

**§ 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 the prospective recipient. These principles are equally applicable if the prospective recipient is a DoD Component, including commands and activities, other Federal agencies, DoD contractors, foreign governments, and others.

(2) Because of the extreme importance to the national security of Top Secret information and information controlled within approved Special Access Programs, employees shall not be permitted to work alone in areas where such information is in use or stored and accessible by those employees. This general policy is an extra safeguarding measure for the nation's most vital classified information and it is

not intended to cast doubt on the integrity of DoD employees. The policy does not apply in those situations where one employee with access is left alone for brief periods during normal duty hours. When compelling operational requirements indicate the need, DoD Component heads may waive this requirement in specific, limited cases. This waiver authority may be delegated to the senior official (§ 159a.93 (b) and (c)) of the DoD Component who may redelegate the authority but only if so authorized by the head of the DoD Component. (Any waiver should include provisions for periodically ensuring the health and welfare of individuals left alone in vaults or secure areas).

(b) *Access by Persons Outside the Executive Branch.* Classified information may be made available to individuals or agencies outside the Executive Branch provided that such information is necessary for performance of a function from which the Government will derive a benefit or advantage, and that such release is not prohibited by the originating department or agency. Heads of DoD Components shall designate appropriate officials to determine, before the release of classified information, the propriety of such action in the interest of national security and assurance of the recipient's trustworthiness and need-to-know.

(1) *Congress.* Access to classified information or material by Congress, its committees, members, and staff representatives shall be in accordance with DoD Directive 5400.4<sup>27</sup>. Any DoD employee testifying before a congressional committee in executive session in relation to a classified matter shall obtain the assurance of the committee that individuals present have a security clearance commensurate with the highest classification of the information that may be discussed. Members of Congress, by virtue of their elected positions, are not investigated or cleared by the Department of Defense.

(2) *Government Printing Office (GPO).* Documents and material of all classifications may be processed by the GPO, which protects the information in ac-

cordance with the DoD/GPO Security Agreement of February 20, 1981.

(3) *Representatives of the General Accounting Office (GAO).* Representatives of the GAO may be granted access to classified information originated by and in possession of the Department of Defense when such information is relevant to the performance of the statutory responsibilities of that office, as set forth in DoD Directive 7650.1<sup>28</sup>. Officials of the GAO, as designated in Appendix B to this part, are authorized to certify security clearances, and the basis therefor. Certifications will be made by these officials pursuant to arrangements with the DoD Component concerned. Personal recognition or presentation of official GAO credential cards are acceptable for identification purposes.

(4) *Industrial, Educational, and Commercial Entities.* (i) Bidders, contractors, grantees, educational, scientific or industrial organizations may have access to classified information only when such access is essential to a function that is necessary in the interest of the national security, and the recipients are cleared in accordance with DoD 5220.22-R.

(ii) Contractor employees whose duties do not require access to classified information are not eligible for personnel security clearance and cannot be investigated under the DISP. In exceptional situations, when a military command is vulnerable to sabotage and its mission is of critical importance to national security, National Agency Checks may be conducted on such individuals with the approval of the DUSD(P).

(5) *Historical Researchers.* Persons outside the Executive Branch who are engaged in historical research projects may be authorized access to classified information provided that an authorized official within the DoD Component with classification jurisdiction over the information:

(i) Makes a written determination that such access is clearly consistent with the interests of national security in view of the intended use of the material to which access is granted by certifying that the requester has been

<sup>27</sup> See footnote 1 to § 159a.3.

<sup>28</sup> See footnote 1 to § 159a.3.

found to be trustworthy pursuant to paragraph (a)(1) of this section;

(ii) Limits such access to specific categories of information over which that DoD Component has classification jurisdiction and to any other category of information for which the researcher obtains the written consent of a DoD Component or non-DoD department or agency that has classification jurisdiction over information contained in or revealed by documents within the scope of the proposed historical research;

(iii) Maintains custody of the classified material at a DoD installation or activity or authorizes access to documents in the custody of the NARA;

(iv) Obtains the researcher's agreement to safeguard the information and to submit any notes and manuscript for review by all DoD Components or non-DoD departments or agencies with classification jurisdiction for a determination that no classified information is contained therein by execution of a statement entitled, "Conditions Governing Access to Official Records for Historical Research Purposes"; and

(v) Issues an authorization for access valid for not more than 2 years from the date of issuance that may be renewed under regulations of the issuing DoD Component.

