

(1) Be responsible for overall policy, guidance, and control of the DoDPSP.

(2) Develop and implement plans, policies, and procedures for the DoDPSP.

(3) Issue and maintain DoD 5200.2-R consistent with DoD 5025.1-M.

(4) Conduct an active oversight program to ensure compliance with DoDPSP requirements.

(5) Ensure that research is conducted to assess and improve the effectiveness of the DoDPSP (DoD Directive 5210.79<sup>5</sup>).

(6) Ensure that the Defense Investigative Service is operated pursuant to 32 CFR part 361.

(7) Ensure that the DoD Security Institute provides the education, training, and awareness support to the DoDPSP under DoD Directive 5200.32.<sup>6</sup>

(8) Be authorized to make exceptions to the requirements of this part on a case-by-case basis when it is determined that doing so furthers the mission of the Department of Defense and is consistent with the protection of classified information from unauthorized disclosure.

(b) The *General Counsel of the Department of Defense* shall:

(1) Be responsible for providing advice and guidance as to the legal sufficiency of procedures and standards implementing the DoDPSP and the DISP.

(2) Exercise oversight of PSP appeals procedures to verify that the rights of individuals are being protected consistent with the constitution, laws of the United States, Executive Orders, Directives, or Regulations that implement the DoDPSP and DISP, and with the interests of national security.

(c) The *Heads of the DoD Components* shall:

(1) Designate a senior official who shall be responsible for implementing the DoDPSP within their components.

(2) Ensure that the DoDPSP is properly administered under this Directive within their components.

(3) Ensure that information and recommendations are provided to the Assistant Secretary of Defense for Command, Control, Communications, and Intelligence on any aspect of the program.

<sup>5</sup> See footnote 1 to 156.1(b).

<sup>6</sup> See footnote 1 to 156.1(b).

## PART 158—GUIDELINES FOR SYSTEMATIC DECLASSIFICATION REVIEW OF CLASSIFIED INFORMATION IN PERMANENTLY VALUABLE DoD RECORDS

Sec.

158.1 Reissuance and purpose.

158.2 Applicability and scope.

158.3 Definitions.

158.4 Policy.

158.5 Procedures.

158.6 Responsibilities.

158.7 Categories of information that require review before declassification.

158.8 Categories of information that require review before declassification: Department of the Army systems.

158.9 Categories of information that require review before declassification: Department of the Navy systems.

158.10 Categories of information that require review before declassification: Department of the Air Force systems.

158.11 Declassification considerations.

158.12 Department of State areas of interest.

158.13 Central Intelligence Agency areas of interest.

AUTHORITY: E.O. 12356, 10 U.S.C.

SOURCE: 48 FR 29840, June 29, 1983, unless otherwise noted.

### § 158.1 Reissuance and purpose.

This part is reissued; establishes procedures and assigns responsibilities for the systematic declassification review of information classified under E.O. 12356 and Information Security Oversight Office Directive No. 1, DoD Directive 5200.1 and DoD 5200.1-R, and prior orders, directives, and regulations governing security classification; and implements section 3.3 of E.O. 12356.

### § 158.2 Applicability and scope.

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

(b) This part applies to the systematic review of permanently valuable classified information, developed by or for the Department of Defense and its

### § 158.3

Components, or its predecessor components and activities, that is under the exclusive or final original classification jurisdiction of the Department of Defense.

(c) Its provisions do not cover Restricted Data or Formerly Restricted Data under the Atomic Energy Act of 1954 or information in nonpermanent records.

(d) Systematic declassification review of records pertaining to intelligence activities (including special activities) or intelligence sources or methods shall be in accordance with special procedures issued by the Director of Central Intelligence.

#### § 158.3 Definitions.

(a) *Cryptologic information.* Information pertaining to or resulting from the activities and operations involved in the production of signals intelligence (SIGINT) or to the maintenance of communications security (COMSEC).

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

(c) *Intelligence method.* Any process, mode of analysis, means of gathering data, or processing system or equipment used to produce intelligence.

(d) *Intelligence source.* A person or technical means that provides intelligence.

