



POLICY

Approved For Release 2006/01/12 : CIA-RDP93B01194R000900060002-5

OFFICE OF THE UNDER SECRETARY OF DEFENSE

WASHINGTON, D.C. 20301

OIS Registry  
87-160/4

06 NOV 1981

STAT

[Redacted]

Directorate of Administration  
Central Intelligence Agency  
Washington, D.C. 20505

STAT

[Redacted]

By letter (I-04123/81) of 12 February 1981 your Agency was furnished a copy of this Department's guidelines for systematic declassification review of 20-year-old classified DoD information. Since that time these guidelines have been revised.

For your information and use I have attached a copy of these guidelines (DoD Directive 5200.30, "Guidelines for Systematic Review of 20-Year-Old Classified Information in Permanently Valuable DoD Records," September 9, 1981).

Please contact me in the event that you have any questions concerning the revised guidelines.

Sincerely,

Arthur F. Van Cook  
Director of Information Security

Attachment

On file OSD release instructions apply.

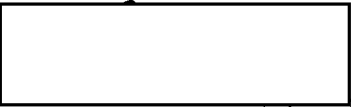
TO: (Name, office symbol, room number, building, Agency/Post)	Initials	Date
1. Chief, CRD		24 Nov 81
2. C/OPS		27 Nov 81
3. C/AOM - NO QUESTIONS		27 NOV 81
4. C/INT		30 Nov 81
5. C/SJT		11-30

Action	File	Note and Return
Approval	For Clearance	Per Conversation
As Requested	For Correction	Prepare Reply
Circulate	For Your Information	See Me
Comment	Investigate	Signature
Coordination	Justify	

REMARKS C/CRD \_\_\_\_\_

Attached is a letter from DoD forwarding their guidelines for systematic classification review for your retention.

If there are any questions, please draft a letter for DIS' signature.



1 TO ALL: ANY QUESTIONS, COMMENTS, ETC.? DOES IT APPEAR THAT OUR MATERIAL WILL BE PROTECTED? IF NOT, WHAT DO YOU SUGGEST WE SEND TO DOD? MAY I HAVE YOUR REACTIONS NLT 11 DEC.

2-1: Info in Declassification Considerations (Encl 3) re intel sources is confusing (paras 25+3). DO NOT use this form as a RECORD of approvals, concurrences, disposals, clearances, and similar actions. C/ER

FROM: (Name, org. symbol, Agency/Post) Room No.—Bldg.  
 Executive Officer, OIS 1206 Ames

STAT

STAT

STAT

STAT

Are clandestine human agents included in  
2 f? Approved For Release 2006/01/12 : CIA-RDP93B01194R000900060002-5

Enclosure 2 seems to include everything  
we want covered in items 4, 7, 8, + 10. One  
question is whether they can identify admin  
records that relate to cover used by us?  
Problems similar to those in State records.

**3-1 THE GUIDELINES ARE FOR OUR INFORMATION-**  
**THEY ARE VERY GENERAL - OUR BEST**  
**PROTECTION IS TO KEEP TRACK OF WHAT**  
**DOB IS DOING BY AN OCCASIONAL VISIT &**  
**CHECK.**



September 9, 1981  
NUMBER 5200.30

USD(P)

## Department of Defense Directive

SUBJECT: Guidelines for Systematic Review of 20-Year-Old Classified Information in Permanently Valuable DoD Records

- References:
- (a) DoD Directive 5200.30, subject as above, June 18, 1979 (hereby canceled)
  - (b) Executive Order 12065, "National Security Information," June 28, 1978
  - (c) Information Security Oversight Office Directive No. 1 Concerning National Security Information, October 2, 1978 (43 FR 194)
  - (d) DoD Directive 5200.1, "DoD Information Security Program," November 29, 1978
  - (e) through (g), see enclosure 1

### A. REISSUANCE AND PURPOSE

This Directive reissues reference (a); establishes guidelines for the systematic declassification review of 20-year-old information classified under references (b) through (e) and prior orders, directives, and regulations governing security classification; implements section 3-402 of reference (b); and delegates authority to implement the DoD systematic declassification review guidelines.

