

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.

(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-5230.23³⁰.

(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

³⁰See footnote 13 to § 159a.33(j).

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 Defense, may not be disseminated outside the Department of Defense without the consent of the originating DoD Component, or higher authority.

(2) Top Secret information, whenever segregable from classified portions bearing lower classifications, shall be distributed separately.

(3) Standing distribution requirements for Top Secret information and materials, such as distribution lists, shall be reviewed at least annually to verify the recipients' need-to-know.

(i) *Dissemination of Secret and Confidential Information*. (1) Secret and Confidential information, originated within the Department of Defense, may be disseminated within the Executive Branch, unless prohibited by the originator. (See § 159a.35(f)).

(2) Standing distribution requirements for Secret and Confidential information and materials, such as distribution lists, shall be reviewed at least annually to verify the recipients' need-to-know.

(j) *Code Words, Nicknames, and Exercise Terms*. The use of code words, nicknames, and exercise terms is subject to the provisions of subpart M and Appendix C.

(k) *Scientific and Technical Meetings*. Use of classified information in scientific and technical meetings is subject to the provisions of DoD Directive 5200.12.

(l) *Limited Dissemination (LIMDIS)*. This section establishes limits on measures for the protection of information beyond those involving access to classified information per se, but not so stringent as to require the establishment of a Special Access Program. It prohibits use of terminology indicating enhancements to need-to-know, such as

Special Need-to-Know (SNTK), MUST KNOW, Controlled Need-to-Know (CNTK), or other similar security upgrade designations and associated unique security requirements such as specialized nondisclosure statements. Limited dissemination controls are the only security enhancement short of a Special Access Program which may be employed for control over specific information for specified periods of time. In this context, these procedures may be initiated and continued on a showing that additional access controls are required in order to assure the security of the designated information. The decision to apply these procedures shall be made at the original classification authority level of command or supervision in accordance with the implementing information security instructions promulgated by the DoD Component. Except by agreement, such requirements shall not be imposed outside of the approving DoD Component. LIMDIS protective measures are restricted to one or more of the following:

(1) Decentralized maintenance of disclosure listings, briefings concerning access limitations, and physical security restrictions limited to requirements such as placing the material in sealed envelopes within approved storage containers to avoid inadvertent disclosure and the commingling with other files;

(2) Using unclassified nicknames (no code words may be assigned to LIMDIS information);

(3) Marking the material as LIMDIS along with the assigned nickname;

(4) Marking inner envelopes containing designated LIMDIS information with the notation: "To be Opened Only By Personnel Authorized Access";

(5) Requiring electronically transmitted messages containing designated information to be marked with the uniform caveat LIMDIS; and

(6) Prescribing unique oversight procedures to be accomplished by Component professional security personnel (industrial security inspections will be conducted in the normal manner by the Defense Investigative Service).