

§ 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 (7-1-98 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