### B. APPLICABILITY AND SCOPE

1. The provisions of this Directive apply to the Office of the Secretary of Defense and to activities assigned for administrative support, the Military Departments, the Organization of the Joint Chiefs of Staff (OJCS), the Unified and Specified Commands, and the Defense Agencies (hereafter referred to as "DoD Components").
2. This Directive applies to the systematic review of 20-year-old permanently valuable classified information, material, or records developed by or for the Department of Defense and its Components, or its predecessor components and activities, that are under the exclusive or final original classification jurisdiction of the Department of Defense.
3. Information that is foreign government information; Restricted Data or Formerly Restricted Data under the Atomic Energy Act of 1954; or in nonpermanent records is outside the scope of this Directive.

C. DEFINITIONS

1. Cryptologic Information. Information pertaining to the activities and operations involved in the production of signals intelligence or to the maintenance of communications security (COMSEC).
2. Intelligence Method. Any human or technological method that is or may be used to collect or analyze foreign intelligence or foreign counterintelligence.
3. Intelligence Source. Any human or technological source from which foreign intelligence or foreign counterintelligence is, has been, or may be derived.
4. Foreign Government Information. Information that is provided to the United States by a foreign government or international organization of governments in the expectation, expressed or implied, that the information is to be kept in confidence; or produced by the United States under a written joint arrangement with a foreign government or international organization of governments requiring that either the information or the arrangement, or both, be kept in confidence. Such a written joint arrangement may be evidenced by an exchange of letters, a memorandum of understanding, or other written record.

D. POLICY AND PROCEDURES

1. DoD classified information that is permanently valuable, as defined by 44 U.S.C. 2103 (reference (f)), shall be systematically reviewed for declassification when it is 20 years old whether the information:
  - a. Has been transferred to the General Services Administration for accession into the Archives of the United States or is in the possession and control of the Administrator of General Services under 44 U.S.C. 2107 or 2107 note (reference (f)), or
  - b. Is in the possession or control of DoD Components.
2. The transition to systematic review at 20 vice 30 years shall be implemented as rapidly as possible, and completed by December 1, 1988.
3. When DoD classified information becomes 20 years old, it shall be:
  - a. Declassified automatically if it is not within one of the categories specified in enclosure 2.
  - b. Reviewed for declassification by responsible DoD reviewers in accordance with enclosure 3, if it is within any of the categories specified in enclosure 2.
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 enclosure 2 shall be declassified if the desig-

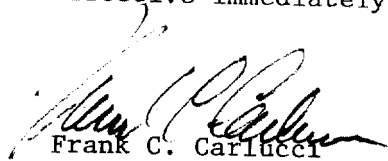
nated DoD reviewer determines, in light of the declassification considerations of enclosure 3, that classification is no longer required. In the absence of such a determination, the designated DoD reviewer shall recommend continued classification in accordance with the procedures of DoD 5200.1-R (reference (e)). Enclosure 4 is a listing of those categories of DoD information the classification of which has been extended beyond 20 years by the Secretary of Defense.

E. RESPONSIBILITY AND AUTHORITY

1. The Deputy Under Secretary of Defense for Policy shall:
  - a. Exercise oversight and policy supervision over the implementation of this Directive;
  - b. Request DoD Components to review enclosures 2 and 3 of this Directive every 2 years;
  - c. Revise enclosures 2, 3, and 4 to ensure they meet DoD needs; and
  - d. Authorize, when appropriate, other departments and agencies to apply the guidelines of this Directive to DoD information in their possession.
2. The Head of each DoD Component shall:
  - a. Recommend changes to enclosures 2 and 3 of this Directive;
  - b. Propose, with respect to specific programs, projects, and systems under their classification jurisdiction, supplements to enclosures 2 and 3 of this Directive;
  - c. Ensure that the records of the Component that have not been accessioned by the Archivist of the United States and, upon request of the Archivist, those that have been accessioned are reviewed by DoD personnel designated for the purpose in accordance with this Directive; and
  - d. Provide advice and assistance to the Archivist of the United States in the systematic review of records under this Directive.
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.
4. The Archivist of the United States is authorized to apply this Directive when reviewing 20-year-old DoD classified information that has been accessioned into the Archives of the United States.

