

# INFORMATION TECHNOLOGY SECURITY POLICY

2400.25

## 2.0 ROLES AND RESPONSIBILITIES

Responsibility for protecting the confidentiality and integrity of HUD's information and technological resources is shared jointly by its employees, business partners, and contractors. However, in an effort to enable effective and complete implementation of this policy, specific duties have been assigned to individuals who will be fully accountable for fulfilling the associated requirements. This section describes the specific information security roles and responsibilities.

### 2.1 Secretary of the Department of Housing and Urban Development

The Secretary of HUD is responsible for ensuring that HUD IT systems and their data are protected in accordance with congressional and presidential directives. To that end, the Secretary will:

- \* Ensure the integrity, confidentiality, and availability of information and information systems.
- \* Ensure that HUD adheres to the requirements of its Information Security Program throughout the life cycle of each HUD system.
- \* Submit the results of independent evaluations performed by the HUD Inspector General (IG) to the Director of the OMB annually. These evaluations are to accompany HUD annual budget submissions.

### 2.2 Chief Information Officer

The HUD Chief Information Officer (CIO) will establish and oversee the department-wide Information Security Program and provide consulting assistance to all HUD offices for their individual programs. In addition, the CIO has the following information security responsibilities:

- \* Appoint, in writing, a federal employee to serve as the CISO.
- \* Participate in developing HUD performance plans, including descriptions of timeframes and budget, staffing, and training resources required to implement the departmentwide Information Security Program.
- \* Establish policy and oversight procedures to ensure that all information systems acquisition documents, including existing contracts, incorporate appropriate IT security requirements and comply with HUD IT security policies.
- \* Ensure that HUD's Information Security Program integrates fully into the HUD EA and CPIC processes.
- \* Ensure that Program Officials and/or System Owners understand and appropriately address risks, especially interconnectivity with other programs and systems outside their control.
- \* Review and evaluate the Information Security Program at least annually.
- \* Ensure that an IT Security Performance Metrics Program is developed, implemented, and funded.
- \* Report to the Secretary on matters relating to the security of HUD

IT systems.

- \* Continuously strengthen the Information Security Program.
- \* Ensure that adequate resources are provided for the Information Security Program.
- \* Direct that all IT security requirements be followed.
- \* Accept responsibility for the Information Security Program successfully meeting all federal regulations.
- \* Ensure overall program success.

### 2.3 Chief Information Security Officer

The Chief Information Security Officer (CISO) reports directly to the CIO on matters pertaining to IT security within HUD. The CISO will perform the following duties:

- \* Serve as the departmentwide principal advisor on IT security matters.
- \* Issue department-wide IT security policy, guidance, and architecture requirements for all HUD IT systems and networks and provide oversight to ensure these policies are implemented.
- \* Serve as the principal departmental liaison with organizations outside HUD for matters relating to IT security.
- \* Review and approve the processes, techniques, and methodologies planned for use in certifying and accrediting HUD IT systems. These include security test and evaluation plans, contingency plans, and risk assessments.
- \* Carry out CISO responsibilities under FISMA.
- \* Possess the professional qualifications, including training and experience, required to administer the functions described.
- \* Head an office with the mission and resources required to assist in ensuring HUD compliance.
- \* Develop and maintain a HUD Information Security Program.
- \* Direct HUD's day-to-day management of the Information Security Program.
- \* Coordinate all security-related interactions among Program Offices involved in the Information Security Program, as well as those external to HUD.
- \* Support Information System Security Officers (ISSO) and participate in the selection of qualified staff from the Program Offices.
- \* Serve as a member in the Technology Investment Board Working Group.

### 2.4 Information System Security Officer

An ISSO shall be appointed in writing by the appropriate Program Official for each general support system and major application. The ISSO can be either a government employee or an appropriately cleared support contractor. The ISSO is responsible for ensuring that management, operational, and technical controls for securing IT systems belonging to the Program Office are in place and followed. The ISSO will perform the following functions for the Program Office:

- \* Serve as the principal Point of Contact (POC) for all matters pertaining to the security of the IT systems for which the ISSO is responsible.
- \* Oversee the preparation of security plans, such as those required for C&A in coordination with the System Owner.
- \* Periodically review computer systems and networks to ascertain if changes have occurred that could adversely affect security.
- \* Ensure that system users receive initial computer security indoctrination and annual follow-on training, as required by applicable directives.
- \* Enforce an access control policy by which only authorized persons

can gain access to HUD IT systems and networks.

- \* Immediately report any security violation, attempt to gain unauthorized access to sensitive data, virus infection, or other event affecting the security of HUD systems and networks to the appropriate Computer Security Incident Response Center (CSIRC).
- \* Enforce the capability to track user activity on a system and report any discrepancies or misuse of automated resources.
- \* Manage the IT Security Metrics Program for the IT system. Collect and analyze data and coordinate with the CISO, as appropriate.
- \* Implement IT security policies as directed by, and in coordination with, higher authority.
- \* Attend required role-based security training.

An ISSO can be assigned to more than one general support system or major application.

## 2.5 Contracting Officer, Government Technical Monitor, and Government Technical Representative

Contracting Officers, Government Technical Monitors (GTM), and Government Technical Representatives (GTR) are responsible for ensuring that security is properly and adequately addressed as part of system acquisition and other contracting activities.

