

§ 159a.47 Responsibility of originator.

The originator or an official higher in the originator's supervisory chain shall, upon receipt of notification of loss or probable compromise of classified information, take action as prescribed in § 159a.15(k).

§ 159a.48 System of control of damage assessments.

Each DoD Component shall establish a system of controls and internal procedures to ensure that damage assessments are conducted when required and that records are maintained in a manner that facilitates their retrieval and use within the Component.

§ 159a.49 Compromises involving more than one agency.

(a) Whenever a compromise involves the classified information or interests of more than one DoD Component or other agency, each such activity undertaking a damage assessment shall advise the others of the circumstances and findings that affect their information and interests. Whenever a damage assessment incorporating the product of two or more DoD Components or other agencies is needed, the affected activities shall agree upon the assignment of responsibility for the assessment.

(b) Whenever a compromise of U.S. classified information is the result of actions taken by foreign nationals, by foreign government officials, or by U.S. nationals employed by international organizations, the activity performing the damage assessment shall ensure, through appropriate intergovernmental liaison channels, that information pertinent to the assessment is obtained. Whenever more than one activity is responsible for the assessment, those activities shall coordinate the request prior to transmittal through appropriate channels.

§ 159a.50 Espionage and deliberate compromise.

Cases of espionage and deliberate unauthorized disclosure of classified information to the public shall be reported in accordance with DoD Instruction 5240.4 and DoD Directive 5210.50 and implementing issuances.

§ 159a.51 Unauthorized absentees.

When an individual who has had access to classified information is on unauthorized absence, an inquiry as appropriate under the circumstances, to include consideration of the length of absence and the degree of sensitivity of the classified information involved, shall be conducted to detect if there are any indications of activities, behavior, or associations that may be inimical to the interest of national security. When such indications are detected, a report shall be made to the DoD Component counterintelligence organization.

Subpart H—Access, Dissemination, and Accountability**§ 159a.53 Access.**

(a) *Policy.* (1) Except as otherwise provided for in paragraph (c) of this section, no person may have access to classified information unless that person has been determined to be trustworthy and unless access is essential to the accomplishment of lawful and authorized Government purposes, that is, the person has the appropriate security clearance and a need-to-know. Further, cleared personnel may not have access until they have been given an initial security briefing (see § 159a.70). Procedures shall be established by the head of each DoD Component to prevent unnecessary access to classified information. There shall be a demonstrable need for access to classified information before a request for a personnel security clearance can be initiated. The number of people cleared and granted access to classified information shall be maintained at the minimum number that is consistent with operational requirements and needs. No one has a right to have access to classified information solely by virtue of rank or position. The final responsibility for determining whether an individual's official duties require possession of or access to any element or item of classified information, and whether the individual has been granted the appropriate security clearance by proper authority, rests upon the individual who has authorized possession, knowledge, or control of the information and not upon