F. EFFECTIVE DATE

The provisions of this Directive are effective immediately.



Frank C. Carlucci  
Deputy Secretary of Defense

Enclosures - 4

1. References
2. Categories of Information to be Reviewed for Declassification
3. Declassification Considerations
4. Categories of Information for which Classification has been Extended Beyond 20 Years by the Secretary of Defense

REFERENCES, continued

- (e) DoD 5200.1-R, "Information Security Program Regulation," October 1980, authorized by DoD Directive 5200.1, November 29, 1978
- (f) Title 44, United States Code, Sections 2103 and 2107
- (g) Executive Order 12036, "United States Intelligence Activities," January 24, 1978



CATEGORIES OF INFORMATION TO BE REVIEWED FOR DECLASSIFICATION

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

1. Nuclear propulsion information.
2. Information concerning the establishment, operation, and support of the U.S. Atomic Energy Detection System, unless otherwise specified by the Joint Department of Energy - Department of Defense Classification Guide for the Nuclear Test Detection Satellite.
3. Information concerning the safeguarding of nuclear materials or facilities.
4. Information that could affect the conduct of current or future U.S. foreign relations, such as plans (whether or not executed) and programs relating to current international security affairs.
5. Information that could affect the current or future military usefulness of policies, programs, weapon systems, operations, or plans.
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.
7. Information concerning or revealing psychological warfare, escape, evasion, cover, or deception plans, procedures, and techniques.
8. Information that reveals sources and methods of intelligence, counterintelligence activities, identities of clandestine human agents, methods of special operations, and analytical techniques for the interpretation of intelligence data. 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.
9. Airborne radar and infrared imagery.
10. Information that reveals space system:
  - a. Design features, capabilities, and limitations (such as antijam characteristics, physical survivability features, command and control design details, design vulnerabilities, or vital parameters).
  - b. Concepts of operation, orbital characteristics, orbital support methods, network configurations, deployments, ground support facility locations, and force structure.
11. Information that reveals operational communications equipment and systems:
  - a. Electronic counter-countermeasures (ECCM) design features or performance capabilities; and

- b. Vulnerability and susceptibility to any or all types of electronic warfare.
12. Information concerning Department of the Army systems listed in attachment A.
13. Information concerning Department of the Navy systems listed in attachment B.
14. Information concerning Department of the Air Force systems listed in attachment C.
15. Information concerning electronic intelligence, telemetry intelligence, and electronic warfare (electronic warfare support measures, electronic countermeasures (ECM), and ECCM) or related activities to include:
  - a. 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.
  - b. 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.
16. Cryptologic information (including cryptologic sources and methods) currently in use. This includes information concerning or revealing the processes, techniques, operations, and scope of signals intelligence (SIGINT) comprising communications intelligence, electronics intelligence, and telemetry intelligence; and the cryptosecurity and emission security components of communications security, including the communications portion of cover and deception plans.
  - a. Recognition of cryptologic information may not always be an easy task. There are several broad classes of cryptologic information, as follows:
    - (1) Those that relate to COMSEC. In documentary form, they provide COMSEC guidance or information. Normally, COMSEC documents and materials are accountable under the Communications Security Material Control System. Examples are: items bearing TSEC nomenclature (TSEC plus three letters), Crypto Keying Material for use in enciphering communications, Controlled COMSEC Items (CCI), and cryptographic keying devices.
    - (2) Those that relate to SIGINT. These appear as reports in various formats that bear security classification, sometimes followed by a five-letter codeword (World War II's ULTRA, for example) and often carrying warning caveats such as "This document contains codeword material," "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.
    - (3) RDT&E reports and information that relate to either COMSEC or SIGINT.
  - b. Commonly used words that may help in identification of cryptologic documents and materials are "cipher," "code," "codeword," "communications in-

telligence" 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," "signal intelligence" or "SIGINT," "signal security," and "TEMPEST."

