SUBJECT: Guidelines for Systematic Declassification Review of Classified Information in Permanently Valuable DoD Records

(b) Executive Order 12356, "National Security Information," April 2, 1982
(c) Information Security Oversight Office Directive No. 1 Concerning National Security Information, June 23, 1982
(d) through (g), see enclosure 1

1. REISSUANCE AND PURPOSE

This Directive reissues reference (a); establishes procedures and assigns responsibilities for the systematic declassification review of information classified under references (b) and (c), DoD Directive 5200.1 and DoD 5200.1-R (references (d) and (e)), and prior orders, Directives, and Regulations governing security classification; and implements section 3.3. of reference (b).

2. APPLICABILITY AND SCOPE

2.1. This Directive 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").
2.2. This Directive applies to the systematic review of permanently valuable classified information, developed by or for the Department of Defense and its Components, or its predecessor Components and activities, that is under the exclusive or final original classification jurisdiction of the Department of Defense.

2.3. Its provisions do not cover Restricted Data or Formerly Restricted Data under the Atomic Energy Act of 1954 (reference (f)) or information in non-permanent records.

2.4. 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.

3. DEFINITIONS

3.1. **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).

3.2. **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.

3.3. **Intelligence Method.** Any process, mode of analysis, means of gathering data, or processing system or equipment used to produce intelligence.

3.4. **Intelligence Source.** A person or technical means that provides intelligence.

4. POLICY

It is the policy of the Department of Defense to ensure 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.
5. **PROCEDURES**

5.1. DoD classified information that is permanently valuable, as defined by 44 U.S.C. 2103 (reference (g)), 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.

5.2. All other DoD classified information and foreign government information that is permanently valuable and in the possession or control of the 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.

5.3. DoD classified information and foreign government information in the possession or control of the 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 enclosure 2 or 3.

5.4. Systematic review for declassification shall be in accordance with procedures contained in DoD 5200.1-R (reference (e)). Information that falls within any of the categories in enclosures 2 and 3 shall be declassified if the designated DoD reviewer determines, in light of the declassification considerations contained in enclosure 4, 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.

5.5. Before any declassification or downgrading action, DoD information under review should be coordinated with the Department of State on subjects cited in enclosure 5, and with the Central Intelligence Agency (CIA) on subjects cited in enclosure 6.
6. RESPONSIBILITIES

6.1. The Deputy Under Secretary of Defense for Policy shall:

6.1.1. Exercise oversight and policy supervision over the implementation of this Directive.

6.1.2. Request the DoD Components to review enclosures 2 and 4 of this Directive every 5 years.

6.1.3. Revise enclosures 2 and 4 to ensure they meet DoD needs.

6.1.4. Authorize, when appropriate, other Federal Agencies to apply this Directive to DoD information in their possession.

6.2. The Head of each DoD Component shall:

6.2.1. Recommend changes to the enclosures of this Directive.

6.2.2. Propose, with respect to specific programs, projects, and systems under his or her classification jurisdiction, supplements to enclosures 2 and 4 of this Directive.

6.2.3. 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 Directive.

6.3. 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.

6.4. The Archivist of the United States is authorized to apply this Directive when reviewing DoD classified information that has been accessioned into the Archives of the United States.
7. EFFECTIVE DATE

This Directive is effective immediately.

Enclosures - 6

E1. References, continued
E2. Categories of Information That Require Review Before Declassification
E4. Declassification Considerations
E5. Department of State Areas of Interest
E6. Central Intelligence Agency Areas of Interest
E1. ENCLOSED 1

REFERENCES, continued

(e) DoD 5200.1-R, "Information Security Program Regulation, August 1982
(f) Public Law 83-703, Atomic Energy Act of 1954
(g) Section 2103 of title 44, United States Code
E2. ENCLOSURE 2

CATEGORIES OF INFORMATION THAT REQUIRE REVIEW BEFORE DECLASSIFICATION

E2.1.1. The following categories of information shall be reviewed systematically for declassification by designated DoD reviewers in accordance with this Directive:

E2.1.1.1. Nuclear propulsion information.

