

safeguarding of information that is owned by, produced for or by, or under the control of the Department of Defense or its Components.

§ 159a.3 Nongovernment operations.

Except as otherwise provided herein, the provisions of this part that are relevant to operations of nongovernment personnel entrusted with classified information shall be made applicable thereto by contracts or other legally binding instruments. (See DOD Directive 5220.22¹, DoD 5220.22-R², and DoD 5220.22-M³.)

§ 159a.4 Combat operations.

The provisions of this part relating to accountability, dissemination, transmission, or safeguarding of classified information may be modified by military commanders but only to the extent necessary to meet local conditions in connection with combat or combat-related operations. Classified information should be introduced into forward combat areas or zones or areas of potential hostile activity only when essential to accomplish the military mission.

§ 159a.5 Atomic energy material.

Nothing in this part supersedes any requirement related to "Restricted Data" in the Atomic Energy Act of August 30, 1954, as amended, or the regulations of the Department of Energy under that Act. "Restricted Data" and material designated as "Formerly Restricted Data," shall be handled, protected, classified, downgraded, and declassified to conform with Pub. L. 83-703 and the regulations issued pursuant thereto.

§ 159a.6 Sensitive compartmented and communications security information.

(a) Sensitive Compartmented Information (SCI) and Communications Se-

¹Copies may be obtained, if needed, from the Naval Publications and Forms Center, Attn: Code 106, 5801 Tabor Avenue, Philadelphia, PA 19120.

²Copies may be obtained at cost, from the National Technical Information Service, 5285 Port Royal Road, Springfield, VA 22161.

³Copies may be obtained, at cost, from the Government Printing Office.

curity (COMSEC) Information shall be handled and controlled in accordance with applicable national directives and DOD Directives and Instructions. Other classified information, while in established SCI or COMSEC areas, may be handled in the same manner as SCI or COMSEC information. Classification principles and procedures, markings, downgrading, and declassification actions prescribed in this part apply to SCI and COMSEC information.

(b) Pursuant to 32 CFR part 159, the Director, National Security Agency/Chief, Central Security Service may prescribe special rules and procedures for the handling, reporting of loss, storage, and access to classified communications security devices, equipments, and materials in mobile, handheld or transportable systems, or that are used in conjunction with commercial telephone systems, or in similar circumstances where operational demands preclude the application of standard safeguards. These special rules may include procedures for safeguarding such devices and materials, and penalties for the negligent loss of government property.

§ 159a.7 Automatic Data Processing systems.

This part applies to protection of classified information processed, stored or used in, or communicated, displayed or disseminated by an automatic data processing (ADP) system. Additional security policy, responsibilities, and requirements applicable specifically to ADP systems are contained in DoD Directive 5200.28⁴ and DoD 5200.28-M.

Subpart B—General Provisions

§ 159a.9 Definitions.

(a) *Access.* The ability and opportunity to obtain knowledge of classified information.

(b) *Applicable Associated Markings.* The markings, other than classification markings, and warning notices listed or referred to in § 159a.31(d).

(c) *Carve-Out.* A classified contract issued in connection with an approved Special Access Program in which the Defense Investigative Service has been

⁴See footnote 1 to § 159a.3.

relieved of inspection, responsibility in whole or in part under the Defense Industrial Security Program.

(d) *Classification Authority*. The authority vested in an official of the Department of Defense to make an initial determination that information requires protection against unauthorized disclosure in the interest of national security.

(e) *Classification Guide*. A document issued by an authorized original classifier that prescribes the level of classification and appropriate declassification instructions for specified information to be classified derivatively. For purposes of this part, this term does not include DD Form 254, "Contract Security Classification Specification."

(f) *Classified Information*. Information or material that is:

(1) Owned by, produced for or by, or under the control of the U.S. Government; and

(2) Determined under E.O. 12356 or prior orders and this part to require protection against unauthorized disclosure; and

(3) So designated.

(g) *Classifier*. An individual who makes a classification determination and applies a security classification to information or material. A classifier may be an original classification authority or a person who derivatively assigns a security classification based on a property classified source or a classification guide.