#### § 158.4 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.

### 32 CFR Ch. I (7-1-02 Edition)

#### § 158.5 Procedures.

(a) DoD classified information that is permanently valuable, as defined by 44 U.S.C. 2103, that has been accessioned into the National Archives of the United States, will be reviewed systematically for declassification by the Archivist of the United States, with the assistance of the DoD personnel designated for that purpose, as it becomes 30 years old; however, file series concerning intelligence activities (including special activities) created after 1945, intelligence sources or methods created after 1945, and cryptology records created after 1945 will be reviewed as they become 50 years old.

(b) All other DoD classified information and foreign government information that is permanently valuable and in the possession or control of DoD Components, including that held in Federal records centers or other storage areas, may be reviewed systematically for declassification by the DoD Component exercising control of such information.

(c) DoD classified information and foreign government information in the possession or control of DoD Components shall be declassified when they become 30 years old, or 50 years old in the case of DoD intelligence activities (including special activities) created after 1945, intelligence sources or methods created after 1945, or cryptology created after 1945, if they are not within one of the categories specified in §§ 158.7 through 158.10 or in 48 FR 4403, January 31, 1983.

(d) Systematic review for declassification shall be in accordance with procedures contained in DoD 5200 1-R. Information that falls within any of the categories in §§ 158.7 through 158.10 and in 44 FR 4403 shall be declassified if the designated DoD reviewer determines, in light of the declassification considerations contained in § 158.11 that classification no longer is required. In the absence of such a declassification determination, the classification of the information shall continue as long as required by national security considerations.

(e) Before any declassification or downgrading action, DoD information under review should be coordinated

with the Department of State on subjects cited in § 158.12, and with the Central Intelligence Agency (CIA) on subjects cited in § 158.13.

#### § 158.6 Responsibilities.

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

(1) Exercise oversight and policy supervision over the implementation of this part.

(2) Request DoD Components to review §§ 158.7 through 158.11 of this part every 5 years.

(3) Revise §§ 158.7 through 158.11 to ensure they meet DoD needs.

(4) Authorize, when appropriate, other Federal agencies to apply this part to DoD information in their possession.

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

(1) Recommend changes to §§ 158.7 through 158.13 of this part.

(2) Propose, with respect to specific programs, projects, and systems under his or her classification jurisdiction, supplements to §§ 158.7 through 158.11 of this part.

(3) Provide advice and designate experienced personnel to provide timely assistance to the Archivist of the United States in the systematic review of records under this part.

(c) The *Director, National Security Agency/Chief, Central Security Service (NSA/CSS)*, shall develop, for approval by the Secretary of Defense, special procedures for systematic review and declassification of classified cryptologic information.

(d) The *Archivist of the United States* is authorized to apply this part when reviewing DoD classified information that has been accessioned into the Archives of the United States.

#### § 158.7 Categories of information that require review before declassification.

The following categories of information shall be reviewed systematically for declassification by designated DoD review in accordance with this part:

(a) Nuclear propulsion information.

(b) Information concerning the establishment, operation, and support of the U.S. Atomic Energy Detection System.

(c) Information concerning the safeguarding of nuclear materials or facilities.

(d) Information that could affect the conduct of current or future U.S. foreign relations. (Also see § 158.12.)

(e) Information that could affect the current or future military usefulness of policies, programs, weapon systems, operations, or plans when such information would reveal courses of action, concepts, tactics, or techniques that are used in current operations plans.

(f) Research, development, test, and evaluation (RDT&E) of chemical and biological weapons and defensive systems; specific identification of chemical and biological agents and munitions; chemical and biological warfare plans; and U.S. vulnerability to chemical or biological warfare attack.

(g) Information about capabilities, installations, exercises, research, development, testing and evaluation, plans, operations, procedures, techniques, organization, training, sensitive liaison and relationships, and equipment concerning psychological operations; escape, evasion, rescue and recovery, insertion, and infiltration and exfiltration; cover and support; deception; unconventional warfare and special operations; and the personnel assigned to or engaged in these activities.

(h) Information that reveals sources or methods of intelligence or counterintelligence, counterintelligence activities, special activities, identities of clandestine human agents, methods of special operations, analytical techniques for the interpretation of intelligence data, and foreign intelligence reporting. This includes information that reveals the overall scope, processing rates, timeliness, and accuracy of intelligence systems and networks, including the means of interconnecting such systems and networks and their vulnerabilities.