E2.1.1.2. Information concerning the establishment, operation, and support of the U.S. Atomic Energy Detection System.

E2.1.1.3. Information concerning the safeguarding of nuclear materials or facilities.

E2.1.1.4. Information that could affect the conduct of current or future U.S. foreign relations. (Also see enclosure 5.)

E2.1.1.5. 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.

E2.1.1.6. 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.

E2.1.1.7. 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.

E2.1.1.8. 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.

E2.1.1.9. 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 enclosure 6.)

E2.1.1.10. Airborne radar and infrared imagery.

E2.1.1.11. Information that reveals space system:

E2.1.1.11.1. Design features, capabilities, and limitations (such as anti-jam characteristics, physical survivability features, command and control design details, design vulnerabilities, or vital parameters).

E2.1.1.11.2. Concepts of operation, orbital characteristics, orbital support methods, network configurations, deployments, ground support facility locations, and force structure.

E2.1.1.12. Information that reveals operational communications equipment and systems:

E2.1.1.12.1. Electronic counter-countermeasures (ECCM) design features or performance capabilities.

E2.1.1.12.2. Vulnerability and susceptibility to any or all types of electronic warfare.

E2.1.1.13. Information concerning electronic intelligence, telemetry intelligence, and electronic warfare (electronic warfare support measures, electronic countermeasures (ECM), and ECCM) or related activities, including:

E2.1.1.13.1. 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.

E2.1.1.13.2. 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.

E2.1.1.15. Information concerning Department of the Navy systems listed in attachment E2.A2.


E2.1.1.17. 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.

E2.1.1.17.1. Recognition of cryptologic information may not always be an easy task. There are several broad classes of cryptologic information, as follows:

E2.1.1.17.1.1. 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.
E2.1.17.1.2. Those that relate to SIGINT. These appear as reports in various formats that bear security classifications, sometimes followed by five-letter code words (World War II's ULTRA, for example) and often carrying warning caveats such as "This document contains code word 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.

E2.1.17.1.3. RDT&E reports and information that relate to either COMSEC or SIGINT.


Attachments - 3
  E1.A1. Department of the Army Systems
  E2.A2. Department of the Navy Systems
  E3.A3. Department of the Air Force Systems
E2.A1. ATTACHMENT 1 TO ENCLOSURE 2

CATEGORIES OF INFORMATION THAT REQUIRE REVIEW BEFORE DECLASSIFICATION DEPARTMENT OF THE ARMY SYSTEMS

E2.A1.1.1. The following categories of Army information shall be reviewed systematically for declassification by designated DoD reviewers in accordance with this Directive.

E2.A1.1.1.1. Ballistic Missile Defense (BMD) missile information, including the principle of operation of warheads (fuzing, arming, firing, and destruct operations); quality or reliability requirements; threat data; vulnerability; ECM and ECCM; details of design, assembly, and construction; and principle of operations.

E2.A1.1.1.2. 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.

E2.A1.1.1.3. BMD optics information that may provide signature characteristics of U.S. and United Kingdom ballistic weapons.


E2.A1.1.1.11. ECM and ECCM to weapons systems.


E2.A1.1.1.32. Sergeant Missile System (less warhead) (as pertains to electronics and penetration aids only).


E2.A1.1.1.35. Terminally Guided Warhead (TWG) for Multiple Launch Rocket System (MLRS).


E2.A2. ATTACHMENT 2 TO ENCLOSURE 2

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 Directive.


E2.A2.1.2. Conventional surface ship information:

E2.A2.1.2.1. Vulnerabilities of protective systems, specifically:

E2.A2.1.2.1.1. Passive protection information concerning ballistic torpedo and underbottom protective systems.

E2.A2.1.2.1.2. Weapon protection requirement levels for conventional, nuclear, biological, or chemical weapons.

