over unprotected communications circuits (to include intercom and closed-circuit TV), at non-official functions, or at any time that it might be revealed to unauthorized persons. Classified information may only be entered into computer systems meeting the appropriate security criteria.

(a) EOP Security Officer. In cooperation with the Associate Director (or Assistant Director) for Administration, the EOP Security Officer supervises the administration of this section. Specifically, he/she:

(1) Promotes the correct understanding of this section and insures that initial and annual briefings about security procedures are given to all new employees.
(2) Provides for periodic inspections of office areas and reviews of produced documents to ensure full compliance with OMB regulations and procedures.
(3) Takes prompt action to investigate alleged violations of security, and recommends appropriate administrative action with respect to violators.
(4) Supervises the annual inventories of Top Secret material.
(5) Ensures that containers used to store classified material meet the appropriate security standards and that combinations to security containers are changed as required.

(b) Heads of Offices. The head of each division or office is responsible for the administration of this section in his/her area. These responsibilities include:

(1) The appointment of accountability control clerks as prescribed in §1312.26.
(2) The maintenance of the prescribed control and accountability records for classified information within the office.
(3) Establishing internal procedures to ensure that classified material is properly safeguarded at all times.

§1312.23 Access to classified information.

Classified information may be made available to a person only when the possessor of the information establishes that the person has a valid “need to know” and the access is essential to the accomplishment of official govern-