

## 1.0 INTRODUCTION

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

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

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

### 1.1 Purpose

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

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

### 1.2 Scope

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

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

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

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

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

### 1.3 Authority for Policy

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

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

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

## 1.4 Policy Basis

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

## 1.5 Relationship to Other Documents and Processes

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

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

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

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

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

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

---

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

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

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

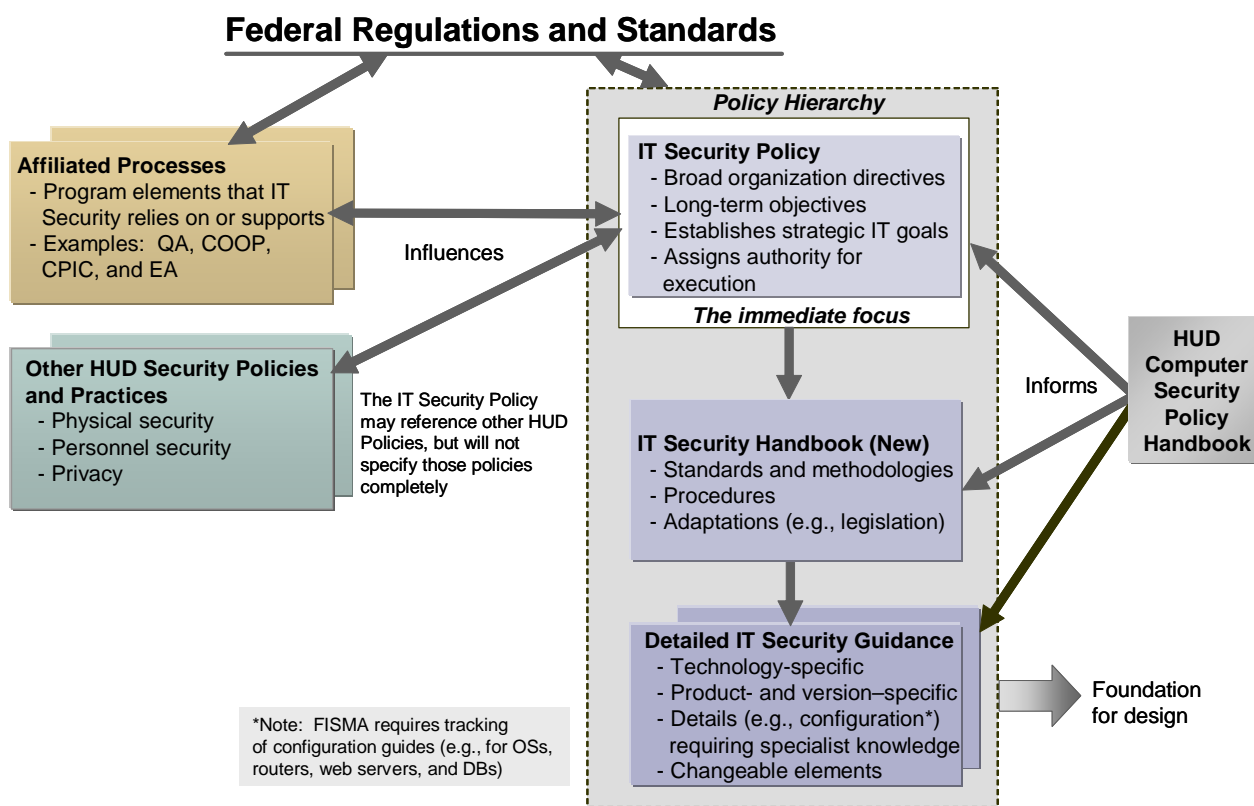


Figure 1. Security Policy Relationships

## 1.6 Document Organization

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

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

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

## 1.7 Laws and Regulations

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

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

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

## 1.8 Definitions

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

### 1.8.1 Sensitive Information

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

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

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

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

## **1.8.2 Public Information**

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

## **1.8.3 Information Technology**

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

## **1.8.4 HUD Information Technology System**

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

### ***1.8.4.1 General Support System***

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

### ***1.8.4.2 Major Application***

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

## 1.9 Exceptions

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