

## INFORMATION TECHNOLOGY SECURITY POLICY

2400.25

### 3.0 MANAGEMENT POLICIES

#### 3.1 Basic Requirements

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

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

##### 3.1.1 Information and Information System Categorization

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

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

..TD:

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

### 3.3 Contractors and Outsourced Operations

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

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

#### HUD Policy

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

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

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

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

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

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

### 3.4 Performance Measures and Metrics

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

HUD security policies, procedures, and controls. At several organizational levels, the routine collection and review of security metrics help identify new security goals and justify investment in them. NIST

SP 800-55, Security Metrics for Information Technology Systems, July 2003, provides guidance in the identification and use of security metrics. NIST prescribes the use of readily obtainable quantifiable measures that are capable of repeatable collection to measure progress toward defined security goals. NIST 800-55 defines security metrics of three types:

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

HUD Policy

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

### 3.5 Critical Infrastructure Protection

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

HUD Policy

- a. The CIO, in coordination with the Program Offices, shall identify all critical assets in accordance with HSPD 7, Critical Infrastructure Identification, Prioritization, and Protection, to determine the interdependencies of these critical assets and develop and implement a CIP Risk Management Plan to ensure that these assets are adequately protected.
- b. The CISO shall conduct yearly vulnerability assessments of IT resources that have been identified as part of HUD's critical infrastructure.

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

### 3.6 Information Technology Contingency Planning

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

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

#### HUD Policy

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

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

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

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

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

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

Be configured to facilitate timely and effective recovery operations

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

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

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

- Be geographically separated from the primary processing site

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

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

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

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

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

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

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

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

- Providers of primary and alternate services have adequate contingency plans

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

### 3.7 System Development Life Cycle

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

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

#### HUD Policy

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

b. Program Offices/System Owners shall ensure information systems

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

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

### 3.8 Configuration Management

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

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

#### HUD Policy

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

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

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

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

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

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

restrictions and provide audit information.

f. Program Offices/System Owners shall ensure that security settings have been set to their most restrictive values consistent with operational requirements. For COTS packages, Program Offices/System Owners shall consult NIST SP 800-70, Security Configuration Checklists Program for IT Products for the Configuration Checklist and configure the system accordingly. For high-impact systems, the system shall use automated mechanisms to centrally apply and verify configuration settings.

g. Program Offices/System Owners of systems that have been rated high shall ensure that their software and information are protected against unauthorized changes. The Program Offices/System Owners shall use automated tools to monitor the integrity of such information and software. Acceptable methods for COTS packages include, but are not limited to, parity checks, cyclical redundancy checks, and cryptographic hashes.

h. Program Offices/System Owners of systems under development that have been rated high shall ensure that the system developer creates and implements a configuration management plan that controls changes to the system during development, tracks security flaws, requires authorization of changes, and provides documentation of the plan and its implementation.

i. Program Offices/System Owners of systems under development that have been rated moderate or high shall ensure that the system developer creates a security test and evaluation plan, implements the plan, and documents the results. Developmental security test results should only be used when no security relevant modifications of the information system have been made subsequent to developer testing and after selective verification of developer test results.

### 3.9 Risk Management and Risk Assessment

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

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

#### HUD Policy

a. Program Offices/System Owners shall ensure that all systems under their purview have been subjected to a current risk assessment in accordance with the NIST SP 800-30, Risk Management Guide for Information Technology Systems. Risk assessments are required prior to the start of C&A.

b. Program Offices/System Owners shall conduct a risk assessment every three years and when a significant change is planned for any system under their purview.

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

E-Authentication Guidance for Federal Agencies.

### 3.10 Certification and Accreditation

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

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

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

### HUD Policy

- a. Program Offices/System Owners shall follow the guidelines contained in NIST SP 800-37, Guidelines for the Security Certification and Accreditation of Federal Information Technology Systems, in certifying and accrediting their information systems.
- b. Program Offices/System Owners shall ensure that whenever changes are made to IT systems, networks, or to their physical environment, interfaces, or user-community makeup, the impact on the security of the information processed is reviewed via a documented security-impact analysis as required by NIST SP 800-37.
- c. Program Offices/System Owners shall ensure that systems are certified and accredited at their initial operating capability every three years thereafter and whenever a significant change occurs in accordance with NIST 800-37.
- d. Existing accreditations completed before the issuance of this policy shall remain in effect if the accreditation complied fully with the policy in effect at the time of accreditation, no significant deficiencies have been identified, and the system configuration has not changed since accreditation.
- e. Program Offices shall update their POA&Ms on a quarterly basis for systems under their purview as required by OMB.
- f. Program Offices/System Owners shall conduct an annual security review of systems under their purview in accordance with NIST SP 800-26, Security Self-Assessment Guide for Information Technology Systems, and NIST SP 800-53, Recommended Security Controls for Federal Information Systems. The results of such reviews shall be

included in the annual FISMA report to OMB.

g. Program Offices/System Owners shall conduct vulnerability assessments and/or security testing to identify vulnerabilities in IT systems under their purview. These assessments shall be conducted yearly and when significant changes are made to the IT systems.

h. Program Offices/System Owners shall authorize and monitor all connections between systems under their purview and other systems outside the accreditation boundary. The connection(s) shall be documented in an Interconnection Security Agreement in accordance with NIST SP 800-47, Security Guide for Interconnecting Information Technology Systems.

i. The CISO shall implement a standard C&A methodology for all HUD systems.

j. Program Offices/System Owners shall use this methodology for all C&As.

### 3.11 Incidents, Violations, and Disciplinary Action

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

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

#### HUD Policy

a. HUD employees may be subject to disciplinary action for failure to comply with HUD security policies, whether or not the failure results in criminal prosecution. IT security-related violations are addressed in U.S. Department of Housing and Urban Development Ethics Letters 92-1, Standards of Conduct and Principles of Ethical Service for Federal Employees.

b. HUD contractors and external users who fail to comply with department security policies shall be subject to having their access to HUD IT systems and facilities terminated, whether or not the failure results in criminal prosecution.

c. Any person who improperly discloses sensitive information shall be subject to criminal and civil penalties and sanctions under a variety of laws (e.g., the Privacy Act).