

- (b) Counterintelligence.
- (c) Special access programs
- (d) Information that identifies clandestine organizations, agents, sources, or methods.
- (e) Information on personnel under official or nonofficial cover or revelation of a cover arrangement.
- (f) Covertly obtained intelligence reports and the derivative information that would divulge intelligence sources or methods.
- (g) Methods or procedures used to acquire, produce, or support intelligence activities.
- (h) CIA structure, size, installations, security, objectives, and budget.
- (i) Information that would divulge intelligence interests, value, or extent of knowledge on a subject.
- (j) Training provided to or by the CIA that would indicate its capability or identify personnel.
- (k) Personnel recruiting, hiring, training, assignment, and evaluation policies.
- (l) Information that could lead to foreign political, economic, or military action against the United States or its allies.
- (m) Events leading to international tension that would affect U.S. foreign policy.
- (n) Diplomatic or economic activities affecting national security or international security negotiations.
- (o) Information affecting U.S. plans to meet diplomatic contingencies affecting national security.
- (p) Nonattributable activities conducted abroad in support of U.S. foreign policy.
- (q) U.S. surreptitious collection in a foreign nation that would affect relations with the country.
- (r) Covert relationships with international organizations or foreign governments.
- (s) Information related to political or economic instabilities in a foreign country threatening American lives and installations therein.
- (t) Information divulging U.S. intelligence collection and assessment capabilities.
- (u) U.S. and allies' defense plans and capabilities that enable a foreign entity to develop countermeasures.

- (v) Information disclosing U.S. systems and weapons capabilities or deployment.
- (w) Information on research, development, and engineering that enables the United States to maintain an advantage of value to national security.
- (x) Information on technical systems for collection and production of intelligence, and their use.
- (y) U.S. nuclear programs and facilities.
- (z) Foreign nuclear programs, facilities, and intentions.
- (aa) Contractual relationships that reveal the specific interest and expertise of the CIA.
- (bb) Information that could result in action placing an individual in jeopardy.
- (cc) Information on secret writing when it relates to specific chemicals, reagents, developers, and microdots.
- (dd) Reports of the Foreign Broadcast Information Service (FBIS) (— Branch, —Division) between July 31, 1946, and December 31, 1950, marked CONFIDENTIAL or above.
- (ee) Reports of the Foreign Documents Division between 1946 and 1950 marked RESTRICTED or above.
- (ff) Q information reports.
- (gg) FDD translations.
- (hh) U reports.

PART 159—DOD INFORMATION SECURITY PROGRAM

- Sec.
- 159.1 Purpose.
- 159.2 Applicability and scope.
- 159.3 Policy.
- 159.4 Procedures.
- 159.5 Responsibilities.

AUTHORITY: E.O. 12356 and 5 U.S.C. 301.

SOURCE: 53 FR 44877, Nov. 7, 1988, unless otherwise noted.

§ 159.1 Purpose.

- (a) This part updates policies and procedures of the DoD information Security Program, implements Executive Order 12356 and 32 CFR part 2001, delegates authority, and assigns responsibilities.
- (b) This part authorizes the development, publication, and maintenance of the following documents, consistent with DoD 5025.1-M.

§ 159.2

32 CFR Ch. I (7–1–99 Edition)

(1) DoD 5200.1-R, “Information Security Program Regulation”;

(2) DoD 5200.1-H, “Department of Defense Handbook for Writing Security Classification Guidance”;

(3) DoD 5200.1-I, “Index of Security Classification Guides”;

(4) DoD 5200.1-PH, “A Guide to Marking Classified Documents”;

(5) Other DoD 5200.1-PH series issuances necessary to ensure or facilitate compliance with and implementation of DoD 5200.1-R and E.O. 12356 and 32 CFR part 2001.

§ 159.2 Applicability and scope.

(a) This part applies to the Office of the Secretary of Defense, the Military Departments, the Organization of the Joint Chiefs of Staff, the Unified and Specified Commands, and the Defense Agencies (hereafter referred to as “DoD Components”).

(b) This part covers all information that is owned, produced by or for, or is under the control of the Department of Defense that shall be protected from unauthorized disclosure in the interest of national security under Executive Order 12356 and ISOO Directive No. 1 and all such information received by the Department of Defense from other sources, including that received from or produced pursuant to or as a result of a joint arrangement with a foreign government or international organization.

§ 159.3 Policy.

It is the policy of the Department of Defense to assure that information that warrants protection against unauthorized disclosure is properly classified and safeguarded as well as to facilitate the flow of unclassified information about DoD operations to the public.

§ 159.4 Procedures.

To carry out this policy, there is established a DoD Information Security Program that shall be administered to ensure that:

(a) Information requiring protection in the interest of national security is properly classified and safeguarded.