Attachments - 3

- A. Department of the Army Systems
- B. Department of the Navy Systems
- C. Department of the Air Force Systems

CATEGORIES OF INFORMATION TO BE REVIEWED FOR DECLASSIFICATION  
DEPARTMENT OF THE ARMY SYSTEMS

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

1. Ballistic Missile Defense (BMD) missile information to include 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.
2. BMD systems data to include 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.
3. BMD optics information that may provide signature characteristics of U.S. and United Kingdom ballistic weapons.
4. Shaped charge technology.
5. Fleshettes.
6. M380 Beehive round.
7. Electromagnetic propulsion technology.
8. Space weapons concepts.
9. Radar fuzing programs.
10. Guided projectiles technology.
11. ECM and ECCM to weapons systems.
12. Armor materials concepts, designs, or research.
13. 2.75-inch Rocket System.
14. Air Defense Command and Coordination System (AN/TSQ-51).
15. Airborne Target Acquisition and Fire Control System.
16. Chaparral Missile System.
17. Dragon Guided Missile System Surface Attack, M47.
18. Forward Area Alerting Radar (FAAR) System.

19. Ground laser designators.
20. Hawk Guided Missile System.
21. Heliborne, Laser, Air Defense Suppression and Fire and Forget Guided Missile System (HELLFIRE).
22. Honest John Missile System.
23. Lance Field Artillery Missile System.
24. Land Combat Support System (LCSS).
25. M22 (SS-11 ATGM) Guided Missile System, Helicopter Armament Subsystem.
26. Guided Missile System, Air Defense (NIKE HERCULES with Improved Capabilities with HIPAR and ANTIJAM Improvement).
27. Patriot Air Defense Missile System.
28. Pershing IA Guided Missile System.
29. Pershing II Guided Missile System.
30. Guided Missile System, Intercept Aerial M41 (REDEYE) and Associated Equipment.
31. U.S. Roland Missile System.
32. Sergeant Missile System (less warhead) (as pertains to electronics and penetration aids only).
33. Shillelagh Missile System.
34. Stinger/Stinger-Post Guided Missile System (FIM-92A).
35. Terminally Guided Warhead (TWG) for Multiple Launch Rocket System (MLRS).
36. TOW Heavy Antitank Weapon System.
37. Viper Light Antitank/Assault Weapon System.

CATEGORIES OF INFORMATION TO BE REVIEWED FOR DECLASSIFICATION  
DEPARTMENT OF THE NAVY SYSTEMS

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

1. Naval Nuclear Propulsion Information.
2. Conventional surface ship information:
  - a. Vulnerabilities of protective systems, specifically:
    - (1) Passive protection information concerning ballistic torpedo and underbottom protective systems.
    - (2) Weapon protection requirement levels for conventional, nuclear, biological, or chemical weapons.
    - (3) General arrangements, drawings, and booklets of general plans (applicable to carriers only).
  - b. Ship-silencing information relative to:
    - (1) Signatures (acoustic, seismic, infrared, magnetic (including alternating magnetic (AM)), pressure, and underwater electric potential (UEP)).
    - (2) Procedures and techniques for noise reduction pertaining to an individual ship's component.
    - (3) Vibration data relating to hull and machinery.
  - c. Operational characteristics related to performance as follows:
    - (1) Endurance or total fuel capacity.
    - (2) Tactical information, such as times for ship turning, zero to maximum speed, and maximum to zero speed.
3. All information that is uniquely applicable to nuclear-powered surface ships or submarines.
4. Information concerning diesel submarines as follows:
  - a. Ship-silencing data or acoustic warfare systems relative to:
    - (1) Oversight, platform, and sonar noise signature.
    - (2) Radiated noise and echo response.
    - (3) All vibration data.