E2.A2.1.2.1.3. General arrangements, drawings, and booklets of general plans (applicable to carriers only).

E2.A2.1.2.2. Ship-silencing information relative to:

E2.A2.1.2.2.1. Signatures (acoustic, seismic, infrared, magnetic (including alternating magnetic (AM)), pressure, and underwater electric potential (UEP)).

E2.A2.1.2.2.2. Procedures and techniques for noise reduction pertaining to an individual ship’s component.

E2.A2.1.2.2.3. Vibration data relating to hull and machinery.

E2.A2.1.2.3. Operational characteristics related to performance as follows:

E2.A2.1.2.3.1. Endurance or total fuel capacity.

E2.A2.1.2.3.2. Tactical information, such as times for ship turning, zero to maximum speed, and maximum to zero speed.
E2.A2.1.3. All information that is uniquely applicable to nuclear-powered surface ships or submarines.

E2.A2.1.4. Information concerning diesel submarines as follows:

   E2.A2.1.4.1. Ship-silencing data or acoustic warfare systems relative to:

      E2.A2.1.4.1.2. Radiated noise and echo response.
      E2.A2.1.4.1.3. All vibration data.
      E2.A2.1.4.1.4. Seismic, magnetic (including AM), pressure, and UEP signature data.

      E2.A2.1.4.2. Details of operational assignments, that is, war plans, antisubmarine warfare (ASW), and surveillance tasks.

      E2.A2.1.4.3. General arrangements, drawings, and plans of SS563 class submarine hulls.

   E2.A2.1.5. Sound Surveillance System (SOSUS) data.


      E2.A2.1.7. ECM or ECCM features and capabilities of any electronic equipment.

      E2.A2.1.8. Torpedo information as follows:


         E2.A2.1.8.2. Tactical performance, tactical doctrine, and vulnerability to countermeasures.

The Department of the Air Force has determined that the categories identified in enclosure 2 of this Directive shall apply to Air Force information.
E3. ENCLOSURE 3

Monday
January 31, 1983

Part III

Information Security Oversight Office

National Security Information; General Guidelines for Systematic Declassification
Review of Foreign Government Information; Final Rule
INFORMATION SECURITY OVERSIGHT OFFICE

32 CFR Part 2002

National Security Information; General Guidelines for Systematic Declassification Review of Foreign Government Information

AGENCY: Information Security Oversight Office (ISOO).

ACTION: Final rule.

SUMMARY: The Information Security Oversight Office is revising its guidelines which relate to the systematic declassification review of foreign government information. These guidelines are issued pursuant to the provisions of Section 3.3 of Executive Order 12356, which superseded Executive Order 12065. The Executive Order prescribes a uniform information security system; it also requires the establishment of guidelines for the systematic declassification review of certain information. The purpose of these guidelines is to assist in implementing Executive Order 12356.

EFFECTIVE DATE: January 31, 1983.

FOR FURTHER INFORMATION CONTACT: Steven Garfinkel, Director, ISOO. Telephone: 202-803-7251.

SUPPLEMENTARY INFORMATION:

List of Subjects in 32 CFR Part 2002

Archives and records, classified information, Executive orders, Information, Intelligence, National defense, National security information, Presidential documents, Security information.

Title 32 of the Code of Federal Regulations, Part 2002, is revised as follows:

PART 2002—GENERAL GUIDELINES FOR SYSTEMATIC DECLASSIFICATION REVIEW OF FOREIGN GOVERNMENT INFORMATION

Sec. 2002.1 Purpose.
Sec. 2002.2 Definition.
Sec. 2002.3 Scope.
Sec. 2002.4 Responsibilities.
Sec. 2002.5 Effect of publication.
Sec. 2002.6 Categories requiring item-by-item review.
Sec. 2002.7 Referral and discussion.
Sec. 2002.8 Downgrading.

