information Security Officer
CSAM	Cybersecurity Assessment and Management
CSF	Cybersecurity Framework
CUI	Controlled Unclassified Information
DR	Disaster Recovery
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Modernization Act of 2014
GSS	General Support System
HIPAA	Health Insurance Portability and Accountability Act
HUD	Department of Housing and Urban Development
IOO	Office of Infrastructure and Operations
ISA	Interconnection Security Agreement
ISCM	Information Security Continuous Monitoring

ACRONYM	DEFINITION
ISSO	Information System Security Officer
IT	Information Technology
NIST	National Institute of Standards and Technology
OIG	Office of Inspector General
OITS	Office of IT Security
OMB	Office of Management and Budget
OTC	Office Technical Coordinator
PKI	Public Key Infrastructure
PII	Personally Identifiable Information
POA&Ms	Plan of Action and Milestones
POC	Point of Contact
SA&A	Security Assessment and Authorization
SP	Special Publication
VPN	Virtual Private Network