(h) *Communications Security (COMSEC)*. The protection resulting from all measures designed to deny unauthorized persons information of value which might be derived from the possession and study of telecommunications and to ensure the authenticity of such communications. COMSEC includes cryptosecurity, emission security, transmission security, and physical security of COSMEC material and information.

(i) *Compromise*. The disclosure of classified information to persons not authorized access thereto.

(j) *Confidential Source*. Any individual or organization that has provided, or that may reasonably be expected to provide, information to the United States on matters pertaining to the national security with the expectation,

expressed or implied, that the information or relationship, or both, be held in confidence.

(k) *Continental United States (CONUS)*. United States territory, including adjacent territorial waters, located within the North American continent between Canada and Mexico.

(l) *Controlled Cryptographic Item (CCI)*. A secure telecommunications or information handling equipment ancillary device, or associated cryptographic component, which is unclassified but controlled.

NOTE: Equipments and components so designated bear the designator "Controlled Cryptographic Item" or "CCI."

(m) *Critical Nuclear Weapon Design Information*. That Top Secret Restricted Data or Secret Restricted Data revealing the theory of operation or design of the components of a thermo-nuclear or implosion-type fission bomb, warhead, demolition munition or test device. Specifically excluded is information concerning arming, fuzing, and firing systems; limited life components; and total contained quantities of fissionable, fusionable, and high explosive materials by type. Among these excluded items are the components which DoD personnel set, maintain, operate, test, or replace.

(n) *Custodian*. An individual who has possession of or is otherwise charged with the responsibility for safeguarding or accounting for classified information.

(o) *Declassification*. The determination that classified information no longer requires, in the interest of national security, any degree of protection against unauthorized disclosure, together with a removal or cancellation of the classification designation.

(p) *Declassification Event*. An event that eliminates the need for continued classification of information.

(q) *Derivative Classification*. A determination that information is in substance the same as information currently classified, and the application of the classification markings.

(r) *Document*. Any recorded information regardless of its physical form or characteristics, including, without limitation, written or printed matter, data processing cards and tapes, maps, charts, paintings, drawings,

engravings, sketches, working notes and papers, or reproductions by any means or process, and sound, voice, magnetic or electronic recordings in any form.

(s) *DoD Component*. The Office of the Secretary of Defense (OSD), the Military Departments, the Organization of the Joint Chiefs of Staff (OJCS), the Unified and Specified Commands, and the Defense Agencies.

(t) *Downgrade*. A determination that classified information requires, in the interest of national security, a lower degree of protection against unauthorized disclosure than currently provided, together with a changing of the classification designation to reflect such lower degree of protection.

(u) *Foreign Government Information*. Information that is:

(1) Provided to the United States by a foreign government or governments, an international organization of governments, or any element thereof with the expectation, expressed or implied, that the information, the source of the information, or both, are to be held in confidence; or

(2) Produced by the United States pursuant to or as a result of a joint arrangement with a foreign government or governments or an international organization of governments, or any element thereof, requiring that the information, the arrangement, or both, are to be held in confidence.

(v) *Formerly Restricted Data*. Information removed from the Restricted Data category upon a joint determination by the Department of Energy (or antecedent agencies) and the Department of Defense that such information relates primarily to the military utilization of atomic weapons and that such information can be safeguarded adequately as classified defense information. For purposes of foreign dissemination, however, such information is treated in the same manner as Restricted Data.

(w) *Information*. Knowledge that can be communicated by any means.

(x) *Information Security*. The result of any system of policies and procedures for identifying, controlling, and protecting from unauthorized disclosure, information whose protection is authorized by executive order or statute.

(y) *Intelligence Activity*. An activity that an agency within the Intelligence Community is authorized to conduct under E.O. 12333.

(z) *Limited Dissemination*. Restrictive controls for classified information established by an original classification authority to emphasize need-to-know protective measures available within the regular security system.

(aa) *Material*. Any product or substance on, or in which, information is embodied.

(bb) *National Security*. The national defense and foreign relations of the United States.