Authority: Sec. 3.3, E.O. 12356, 47 FR 14874, April 8, 1982.

§ 2002.1 Purpose.

These general guidelines for the systematic declassification review of foreign government information have been developed in accordance with the provisions of Section 3.3 of Executive Order 12356, "National Security Information," and Section 2002.31 of Information Security Oversight Office Directive No. 1. All foreign government information that has been incorporated into the permanently valuable records of the United States Government and that has been accessioned into the National Archives of the United States shall be systematically reviewed for declassification by the Archivist of the United States. Declassification reviews shall be conducted in accordance with the provisions of these guidelines or, if available, in accordance with specific systematic review guidelines for foreign government information provided by the agency heads who have declassification authority over that information. All foreign government information is not identified in § 2002.6 of these general guidelines or in specific agency guidelines as requiring item-by-item declassification review and final determination by an agency declassification authority, and (b) for which a prior declassification date has not been established, shall be declassified as that information becomes thirty years old.

§ 2002.2 Definition.

"Foreign government information" as used in these guidelines means:

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

(b) Information 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.

§ 2002.3 Scope.

(a) These guidelines apply to foreign government information that has been received or classified by the United States Government or its agents and has been incorporated into records determined by the Archivist of the United States to have permanent value.

(b) Atomic energy information [including information originated prior to 1947 and not marked as such] information received from the United Kingdom or Canada marked "Atomic," or information received from NATO marked "Atalym") that is defined and identified as "Restricted Data" or "Formerly Restricted Data" in Sections 11y and 1142 of the Atomic Energy Act of 1954, as amended, is outside the scope of these guidelines. Such information is not subject to systematic review and may not be automatically downgraded or declassified. Any document containing information within the definition of "Restricted Data" or "Formerly Restricted Data" that is not so marked shall be referred to the Department of Energy Office of Classification for review and appropriate marking, except for licensing and related regulatory matters which shall be referred to the Division of Security, U.S. Nuclear Regulatory Commission.

§ 2002.4 Responsibilities.

(a) Foreign government information transferred to the General Services Administration for accession into the National Archives of the United States shall be reviewed by the Archivist of the United States for declassification in accordance with Executive Order 12356, the directives of the Information Security Oversight Office, these general guidelines, and any specific systematic declassification guidelines provided by the agency with declassification authority over the information.

(b) Accessioned foreign government information in file series concerning intelligence activities (including special activities), or intelligence sources or methods created after 1945, and cryptography records created after 1945, shall be subject to review by the Archivist for declassification as it becomes 50 years old. All other accessioned foreign government information shall be subject to review by the Archivist for declassification as it becomes 30 years old.

(c) Agency heads who have declassification responsibility over permanently valuable foreign government information in agency records not yet accessioned into the National Archives of the United States are encouraged to conduct systematic declassification reviews of it in accordance with the time limits specified in paragraph (b) of this section. These reviews shall comply with the provisions of Executive Order 12356, the directives of the Information Security Oversight Office, these general guidelines, and specific agency systematic review guidelines that have been issued in consultation with the Archivist of the United States and the ISOO Director.
(d) Foreign government information falling within any of the categories listed in §202.5 of these guidelines shall be declassified by agencies having declassification authority over it, or shall be exempted from declassification under any joint arrangement evidenced by an exchange of letters, memorandum of understanding, or other written record, with the foreign government or international organization of governments, or element(s) thereof, that furnished the information. Questions concerning the existence or applicability of such arrangements shall be referred to the agency or agencies having declassification authority over the records under review.

(b) Information related to the safeguarding of nuclear materials or facilities foreign and domestic, including but not necessarily limited to vulnerabilities and vulnerability assessments of nuclear facilities and Special Nuclear Material.

(c) Nuclear weapon control information (see also paragraph (k) of this section).