Specifically, these individuals will ensure that:

- \* New contracts include appropriate language and clauses to enforce HUD IT security policy and that existing contracts include appropriate language when modified.
- \* Any security clauses are developed and used in accordance with Departmental procurement policy, the HUD Acquisition Regulation (HUDAR) and Federal Acquisition Regulation (FAR).
- \* All new or modified HUD contracts include a clause requiring IT security awareness training and, where appropriate, role-based training for specific job categories with security responsibilities.
- \* All new or modified HUD contracts include a clause requiring contractor compliance with HUD computer security incident identification and reporting policy and procedures.
- \* IT security functional and assurance requirements are incorporated in information system procurement documents in accordance with HUD IT security policy.
- \* Contractors and subcontractors provide copies of their internal IT security plans and procedures to the CISO upon request.
- \* Existing and future contracts include requirements to have qualified security representatives (e.g., CISO, ISSO, or other designated HUD Program Office personnel) conduct site surveys at non-HUD facilities.

## 2.6 Help Desk

The help desk staff will:

- \* Assist HUD employees in technical security matters.
- \* Recognize and report security incidents to HUD CSIRC, engage resources for corrective action, and assist users in recovery.

## 2.7 Physical Security/Facilities Group/Security Officer

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

The physical security staff and security officer will:

- \* Develop and enforce appropriate physical security controls.
- \* Identify and address the physical security needs of computer

installations, office environments, and backup installations.

- \* Process and maintain personal background checks and security clearance records.

- \* Issue HUD Identification (ID) badges to employees and contractors in accordance with HSPD-12.

## 2.8 Deputy Chief Information Officer for Information Technology Operations

The Deputy CIO for IT Operations will:

- \* Monitor security technology developments and evaluate their usefulness for, or impact upon, HUD mission, architecture, and operations.

- \* Direct IT contingency planning.

- \* Work with the Program Offices, functional managers, and System Owners on technology and contingency planning issues.

- \* Own and secure the IT infrastructure (e.g., general support systems) that provides shared services across Program Offices.

## 2.9 Program Offices/System Owners

Program Offices, or System Owners, use IT to help fulfill the business requirements necessary to achieve the mission needs within their program area of responsibility. As such, they are responsible for the successful operation of IT systems within their program area and are ultimately accountable for the security of the IT systems and programs under their control. The Office of the Chief Information Officer is the Program Office responsible for most General Support Systems at HUD; the Deputy CIO for IT Operations is the System Owner for such systems. The Program Offices/System Owners will:

- \* Work closely with the CIO and other program and IT managers to ensure a complete understanding of risks, especially the increased risks resulting from interconnectivity with other programs and systems over which the Program Offices have little or no control.

- \* Prepare information system security plans and risk assessments for information systems under their purview.

- \* Ensure information systems under their purview are certified and accredited.

- \* Review, in consultation with the CISO, the IT system security within their program area at least annually.

- \* Manage the procurement and operation of their Program Office information systems.

- \* Assure adherence to information security policy in the design and operation of application systems.

- \* Coordinate with the Deputy CIO for IT Operations and the CISO on security matters involving HUD information architecture, as a whole.

## 2.10 HUD Managers, Supervisors, and Employees

All HUD personnel and support contractors who have been authorized access to sensitive data are responsible for protecting that data.

These responsibilities include the following:

- \* Comply with IT security policy and apply its principles to daily work activities.

- \* Enforce IT security policy and ensure that employees and contractors comply with IT policies and procedures.

- \* Assume accountability for protecting sensitive information under their control in accordance with this policy.

- \* Attend annual IT Security Awareness training.

- \* Attend required role-based security training-pertains to those having a security-related role (e.g., system and network administrators).

- \* Report IT security incidents (e.g., virus and malicious code

attacks) to the appropriate CSIRC according to established procedures.

- \* Cooperate with CSIRC Team members.
- \* Cooperate with Information Security Program representatives or other designated HUD Program Office personnel during security compliance reviews at HUD Program Office facilities and site surveys at non-HUD facilities.
- \* Ensure that IT security metrics data are collected in accordance with direction from the CISO and ISSO-Managers/Supervisors.
- \* Understand and comply with HUD policies, standards, and procedures regarding the protection of sensitive HUD information assets.

#### 2.11 Authorizing Official

The Authorizing Official (AO) is a senior government management official with the authority to formally assume responsibility for operating an IT system at an acceptable level of risk. AOs control personnel, operations, maintenance, and budgets for their systems or field sites; therefore, AOs shall control the resources necessary to mitigate risks. An AO shall be assigned to each general support system and major application. The AO shall be a Senior Official who is the Program Assistant Secretary, Deputy Assistant Secretary, or equivalent Program Head.

The AO may assign a designated representative to act on the AO's behalf and be empowered to make certain decisions with regard to the planning and resourcing of security C&A activities, the acceptance of system security plans, and the determination of risk to agency operations, agency assets, and individuals. The only activity the AO cannot delegate is the security accreditation decision and signing the associated accreditation decision letter (i.e., the acceptability of risk to the agency).

AOs are responsible for the following:

- \* Reviewing and approving the corrective actions necessary to mitigate residual risks.
- \* Approving/disapproving system accreditation.
- \* Terminating system operations if security conditions warrant such action.

An AO can be responsible for more than one general support system or major application.

#### 2.12 Certification Agent

A Certification Agent is assigned to each HUD IT system by an appropriate department-level official. Normally, the CISO is designated as the Certification Agent for all IT systems under the department's control.

To preserve the impartial and unbiased nature of security certification, the Certification Agent should be in a position that is independent from individuals directly responsible for information system development and day-to-day system operations. The Certification Agent should also be independent of those individuals responsible for correcting security deficiencies that are identified during security certification.

Certification Agents must be government employees and must be designated in writing at the department level. Designation letters shall be signed by the appropriate Under Secretary or Program Office Head. For each IT system, the Certification Agent shall:

- \* Ensure that a risk analysis is performed, that required C&A activities are completed, and that the results are documented.
- \* Prepare a Security Evaluation Report that clearly documents residual risks on the status of the certification for the AO.

A Certification Agent can be responsible for more than one general support system or major application.