(i) Information that relates to intelligence activities conducted jointly by the Department of Defense with other Federal agencies or to intelligence activities conducted by other Federal agencies in which the Department of Defense has provided support. (Also see § 158.13.)

§ 158.7

32 CFR Ch. I (7-1-02 Edition)

(j) Airborne radar and infrared imagery.

(k) Information that reveals space system:

(1) Design features, capabilities, and limitations (such as antijam characteristics, physical survivability features, command and control design details, design vulnerabilities, or vital parameters).

(2) Concepts of operation, orbital characteristics, orbital support methods, network configurations, deployments, ground support facility locations, and force structure.

(l) Information that reveals operational communications equipment and systems:

(1) Electronic counter-counter-measures (ECCM) design features or performance capabilities.

(2) Vulnerability and susceptibility to any or all types of electronic warfare.

(m) Information concerning electronic intelligence, telemetry intelligence, and electronic warfare (electronic warfare support measures, electronic countermeasures (ECM), and ECCM) or related activities, including:

(1) Information concerning or revealing nomenclatures, functions, technical characteristics, or descriptions of foreign communications and electronic equipment, its employment or deployment, and its association with weapon systems or military operations.

(2) Information concerning or revealing the processes, techniques, operations, or scope of activities involved in acquiring, analyzing, and evaluating the above information, and the degree of success obtained.

(n) Information concerning Department of the Army systems listed in §158.8.

(o) Information concerning Department of the Navy systems listed in §158.9.

(p) Information concerning Department of the Air Force systems listed in §158.10.

(q) Cryptologic information (including cryptologic sources and methods). This includes information concerning or revealing the processes, techniques, operations, and scope of SIGINT comprising communications intelligence, electronics intelligence, and telemetry

intelligence; and the cryptosecurity and emission security components of COMSEC, including the communications portion of cover and deception plans.

(1) Recognition of cryptologic information may not always be an easy task. There are several broad classes of cryptologic information, as follows:

(i) Those that relate to COMSEC. In documentary form, they provide COMSEC guidance or information. Many COMSEC documents and materials are accountable under the Communications Security Material Control System. Examples are items bearing transmission security (TSEC) nomenclature and crypto keying material for use in enciphering communications and other COMSEC documentation such as National COMSEC Instructions, National COMSEC/Emanations Security (EMSEC) Information Memoranda, National COMSEC Committee Policies, COMSEC Resources Program documents, COMSEC Equipment Engineering Bulletins, COMSEC Equipment System Descriptions, and COMSEC Technical Bulletins.

(ii) Those that relate to SIGINT. These appear as reports in various formats that bear security classifications, sometimes followed by five-letter codewords (World War II's ULTRA, for example) and often carrying warning caveats such as "This document contains codeword material" and "Utmost secrecy is necessary . . ." Formats may appear as messages having addressees, "from" and "to" sections, and as summaries with SIGINT content with or without other kinds of intelligence and comment.

(iii) RDT&E reports and information that relate to either COMSEC or SIGINT.

(2) Commonly used words that may help in identification of cryptologic documents and materials are "cipher," "code," "codeword," "communications intelligence" or "COMINT," "communications security" or "COMSEC," "cryptanalysis," "crypto," "cryptography," "cryptosystem," "decipher," "decode," "decrypt," "direction finding," "electronic intelligence" or

“ELINT,” “electronic security,” “encipher,” “encode,” “encrypt,” “intercept,” “key book,” “signals intelligence” or “SIGINT,” “signal security,” and “TEMPEST.”

**§ 158.8 Categories of information that require review before declassification: Department of the Army systems.**

The following categories of Army information shall be reviewed systematically for declassification by designated DoD reviewers in accordance with this part.

(a) Ballistic Missile Defense (BMD) missile information, including the principle of operation of warheads (fuzing, arming, and destruct operations); quality or reliability requirements; threat data; vulnerability; ECM and ECCM); details of design, assembly, and construction; and principle of operations.

(b) BMD systems data, including the concept definition (tentative roles, threat definition, and analysis and effectiveness); detailed quantitative technical system description-revealing capabilities or unique weaknesses that are exploitable; overall assessment of specific threat-revealing vulnerability or capability; discrimination technology; and details of operational concepts.