(d) Information regarding foreign nuclear programs (other than "Restricted Data" and "Formerly Restricted Data"), such as:

1. Nuclear weapon testing;
2. Nuclear weapons storage and stockpile;
3. Nuclear weapons effects, hardness, and vulnerability;
4. Nuclear weapons safety;
5. Cooperation in nuclear programs including, but not limited to, peaceful and military applications of nuclear energy;
6. Exploration, production and import of uranium and thorium from foreign countries.

(e) Information concerning intelligence activities (including special activities) or intelligence or counterintelligence sources or methods including but not limited to intelligence, counterintelligence and covert action programs, plans, policies, operations or assessments, or which would reveal or identify:

1. Any present, past or prospective undercover personnel, installation, unit or clandestine human agent of the United States or a foreign government;
2. Any present, past or prospective method, procedure, mode, technique or requirement used or being developed by the United States or by foreign governments, individually or in combination to produce, acquire, transmit, analyze, correlate, assess, evaluate or process intelligence or counterintelligence, or to support an intelligence or counterintelligence source, operation, or activity;
3. The present, past or proposed existence of any joint United States and foreign government intelligence, counterintelligence, or covert action activity or facility, or the nature thereof.


(f) Information that could result in or lead to actions which would place an individual in jeopardy attributable to disclosure of the information, including but not limited to:

1. Information identifying any individual or organization as a confidential source of intelligence or counterintelligence.
2. Information revealing the identity of an intelligence or covert action agent or agent.
3. Information identifying any individual or organization used to develop or support intelligence, counterintelligence, or covert action agents, sources, or activities.
4. Information about foreign intelligence organizations or entities which if disclosed, could be expected to:
5. Adversely affect a foreign country's or international organization's present or future relations with the United States.
6. Adversely affect present or future confidential exchanges between the United States and any foreign government or international organization of governments.
7. Information related to plans (whether executed or not) whether presented in whole or in part, programs, operations, negotiations, and assessments shared by one or several foreign governments with the United States, including, but not limited to, those involving the territorial, political, or economic interest of foreign governments or government of another country, and which if disclosed could be expected to adversely affect the conduct of U.S. foreign policy or the conduct of another country's foreign policy with respect to a third country or countries. This item would include contingency plans, plans for covert political, military or paramilitary activities or operations by a foreign government acting alone or jointly with the United States Government, and positions or actions taken by the foreign government alone or jointly with the United States concerning border disputes or other territorial issues.

(i) Information concerning arrangements with respect to foreign banking of cryptographic operations and/or foreign policy considerations relating thereto.
DODD 5200.30, March 21, 1983

ENCLOSURE 3

[Text content]

DOD 5200.30, March 21, 1983

20 ENCLOSURE 3
§ 2002.8 Downgrading.

Foreign government information classified "Top Secret" may be downgraded to "Secret" after 30 years unless the agency with declassification authority over it determines, on its own, or after consultation, as appropriate, with the foreign government or international organization of governments which furnished the information, that it requires continued protection at the "Top Secret" level.

Date: January 27, 1983.

Steven Garfinkel,
Director, Information Security Oversight Office.
E4. ENCLOSURE 4

DECLASSIFICATION CONSIDERATIONS

E4.1.1. 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.

E4.1.2. The following are examples of considerations that may be appropriate in deciding whether information in the categories listed in enclosure 2 may be declassified when it is reviewed:

E4.1.2.1. The information no longer provides the United States a scientific, engineering, technical, operational, intelligence, strategic, or tactical advantage over other nations.

E4.1.2.2. The operational military capability of the United States revealed by the information no longer constitutes a limitation on the effectiveness of the Armed Forces.

E4.1.2.3. 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.

E4.1.2.4. The program, project, or system information no longer reveals a current weakness or vulnerability.

E4.1.2.5. 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.

E4.1.2.6. 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.
E4.1.2.7. 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.

E4.1.3. 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.