(6) *Former Presidential Appointees.* Persons who previously occupied policy making positions to which they were appointed by the President may not remove classified information upon departure from office as all such material must remain under the security control of the U.S. Government. Such persons may be authorized access to classified information that they originated, received, reviewed, signed, or that was addressed to them while serving as such an appointee, provided that an authorized official within the DoD Component with classification jurisdiction for such information:

(i) Makes a written determination that such access is clearly consistent with the interests of national security in view of the intended use of the material to which access is granted and by certifying that the requester has been found to be trustworthy pursuant to paragraph (a)(1) of this section;

(ii) Limits such access to specific categories of information over which that DoD Component has classification jurisdiction and to any other category of information for which the former appointee obtains the written consent of a DoD Component or non-DoD department or agency that has classification jurisdiction over information contained in or revealed by documents with the scope of the proposed access;

(iii) Retains custody of the classified material at a DoD installation or activity or authorizes access to documents in the custody of the National Archives and Records Service; and

(iv) Obtains the former presidential appointee's agreement to safeguard the information and to submit any notes and manuscript for review by all DoD Components or non-DoD departments or agencies with classification jurisdiction for a determination that no classified information is contained therein.

(7) *Judicial Proceedings.* DoD Directive 5405.2<sup>29</sup> governs the release of classified information in litigation.

(c) *Access by Foreign Nationals, Foreign Governments, and International Organizations.* (1) Classified information may be released to foreign nationals, foreign governments, and international organizations only when authorized under the provisions of the National Disclosure Policy and DoD Directive 5230.11; and

(2) Access to COMSEC information by foreign persons and activities shall be in accordance with policy issuances of the National Telecommunications and Information Systems Security Committee (NTISSC).

(d) *Other Situations.* When necessary in the interests of national security, heads of DoD Components, or their single designee, may authorize access by persons outside the Federal government, other than those enumerated in paragraphs (b) and (c) of this section, to classified information upon determining that the recipient is trustworthy for the purpose of accomplishing a national security objective; and that the recipient can and will safeguard the information from unauthorized disclosure.

<sup>29</sup> See footnote 1 to § 159a.3.

(e) *Access Required by Other Executive Branch Investigative and Law Enforcement Agents.* (1) Normally, investigative agents of other departments or agencies may obtain access to DoD information through established liaison or investigative channels.

(2) When the urgency or delicacy of a Federal Bureau of Investigation (FBI), Drug Enforcement Administration (DEA), or Secret Service investigation precludes use of established liaison or investigative channels, FBI, DEA, or Secret Service agents may obtain access to DoD information as required. However, this information shall be protected as required by its classification. Before any public release of the information so obtained the approval of the head of the activity or higher authority shall be obtained.

(f) *Access by Visitors.* Procedures shall be established to control access to classified information by visitors. (DoD Instruction 5230.20 provides further guidance regarding foreign visitors.)

(1) Except when a continuing, frequent working relationship is established, through which current security clearance and need-to-know are determined, DoD personnel visiting other activities of the Department of Defense, its contractors, and other agencies shall provide advance notification of the pending visit that establishes the visitor's security clearance and the purpose of the visit. Visit requests shall be signed by an official other than the visitor who is in a position to verify the visitor's security clearance.

(2) Visit requests normally should include the following:

- (i) Full name, date and place of birth, social security number, and rank or grade of visitor;
- (ii) Security clearance of the visitor;
- (iii) Employing activity of the visitor;
- (iv) Name and address of activity to be visited;
- (v) Date and duration of proposed visit;
- (vi) Purpose of visit in sufficient detail to establish need-to-know; and
- (vii) Names of persons to be contacted.

(3) Visit requests may remain valid for not more than 1 year.

#### § 159a.54 Dissemination.

(a) *Policy.* DoD Components shall establish procedures consistent with this Regulation for the dissemination of classified material. The originating official or activity may prescribe specific restrictions on dissemination of classified information when necessary. (See § 159a.35(f). Particular emphasis shall be placed on traditional need-to-know measures to aid in the strict control of classified information.)

(b) *Restraints on Special Access Requirements.* Special requirements with respect to access, distribution, and protection of classified information shall require prior approval in accordance with subpart M of this part.

(c) *Information Originating in a Non-DoD Department or Agency.* Except under rules established by the Secretary of Defense, or as provided by section 102 of the National Security Act, classified information originating in a department or agency other than Department of Defense shall not be disseminated outside the Department of Defense without the consent of the originating department or agency.

(d) *Foreign Intelligence Information.* Dissemination of foreign intelligence information shall be in accordance with the provisions of DoD Instruction 5230.22 and DoD Directive C-5230.23<sup>30</sup>.

(e) *Restricted Data and Formerly Restricted Data.* Information bearing the warning notices prescribed in § 159a.35 (b) and (c) shall not be disseminated outside authorized channels without the consent of the originator. Access to and dissemination of Restricted Data by DoD personnel shall be subject to DoD Directive 5210.2.

(f) *NATO Information.* Classified information originated by NATO shall be safeguarded in accordance with DoD Directive 5100.55.

(g) *COMSEC Information.* COMSEC information shall be disseminated in accordance with NACSI 4005 and implementing instructions.

(h) *Dissemination of Top Secret Information.* (1) Top Secret information, originated within the Department of

<sup>30</sup>See footnote 13 to § 159a.33(j).