(c) BMD optics information that may provide signature characteristics of U.S. and United Kingdom ballistic weapons.

(d) Shaped-charge technology.

(e) Fleshettes.

(f) M380 Beehive round.

(g) Electromagnetic propulsion technology.

(h) Space weapons concepts.

(i) Radar-fuzing programs.

(j) Guided projectiles technology.

(k) ECM and ECCM to weapons systems.

(l) Armor materials concepts, designs, or research.

(m) 2.75-inch Rocket System.

(n) Air Defense Command and Coordination System (AN/TSQ-51).

(o) Airborne Target Acquisition and Fire Control System.

(p) Chaparral Missile System.

(q) Dragon Guided Missile System Surface Attack, M47.

(r) Forward Area Alerting Radar (FAAR) System.

(s) Ground laser designators.

(t) Hawk Guided Missile System.

(u) Heliborne, Laser, Air Defense Suppression and Fire and Forget Guided Missile System (HELLFIRE).

(v) Honest John Missile System.

(w) Lance Field Artillery Missile System.

(x) Land Combat Support System (LCSS).

(y) M22 (SS-11 ATGM) Guided Missile System, Helicopter Armament Subsystem.

(z) Guided Missile System, Air Defense (NIKE HERCULES with Improved Capabilities with HIPAR and ANTIJAM Improvement).

(aa) Patriot Air Defense Missile System.

(bb) Pershing IA Guided Missile System.

(cc) Pershing II Guided Missile System.

(dd) Guided Missile System, Intercept Aerial M41 (REDEYE) and Associated Equipment.

(ee) U.S. Roland Missile System.

(ff) Sergeant Missile System (less warhead) (as pertains to electronics and penetration aids only).

(gg) Shillelagh Missile System.

(hh) Stinger/Stinger-Post Guided Missile System (FIM-92A).

(ii) Terminally Guided Warhead (TWG) for Multiple Launch Rocket System (MLRS).

(jj) TOW Heavy Antitank Weapon System.

(kk) Viper Light Antitank/Assault Weapon System.

**§ 158.9 Categories of information that require review before declassification: Department of the Navy systems.**

The following categories of Navy information shall be reviewed systematically for declassification by designated DoD reviewers in accordance with this part.

(a) Naval nuclear propulsion information.

(b) Conventional surface ship information:

(1) Vulnerabilities of protective systems, specifically:

## § 158.10

(i) Passive protection information concerning ballistic torpedo and under-bottom protective systems.

(ii) Weapon protection requirement levels for conventional, nuclear, biological, or chemical weapons.

(iii) General arrangements, drawings, and booklets of general plans (applicable to carriers only).

(2) Ship-silencing information relative to:

(i) Signatures (acoustic, seismic, infrared, magnetic (including alternating magnetic (AM)), pressure, and underwater electric potential (UEP)).

(ii) Procedures and techniques for noise reduction pertaining to an individual ship's component.

(iii) Vibration data relating to hull and machinery.

(3) Operational characteristics related to performance as follows:

(i) Endurance or total fuel capacity.

(ii) Tactical information, such as times for ship turning, zero to maximum speed, and maximum to zero speed.

(c) All information that is uniquely applicable to nuclear-powered surface ships or submarines.

(d) Information concerning diesel submarines as follows:

(1) Ship-silencing data or acoustic warfare systems relative to:

(i) Oversight, platform, and sonar noise signature.

(ii) Radiated noise and echo response.

(iii) All vibration data.

(iv) Seismic, magnetic (including AM), pressure, and UEP signature data.

(2) Details of operational assignments, that is, war plans, antisubmarine warfare (ASW), and surveillance tasks.

(3) General arrangements, drawings, and plans of SS563 class submarine hulls.

(e) Sound Surveillance System (SOSUS) data.

(f) Information concerning mine warfare, mine sweeping, and mine countermeasures.

(g) ECM or ECCM features and capabilities of any electronic equipment.

(h) Torpedo information as follows:

(1) Torpedo countermeasures devices: T-MK6 (FANFARE) and NAE beacons.

## 32 CFR Ch. I (7-1-02 Edition)

(2) Tactical performance, tactical doctrine, and vulnerability to countermeasures.

(i) Design performance and functional characteristics of guided missiles, guided projectiles, sonars, radars, acoustic equipments, and fire control systems.

### § 158.10 Categories of information that require review before declassification: Department of the Air Force systems.

The Department of the Air Force has determined that the categories identified in §158.7 of this part shall apply to Air Force information.

### § 158.11 Declassification considerations.

(a) Technological developments; widespread public knowledge of the subject matter; changes in military plans, operations, systems, or equipment; changes in the foreign relations or defense commitments of the United States; and similar events may bear upon the determination of whether information should be declassified. If the responsible DoD reviewer decides that, in view of such circumstances, the public disclosure of the information being reviewed no longer would result in damage to the national security, the information shall be declassified.

(b) The following are examples of considerations that may be appropriate in deciding whether information in the categories listed in §§158.7 through 158.10 may be declassified when it is reviewed:

(1) The information no longer provides the United States a scientific, engineering, technical, operational, intelligence, strategic, or tactical advantage over other nations.

(2) The operational military capability of the United States revealed by the information no longer constitutes a limitation on the effectiveness of the Armed Forces.

(3) The information is pertinent to a system that no longer is used or relied on for the defense of the United States or its allies and does not disclose the capabilities or vulnerabilities of existing operational systems.

(4) The program, project, or system information no longer reveals a current weakness or vulnerability.

(5) The information pertains to an intelligence objective or diplomatic initiative that has been abandoned or achieved and will no longer damage the foreign relations of the United States.

(6) The information reveals the fact or identity of a U.S. intelligence source, method, or capability that no longer is employed and that relates to no current source, method, or capability that upon disclosure could cause damage to national security or place a person in immediate jeopardy.

(7) The information concerns foreign relations matters whose disclosure can no longer be expected to cause or increase international tension to the detriment of the national security of the United States.

(c) Declassification of information that reveals the identities of clandestine human agents shall be accomplished only in accordance with procedures established by the Director of Central Intelligence for that purpose.

(d) The NSA/CSS is the sole authority for the review and declassification of classified cryptologic information. The procedures established by the NSA/CSS to facilitate the review and declassification of classified cryptologic information are:

(1) *COMSEC documents and materials.*

(i) If records or materials in this category are found in agency files that are not under COMSEC control, refer them to the senior COMSEC authority of the agency concerned or by appropriate channels to the following address: Director, National Security Agency, Attn: Director of Policy (Q4), Fort George G. Meade, Maryland 20755.

(ii) If the COMSEC information has been incorporated into other documents by the receiving agency, referral to the NSA/CSS is necessary before declassification.

(2) *SIGINT information.* (i) If the SIGINT information is contained in a document or record originated by a DoD cryptologic organization, such as the NSA/CSS, and is in the files of a noncryptologic agency, such material will not be declassified if retained in accordance with an approved records disposition schedule. If the material

must be retained, it shall be referred to the NSA/CSS for systematic review for declassification.

(ii) If the SIGINT information has been incorporated by the receiving agency into documents it produces, referral to the NSA/CSS is necessary before any declassification.

**§ 158.12 Department of State areas of interest.**

(a) Statements of U.S. intent to defend, or not to defend, identifiable areas, or along identifiable lines, in any foreign country or region.

(b) Statements of U.S. intent militarily to attack in stated contingencies identifiable areas in any foreign country or region.

(c) Statements of U.S. policies or initiatives within collective security organizations (for example, North Atlantic Treaty Organization (NATO) and Organization of American States (OAS)).

(d) Agreements with foreign countries for the use of, or access to, military facilities.

(e) Contingency plans insofar as they involve other countries, the use of foreign bases, territory or airspace, or the use of chemical, biological, or nuclear weapons.

(f) Defense surveys of foreign territories for purposes of basing or use in contingencies.

(g) Reports documenting conversations with foreign officials, that is, foreign government information.

**§ 158.13 Central Intelligence Agency areas of interest.**

(a) Cryptologic, cryptographic, or SIGINT. (Information in this category shall continue to be forwarded to the NSA/CSS in accordance with § 158.11(d). The NSA/CSS shall arrange for necessary coordination.)

(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

§ 158.13

32 CFR Ch. I (7-1-02 Edition)

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.