E4.1.4. 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:

E4.1.4.1. **COMSEC Documents and Materials**

E4.1.4.1.1. 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:

National Security Agency
ATTN: Director of Policy (Q4)
Fort George G. Meade, MD 20755

E4.1.4.1.2. If the COMSEC information has been incorporated into other documents by the receiving Agency, referral to the NSA/CSS is necessary before declassification.

E4.1.4.2. **SIGINT Information**

E4.1.4.2.1. 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 non-cryptologic 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.

E4.1.4.2.2. 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.
E5. ENCLOSURE 5

DEPARTMENT OF STATE AREAS OF INTEREST

E5.1.1. Statements of U.S. intent to defend, or not to defend, identifiable areas, or along identifiable lines, in any foreign country or region.

E5.1.2. Statements of U.S. intent militarily to attack in stated contingencies identifiable areas in any foreign country or region.

E5.1.3. Statements of U.S. policies or initiatives within collective security organizations (for example, North Atlantic Treaty Organization (NATO) and Organization of American States (OAS)).

E5.1.4. Agreements with foreign countries for the use of, or access to, military facilities.

E5.1.5. 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.

E5.1.6. Defense surveys of foreign territories for purposes of basing or use in contingencies.

E5.1.7. Reports documenting conversations with foreign officials, that is, foreign government information.
E6. ENCLOSURE 6

CENTRAL INTELLIGENCE AGENCY AREAS OF INTEREST

E6.1.1. Cryptologic, cryptographic, or SIGINT. (Information in this category shall continue to be forwarded to the NSA/CSS in accordance with enclosure 4, paragraph E4.1.4. The NSA/CSS shall arrange for necessary coordination.)

E6.1.2. Counterintelligence.

E6.1.3. Special access programs.

E6.1.4. Information that identifies clandestine organizations, agents, sources, or methods.

E6.1.5. Information on personnel under official or nonofficial cover or revelation of a cover arrangement.

E6.1.6. Covertly obtained intelligence reports and the derivative information that would divulge intelligence sources or methods.

E6.1.7. Methods or procedures used to acquire, produce, or support intelligence activities.

E6.1.8. CIA structure, size, installations, security, objectives, and budget.

E6.1.9. Information that would divulge intelligence interests, value, or extent of knowledge on a subject.

E6.1.10. Training provided to or by the CIA that would indicate its capability or identify personnel.

E6.1.11. Personnel recruiting, hiring, training, assignment, and evaluation policies.

E6.1.12. Information that could lead to foreign political, economic, or military action against the United States or its allies.

E6.1.13. Events leading to international tension that would affect U.S. foreign policy.
E6.1.14. Diplomatic or economic activities affecting national security or international security negotiations.

E6.1.15. Information affecting U.S. plans to meet diplomatic contingencies affecting national security.


E6.1.17. U.S. surreptitious collection in a foreign nation that would affect relations with the country.

E6.1.18. Covert relationships with international organizations or foreign governments.

E6.1.19. Information related to political or economic instabilities in a foreign country threatening American lives and installations therein.


E6.1.21. U.S. and allies' defense plans and capabilities that enable a foreign entity to develop countermeasures.

E6.1.22. Information disclosing U.S. systems and weapons capabilities or deployment.

E6.1.23. Information on research, development, and engineering that enables the United States to maintain an advantage of value to national security.


E6.1.25. U.S. nuclear programs and facilities.


E6.1.27. Contractual relationships that reveal the specific interest and expertise of the CIA.

E6.1.28. Information that could result in action placing an individual in jeopardy.
E6.1.29. Information on secret writing when it relates to specific chemicals, reagents, developers, and microdots.

E6.1.30. Reports of the Foreign Broadcast Information Service (FBIS) (-- Branch, -- Division) between July 31, 1946, and December 31, 1950, marked CONFIDENTIAL or above.

E6.1.31. Reports of the Foreign Documents Division between 1946 and 1950 marked RESTRICTED or above.

E6.1.32. Q information reports.

E6.1.33. FDD translations.

E6.1.34. U reports.