(b) Overclassification and unnecessary classification are avoided.

(c) Information is classified as long as required by national security considerations.

(d) Unnecessary expense to the Department of Defense, industry, and the U.S. government, resulting from protection of information no longer requiring classification, is eliminated.

(e) Declassified information is made available to the public under 32 CFR part 285.

(f) Classified inventories are reduced to the minimum necessary to meet operational requirements, thereby affording better protection to that which remains.

(g) DoD military and civilian personnel, who require access to classified information in the conduct of official business, are familiar with the requirements of DoD 5200.1-R and E.O. 12356 and 32 CFR part 2001, and that they comply with those requirements.

§ 159.5 Responsibilities.

(a) The *Deputy Under Secretary of Defense (Policy)* shall:

(1) Direct and administer the DoD Information Security Program, establish policy, standards, criteria, and procedures to comply with E.O. 12356, except its section 3.4.

(2) Conduct an active oversight program to ensure effective implementation of DoD 5200.1-R, Executive Order 12356, and 32 CFR part 2001, to include security education and training.

(3) Consider and take action on complaints and suggestions from persons within or outside the government regarding the DoD information Security Program.

(b) The *Assistant Secretary of Defense (Public Affairs)* shall direct and administer a DoD Mandatory Declassification Review Program under section 3.4., E.O. 12356, and establish policies and procedures for processing mandatory declassification review requests, including appeals, under section 3.4(d) of E.O. 12356 and section 2001.32(a)(2)(iii) of Information Security Oversight Office (ISOO) Directive No. 1¹ that make

¹Copies may be obtained, if needed, from the Director, Information Security Oversight, General Service Administration, Washington, DC 20405.

maximum use of DoD Component resources and systems established to implement 32 CFR part 285.

(c) The *Head of each DoD Component* shall:

(1) Designate a senior official who shall be responsible for the direction and administration of the Component's Information Security Program, to include active oversight, and security education and training programs to ensure implementation of DoD 5200.1-R within the Component.

(2) Ensure that funding and resources are adequate to carry out such oversight, and security education and training programs.

(3) Consider and take action on complaints and suggestions from persons within or outside the government regarding the Component's Information Security Program.

(4) Establish procedures to limit access to classified information to those who need to know.

(5) Develop plans for the protection, removal, or destruction of classified material in case of fire, natural disaster, civil disturbance, terrorist activities, or enemy action. These plans shall include the treatment of classified information located in foreign countries.

(d) Pursuant to E.O. 12356, the *Director, National Security Agency/Chief, Central Security Service*, as the designee of the Secretary of Defense, is authorized to impose special requirements with respect to the marking, reproduction, distribution, accounting, and protection of and access to classified cryptologic information. The Director, National Security Agency/Chief, Central Security Service, will develop special procedures for the declassification review of cryptologic information. This authority may not be redelegated.

PART 159a—INFORMATION SECURITY PROGRAM REGULATION

Subpart A—Policy

- Sec.
159a.1 Purpose.
159a.2 Applicability.
159a.3 Nongovernment operations.
159a.4 Combat operations.
159a.5 Atomic energy material.

- 159a.6 Sensitive compartmented and communications security information.
159a.7 Automatic Data Processing systems.

Subpart B—General Provisions

- 159a.9 Definitions.
159a.10 Policies.
159a.11 Security classification designations.
159a.12 Authority to classify, downgrade, and declassify.

Subpart C—Classification

- 159a.14 Classification responsibilities.
159a.15 Classification principles, criteria, and considerations.
159a.16 Duration of original classification.
159a.17 Classification guides.
159a.18 Resolution of conflicts.
159a.19 Obtaining classification evaluations.
159a.20 Information developed by private sources.
159a.21 Regrading.
159a.22 Industrial operations.

Subpart D—Declassification and Downgrading

- 159a.24 General provisions.
159a.25 Systematic review.
159a.26 Mandatory declassification review.
159a.27 Declassification of transferred documents or material.
159a.28 Downgrading.
159a.29 Miscellaneous.

Subpart E—Marking

- 159a.31 General provisions.
159a.32 Specific markings on documents.
159a.33 Markings on special categories of material.
159a.34 Classification authority, duration, and change in classification markings.
159a.35 Additional warning notices.
159a.36 Remarking old material.

Subpart F—Safekeeping and Storage

- 159a.37 Storage and storage equipment.
159a.38 Custodial precautions.
159a.39 Activity entry and exit inspection program.

Subpart G—Compromise of Classified Information

- 159a.41 Policy.
159a.42 Cryptographic and sensitive compartmented information.
159a.43 Responsibility of discoverer.
159a.44 Preliminary inquiry.
159a.45 Investigation.
159a.46 Responsibility of authority ordering investigation.
159a.47 Responsibility of originator.