CHAPTER 2. RESPONSIBILITY FOR SAFEGUARDING CLASSIFIED INFORMATION

2-1 Organization Heads. Headquarters Primary Organization Heads, Regional Administrators, and Managers shall be responsible for safeguarding all classified information coming within the custody or control of their organizations, maintaining a high degree of security conscientiousness among their employees and assuring compliance with this Handbook. The head of each organization may delegate any or all of the responsibilities to qualified and responsible persons in the organization.

2-2 Inspector General Responsibilities. The Inspector General has overall responsibility for promulgating and administering policies, standards, and procedures that ensure effective compliance with and implementation of Executive Order 12356 and this Handbook. These functions of the Inspector General will be performed under the supervision of the Assistant Director for Security within the Office of the Assistant Inspector General for Investigation. The Inspector General will:

A. Ensure that a demonstrable need for access to classified information is established before initiating administrative clearance procedures, and that the number of persons granted access to classified information is limited to the minimum number consistent with operational requirements and needs.

B. Establish and maintain procedures which will enable the prompt identification of any existing practice or condition which fails to afford adequate safeguarding of all classified information in the possession of the Department and take prompt and effective action to correct any deficiency noted or reported.

C. Promptly and fully determine the circumstances of any loss or subjection to compromise of classified information and take all appropriate action in connection therewith, including advice to the originating department or agency.

D. Approve the modification or substitution of any standard procedure, specification or guide set forth in this Handbook, based on his or her specific determination that such modification or substitution provides protection for classified information at least equal to that prescribed by the Executive Order, Information Security Oversight Office (ISOO) Directive No. 1 and this Handbook.

E. Establish standards, procedures, specifications, or guidelines other than those prescribed in this Handbook, whenever conditions or circumstances arise which indicate that increased safeguards are necessary in the interests of national security.

F. Ensure that all employees responsible for the handling of classified information receive an initial briefing (see Appendix 6) on their security responsibilities and execute Standard Form 312, Classified Information Nondisclosure Agreement, before accessing classified information. When need for access ends, e.g., retirement or separation-transfer, employees will complete Form HUD-70029, Security Termination Statement (see Appendix 7). The Assistant Director for Security and Administrative Officers will provide briefing, refresher training, and debriefing of all Headquarters employees. The Regional Directors of Administration will perform these functions in the Regions.

G. Continuously review safeguarding practices and eliminate those which are unnecessary.

H. Ensure that unauthorized classified disclosures are promptly reported.

2-3 HUD Employee Responsibilities.

A. Reporting Violations. Under NSDD-197, Reporting Hostile Contacts and Security Awareness, all U.S. Government Executive Branch employees are required to report contacts with individuals of any nationality, either within or outside the scope of the employee's official activities, in the following instances:

1. When illegal or unauthorized access is sought to classified or other sensitive information;

2. When the employee is concerned that he or she may be the target of an attempted exploitation by a foreign entity. A list of such entities will be disseminated annually.

This requirement is designed to maintain a high level of security awareness regarding contacts with foreign nationals, not only with regard to classified information, but also to maintain security awareness regarding proprietary or other sensitive information held at HUD. Such other sensitive information includes restricted business information, sensitive computer system information, and personnel information protected under privacy considerations.

Any such contacts shall be reported to the Assistant Director for Security, Headquarters Operations Division, Office of Investigation, Office of Inspector General.

B. If classified information is lost, the employee should report as above.

C. Care of Information. Each HUD employee who controls access to Classified information prior to giving a prospective recipient access to that information will ensure that he or she has both:

1. A security clearance to at least the same level of classification of the information sought, and

2. A valid need to know the information in connection with his or her official duties.

D. Supervisors. Each HUD supervisor entrusted with classified information will be responsible for ensuring that:

1. All such information is provided adequate safeguarding at all times and under all circumstances.

2. Each HUD employee under his or her supervision and/or each non-HUD employee is adequately instructed in, and fully complies with all provisions of this handbook.

E. News Media Contacts

1. All media requests for classified information or material shall be referred to the Inspector General who will coordinate the request with the original classification authority for direct handling with the news media. The requestor shall be advised of this action.

2-4 Challenges to Classification. Custodians of classified information are encouraged to challenge in cases where there is reasonable cause to believe that information is classified unnecessarily, improperly, or for an inappropriate period of time. Requests should be sent to the Assistant Director for Security, Office of Investigation, who will, within 20 days, resolve the question of classification with the original classification authority and provide notification to the challenger of the results. The anonymity of the challenger shall be preserved whenever he or she requests it.