- (4) Seismic, magnetic (including AM), pressure, and UEP signature data.
  - b. Details of operational assignments, that is, war plans, antisubmarine warfare (ASW), and surveillance tasks.
  - c. General arrangements, drawings, and plans of SS563 class submarine hulls.
- 5. Sound Surveillance System (SOSUS) data.
- 6. Information concerning mine warfare, mine sweeping, and mine countermeasures.
- 7. ECM or ECCM features and capabilities of any electronic equipment.
- 8. Torpedo information as follows:
  - a. Torpedo countermeasures devices: T-MK6 (FANFARE) and NAE beacons.
  - b. Tactical performance, tactical doctrine, and vulnerability to countermeasures.
- 9. Design performance and functional characteristics of guided missiles, guided projectiles, sonars, radars, acoustic equipments, and fire control systems.

CATEGORIES OF INFORMATION TO BE REVIEWED FOR DECLASSIFICATION  
DEPARTMENT OF THE AIR FORCE SYSTEMS

The Department of the Air Force has determined that there are no categories of information pertaining to specific Air Force systems that must be systematically reviewed for declassification but that the categories identified in enclosure 2 of this Directive shall apply to Air Force information reviewed at 20 years.



DECLASSIFICATION CONSIDERATIONS

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 would no longer result in at least identifiable damage to the national security, the information must be declassified.

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:

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

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

c. The information is pertinent to a system that is no longer 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.

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

e. 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.

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

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

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

4. Special procedures of the NSA/CSS apply to the review and declassification of classified cryptologic information. The following shall be observed in the review of such information:

a. COMSEC Documents and Materials. If records or materials in this category are found in agency or department files that are not under COMSEC control, refer them to the senior COMSEC authority of the agency or department concerned or by appropriate channels to the following address:

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

b. SIGINT Information

(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 noncryptologic agency or department, such material will not be declassified if retained in accordance with an approved records disposition schedule. If the material must be retained, it must be referred to the NSA/CSS for systematic review for declassification.

(2) If the SIGINT information has been incorporated by the receiving agency or department into documents it produces, referral to the NSA/CSS is necessary prior to any declassification action.

CATEGORIES OF INFORMATION FOR WHICH CLASSIFICATION HAS BEEN EXTENDED  
BEYOND 20 YEARS BY THE SECRETARY OF DEFENSE

The classification of the following categories of information has been extended beyond 20 years by the Secretary of Defense in accordance with the provisions of this Directive. The organization of primary responsibility is shown parenthetically for each category extended.

1. Information encompassing strategic and tactical cover and deception plans, policies, procedures, and organization. (OJCS)
2. Information involving operational planning when such information would reveal courses of action, concepts, tactics, or techniques that are used in current operations plans that are classified. (OJCS)
3. Information revealing intelligence sources, methods, or activities including intelligence plans, policies, or operations, when it is determined that declassification would reasonably be expected to cause identifiable damage to the national security. (Defense Intelligence Agency (DIA)/OJCS)
4. Counterintelligence information, as defined in section 4-202 of Executive Order 12036 (reference (g)). (DIA/OJCS)
5. Cryptologic information, as defined in subsection C.1. of this Directive. (NSA/CSS)

Information concerning categories of information for which classification has been extended beyond 20 years by the Secretary of a Military Department may be obtained from the appropriate office listed below:

Director of Counterintelligence  
Office of the Assistant Chief of Staff for Intelligence  
Department of the Army

Director, Security of Military Information Division  
Office of the Chief of Naval Operations (OP-009D)  
Department of the Navy

Director, Information Security  
Air Force Office of Security Police  
Kirtland Air Force Base  
Department of the Air Force