(cc) *Need-to-know*. A determination made by a possessor of classified information that a prospective recipient, in the interest of national security, has a requirement for access to, or knowledge, or possession of the classified information in order to accomplish lawful and authorized Government purposes.

(dd) *Original Classification*. An initial determination that information requires, in the interest of national security, protection against unauthorized disclosure, together with a classification designation signifying the level of protection required.

(ee) *Regrade*. A determination that classified information requires a different degree of protection against unauthorized disclosure than currently provided, together with a change of classification designation that reflects such different degree of protection.

(ff) *Restricted Data*. All data concerning:

(1) Design, manufacture or utilization of atomic weapons;

(2) The production of special nuclear material; or

(3) The use of special nuclear material in the production of energy, but shall not include data declassified or removed from the Restricted Data category under section 142 of Pub. L. 83-703.

(gg) *Security Clearance*. A determination that a person is eligible under the standards of DoD 5200.2-R for access to classified information.

(hh) *Senior Information Security Authority*. A senior official designated in

writing by the head of each DoD Component to be responsible for implementation of the Information Security Program within the Component.

(ii) *Sensitive Compartmented Information.* Information and material that requires special controls for restricted handling within compartmented intelligence systems and for which compartmentation is established.

(jj) *Special Access Program.* Any program approved in accordance with subpart M of this part which imposes need-to-know or access controls beyond those normally required for access to Confidential, Secret, or Top Secret information.

(kk) *Special Activity.* An activity, or functions in support of such activity, conducted in support of national foreign policy objectives abroad that is planned and executed so that the role of the U.S. Government is neither apparent nor acknowledged publicly; but that is not intended to influence U.S. political processes, public opinion, policies, or media, and does not include diplomatic activities or the collection and production of intelligence or related support functions.

(ll) *Unauthorized Disclosure.* A communication or physical transfer of classified information to an unauthorized recipient.

(mm) *United States and Its Territories, Possessions, Administrative, and Commonwealth Areas.* The 50 States; the District of Columbia; the Commonwealth of Puerto Rico; the Territories of Guam, American Samoa, and the Virgin Islands; the Trust Territory of the Pacific Islands; and the Possessions, Midway and Wake Islands.

(nn) *Upgrade.* A determination that certain classified information requires, in the interest of national security, a higher degree of protection against unauthorized disclosure than currently provided, together with a changing of the classification designation to reflect such higher degree.

§ 159a.10 Policies.

(a) *Classification*—(1) *Basic Policy.* Except as provided in the Atomic Energy Act of 1954, as amended, E.O. 12356, as implemented by the ISOO Directive No. 1, and this part, provides the only basis for classifying information. It is

the policy of the Department of Defense to make available to the public as much information concerning its activities as possible consistent with the need to protect the national security. Accordingly, security classification shall be applied only to protect the national security.

(2) *Resolution of Doubts.* Unnecessary classification and higher than necessary classification should be avoided. If there is reasonable doubt about the need to classify information, it shall be safeguarded as if it were classified “Confidential” pending a determination by an original classification authority, who shall make this determination within 30 days. If there is reasonable doubt about the appropriate level of classification, it shall be safeguarded at the higher level of classification pending a determination by an original classification authority, who shall make this determination within 30 days. Upon a classification determination, markings shall be applied in accordance with subpart E of this part.

(3) *Duration.* Information shall be classified as long as required by national security considerations. Each decision to classify requires a simultaneous determination of the duration such classification must remain in force or that the duration of classification cannot be determined.

(b) *Declassification.* Decisions concerning declassification shall be based on the loss of the information’s sensitivity with the passage of time or upon the occurrence of a declassification event.

(c) *Safeguarding.* Information classified under this part shall be afforded the level of protection against unauthorized disclosure commensurate with the level of classification assigned under the varying conditions that may arise in connection with its use, dissemination, storage, movement or transmission, and destruction.

§ 159a.11 Security classification designations.

(a) *General.* Information or material that requires protection against unauthorized disclosure in the interest of national security shall be classified in one of three designations, namely: