95-2059

~~SECRET~~

THE JOINT CHIEFS OF STAFF
WASHINGTON, D.C. 20301

SM-800-69
21 November 1969

MEMORANDUM FOR: Chief of Staff, US Army
Chief of Naval Operations
Chief of Staff, US Air Force
Commandant of the Marine Corps
Commander in Chief, Alaska
Commander in Chief, Atlantic
Commander in Chief, Continental Air Defense Command
US Commander in Chief, Europe
Commander in Chief, Pacific
Commander in Chief, US Southern Command
Commander in Chief, US Strike Command/US Commander in Chief, Middle East, Southern Asia, and Africa South of the Sahara
Commander in Chief, Strategic Air Command
Director of Strategic Target Planning
Director, Defense Atomic Support Agency
Director, Defense Communications Agency
Director, Defense Intelligence Agency
Director, National Security Agency
Director, Weapons Systems Evaluation Group

Subject: Safeguarding the Single Integrated Operational Plan

1. Forwarded in the Appendix hereto is the policy of the Joint Chiefs of Staff with regard to security of the SIOP, the basic administrative and handling requirements, and the emphasis which must be placed on control of extremely sensitive SIOP information.

2. The policy in the Appendix supersedes that contained in SM-431-67, dated 20 June 1967, subject as above.

~~SECRET~~

EXCLUDED FROM GDS

#10

3. Without attachment, this memorandum is UNCLASSIFIED.

For the Joint Chiefs of Staff:

ROY C. CROMPTON
Brigadier General, USAF
Secretary

Attachment

APPENDIX

SAFEGUARDING THE SINGLE INTEGRATED OPERATIONAL PLAN (U)

1. (U) General

a. The guidance, as contained herein, sets forth the policy of the Joint Chiefs of Staff with regard to security of the Single Integrated Operational Plan (SIOP). This directive is intended to:

(1) Emphasize the fact that meticulous attention must be given to strict observance of basic security regulations in safeguarding the SIOP.

(2) Emphasize the fact that stringent control must be exercised over SIOP extremely sensitive information (SIOP-ESI), as defined below.

(3) Provide the basic policy for the identification and application of these special controls for SIOP-ESI.

b. Executive Order No. 10501, dated 5 November 1953, and DOD Directive 5200.1, dated 10 July 1968, provide instructions for "Safeguarding Official Information in the Interests of the Defense of the United States." These directives prescribe measures for classification, reproduction, accountability, dissemination, and transmission of official information and include within their scope the documents constituting the SIOP. This directive is supplemental to the preceding directives and applies more specifically to SIOP-ESI, as described herein.

c. The Joint Chiefs of Staff consider that distribution of and access to SIOP-ESI must be strictly limited, based on rigorously justified requirements. Specific security controls and procedures will be established to assure that access is authorized with utmost discrimination in all cases.

GROUP 3
DOWNGRADED AT 12 YEAR INTERVALS;
NOT AUTOMATICALLY DECLASSIFIED.

2. (U) Definitions

a. SIOP-ESI. TOP SECRET information of such a sensitive nature that its disclosure to unauthorized persons would seriously degrade the effective execution of the plan.

b. SIOP Materials. Any recorded information, regardless of its physical form or characteristics, which is part of the JCS SIOP and is derived from or published in support of the SIOP and which may be represented in any of the following forms:

(1) Written material, whether printed, typed, or handwritten.

(2) Painted or drawn material.

(3) Data processed by electronic means.

(4) Sound recordings.

(5) Data processed by photographic means.

(6) Reproduction of the foregoing by whatever process.

(7) Materials used in reproduction of the foregoing (e.g., typewriter ribbons, copying machine belts, etc.).

c. JCS SIOP Documents. The JCS basic SIOP and Annexes, Appendices, Tabs thereto, and associated source data.

d. JSTPS SIOP Documents. Documents published by the Joint Strategic Target Planning Staff (JSTPS) in support of the JCS SIOP.

[ ]

[redacted]

[illegible] are considered to be extremely sensitive and designated, in their entirety, as SIOP-ESI documents. This listing is not to be construed as limiting or all-inclusive, nor is it intended to be maintained in a current status by a change to this directive.

(1) SIOP Annex C and Appendix thereto.

(2) Appendices II and III to SIOP Annex E.

(3) SIOP Annex F and Appendices I,* II, and III thereto.

(4) Annex B to Coordinated Reconnaissance Plan.

(5) SIOP Almanac.

(6) Launch and Impact Summaries.

(7) Weapons Dictionary - Unit Sortie.

(8) Weapons Dictionary - Isle-POZ.

(9) SIOP Analysis Summary Tables.

(10) SIOP War Games.

(11) SIOP Consequences of Execution Analysis.

(12) SIOP Decision Handbook.

3. (U) Security Classification and Marking

a. All SIOP documents shall be classified and marked in accordance with DOD Directive 5200.1. Documents containing SIOP-ESI, as defined and described in paragraph 2 and subparagraph 2a above, shall bear additional markings, as prescribed herein.

* Tabs B and C to this Appendix are not SIOP-ESI

b. SIOP-ESI documents shall be classified TOP SECRET only. In order to permit immediate and positive identification of these documents, the indicator "SIOP-ESI" shall be prominently affixed. This indicator shall also be applied to compilations of documents which, although not SIOP-ESI individually, may, in the aggregate, be so considered.

(1) NATO documents published in accordance with SM-412-66, dated 17 May 1966, will not be marked with the SIOP-ESI indicator. However, the following statement will appear on the cover, the title page, and/or in the letter of promulgation:

"This document contains extremely sensitive information affecting the Single Integrated Operational Plan. Access to this document or the information contained herein shall be strictly limited commensurate with rigorously justified requirements. Use of military or military-controlled vehicles and two officially designated couriers is mandatory."

(2) It is emphasized that the SIOP-ESI indicator is not to be interpreted as a separate security classification. This indicator is intended solely as a mechanism for identification of extremely sensitive SIOP information which shall be controlled in accordance with procedures established by this directive.

(3) Care must be taken to insure that the SIOP-ESI indicator is applied to documents only when the criteria fully warrant and meet the criteria set forth

in subparagraph 3a above. It must be borne in mind that indiscriminate use of the SIOP-ESI indicator will result in unnecessary additions to access rosters and undue restrictions on processing of documents which could ultimately result in lessened security.

c. SIOP documents of a classification lower than TOP SECRET, which are considered to require limited access and/or special handling, shall be disseminated in accordance with Section VII, paragraph D, Enclosure 1, of DOD Directive 5200.1 to appropriately cleared personnel with a valid need to know. Such documents shall not be considered nor identified as SIOP-ESI.

d. SIOP documents, except those modified under the provisions of appropriate directives for distribution to NATO, shall be labeled for no foreign dissemination, i.e., SPECIAL HANDLING REQUIRED NOFORN. Warnings concerning the application of Espionage Laws, Title 18, USC, Sections 793 and 794, shall be affixed to all SIOP documents which are or might be subject to dissemination outside the executive branch of the Government.

5. (U) Distribution of SIOP Material and Extracts

a. The Director for Operations, Joint Staff, Organization of the Joint Chiefs of Staff, will review the requirements of all users of the JCS SIOP prior to the publication of each SIOP and report recommended distribution lists (including the basic plan and annexes thereto) to the Joint Chiefs of Staff. These distribution lists will be approved in the promulgating directives for the SIOP.

(1) Requests for changes to approved distribution lists will be submitted to the Director, Joint Staff, Organization of the Joint Chiefs of Staff, with appropriate justification. Upon consideration and recommendation by the Director for Operations, Joint Staff, the Director, Joint Staff, is authorized to approve/disapprove such requests.

(2) Requests for changes in the number of copies provided by approved distribution lists will be submitted to the Director of Strategic Target Planning (DSTP), with appropriate justification. After informal coordination with the Director for Operations, Joint Staff, the DSTP is authorized to approve/disapprove such requests.

b. The DSTP is authorized to make distribution of JCS SIOP materials for each major revision or update to the SIOP under the provisions of subparagraph 5a, with the following stipulations:

(1) Unless an exception is stated in the approved distribution lists, as provided in subparagraph 5a, or amended under the provisions of subparagraph 5a(1) or 5a(2), JCS SIOP materials distributed by the DSTP will contain only that data pertaining to the user's geographic area of interest.

(2) JSTP-EDI magnetic tapes will be distributed to users within the Washington, D.C., area as follows:

(a) The DSTP will forward one copy of each required tape to "The Joint Chiefs of Staff, Attention: J-3 (NWSL)."

(b) The Director for Operations, Joint Staff, will reproduce tapes, as required, to satisfy the approved requirements of users in the Washington, D. C., area.

(c) Requests for reproduced tapes or portions or printouts thereof will be submitted to the Director for Operations, Joint Staff, who is authorized to approve/disapprove such requests.

c. The DSTP is authorized to make distribution of JSTPS SIOP materials as follows:

(1) All JSTPS SIOP materials:

(a) Joint Chiefs of Staff.

(b) Chief of Staff, US Army; Chief of Naval Operations; Chief of Staff, US Air Force; and Commandant of the Marine Corps.

(c) Commands designated by the Joint Chiefs of Staff to serve as alternate SIOP execution authorities.

(2) Distribution of JSTPS SIOP materials to the commands or agencies not covered in preceding paragraphs will be considered on a case-by-case basis. Except for the JSTPS Air Defense Publication (see subparagraph 5d), requests will be submitted, with sufficient justification to complete an appraisal, to the DSTP. The DSTP may approve such requests that are considered necessary for effective operations. Requests not favorably considered by the DSTP will be forwarded to the Director for Operations, Joint Staff, for review and appropriate action.

d. Requests for copies or changes to the distribution schedule for the JSTPS SIOP publication, "JSTPS Air Defenses Soviet and Asian Communist Bloc JCS SIOP," will be forwarded to the Defense Intelligence Agency Dissemination Center.

e. Requests for JCS SIOP documents not covered above will be submitted to the Director for Operations, Joint Staff, who will review and submit appropriate recommendations to the Director, Joint Staff.

f. Requests for SIOP documents from the Office of the Secretary of Defense, not covered in subparagraph 5a above, shall be referred to the Director for Operations, Joint Staff, who will submit recommended action to the Director, Joint Staff.

g. The Chairman, Joint Chiefs of Staff, consulting the Joint Chiefs of Staff, as appropriate, will review requests for SIOP documents from the White House, the Congress, and other Government departments or agencies for approval/disapproval.

h. Requests for release of SIOP documents to foreign nationals, NATO, SEATO, or CENTO will be submitted to the Director for Operations, Joint Staff, for review and recommendation to the Joint Chiefs of Staff. Subject to the provisions of applicable directives, changes, schedules, and planning information previously released to NATO through the NATO Documents Program and relating directly to the SACEUR/SACLANT area of interest may be provided to the SACEUR/SACLANT representatives at the discretion of the DSIP. Such information must be released on a rigidly discriminatory basis.

i. Recipients of SIOP documents are authorized to extract and reproduce portions thereof for such use, or dissemination to lower echelons, as may be required for [illegible] of assigned tasks, missions, and responsibilities. Reproduction of SIOP document extracts

shall, in every case, be on a rigidly discriminating basis and shall be controlled by the originator (extractor) in accordance with applicable directives, including this directive.

j. Special procedures for extracts from SIOP-ESI documents.

(1) Release of SIOP-ESI data to foreign nationals is prohibited, except as expressly authorized under the NATO Documents Program and as approved by the Joint Chiefs of Staff.

(2) When extracts are made from SIOP-ESI material or when portions of SIOP-ESI material are reproduced, meticulous consideration shall be given to the determination of appropriate classification and identification. It is of particular importance to determine whether or not such extract, or portion reproduced, retains any or all of the characteristics outlined in subparagraph 3a above and should be identified as SIOP-ESI.

k. Recipients of JCS or JSTPS SIOP documents/materials will check the documents/materials for completeness and return receipts within 72 hours of receipt, reporting immediately any discrepancies noted to recipients' parent command. Parent commands will inform the originating agency within 24 hours after being notified, in the event the discrepancy(ies) cannot be resolved.

6. (U) Inventory and Sighting

a. All SIOP materials, as defined and identified in paragraphs 2 and 3 above, will be inventoried annually, as a minimum, or more frequently, as prescribed by the appropriate Service, joint agency, or command classified material control procedures, except as specifically provided below.

b. The basic SIOP and major collections of its annexes (i.e., annexes and appendices maintained at Service, joint agency, and unified and specified command level, except as indicated in subparagraph 6d below, are sightable documents for which inventory shall be required semiannually.

c. Because of the extreme sensitivity of information identified as SIOP-ESI, all documents not covered in subparagraph 6b above, which are identified as containing SIOP-ESI, shall be inventoried, sighted, and reported simultaneously with those required by JCS Memorandum of Policy No. 84.

d. SIOP-ESI documents which are effective for 6 months or less will be controlled by document receipt/certificate of destruction procedures in accordance with applicable Service and joint agency security directives. These documents shall be destroyed within 30 days of supersession. Certificates of destruction shall be maintained as directed by the Service, joint agency, or commanders of unified and specified command security directives. Command internal inspection procedures will be established to assure rigid adherence to these procedures.

e. The DSTP shall, semiannually, as of 31 March and 30 September, provide holders a listing of effective documents described in subparagraphs 6b and 6c above. Documents controlled in accordance with subparagraph 6d above will be exempt. Upon receipt of this listing, holders shall verify the listing and certify the sighting of such documents to the DSTP. The DSTP will forward a consolidated sighting report of each semiannual sighting to the Secretary, Joint Chiefs of Staff. Discrepancies, if any, shall be handled separately in accordance with paragraph 11 below and reported to the Director, Joint Staff.

f. To facilitate this inventory and sighting and to provide the maximum security, holders of SIOP-ESI material should provide for central control of such documents.

(U) 7. ~~(C)~~ Access Control

a. Access to SIOP information not identified as SIOP-ESI will be controlled solely in accordance with standard security procedures governing access to classified information. It is not considered necessary to establish any special controls over access to these data.

b. Access to SIOP information designated SIOP-ESI shall be subject to special control procedures. Services, joint agencies, and commands holding or authorized SIOP-ESI data are requested to provide implementing instructions for the special control procedures outlined below.

(1) Access to SIOP-ESI data shall be on a selective and discriminating basis in accordance with stringent user requirements. Specific duty assignments requiring access to SIOP-ESI should be identified.

(2) Personnel who are to be authorized access to SIOP-ESI shall possess a final TOP SECRET clearance, based on a background investigation. Such investigation will have been completed within the past 5 years, or be in an updating process, if a previously completed background investigation is more than 5 years old.

(3) Prior to being granted access, all personnel will be briefed on the contents of this directive, plus any supplemental directives considered appropriate. Upon termination of access, appropriate debriefing should be accomplished and will include notification of duty and travel restrictions as set forth in subparagraph 7b(4) below. These debriefings shall give

emphasis to the individual's continuing responsibility for the protection of information obtained as a result of his access. To satisfy these requirements, each individual who is granted SIOP-ESI access will execute an appropriate briefing/debriefing certificate which will be maintained as a permanent part of his security file.

(4) Personnel who have broad or continuing access to an operational category of SIOP-ESI (see the Annex hereto) at Service, joint agency, or unified and specified command level will be subject to appropriate travel restrictions, as determined by the authority granting access. Certification of this travel restriction and of future duty assignment restriction will be forwarded to the parent Service personnel distribution control agency. This certification will be effective for a minimum of 1 year after termination of access or detachment, whichever occurs first. A waiver of these restrictions may be granted only upon approval by the authority granting access. Determination of restrictions to be imposed on personnel at lower levels of command will be made by the appropriate Service and command involved.

(5) Prior to visits by personnel who will require access to SIOP-ESI data, the appropriate headquarters will be notified of the category of SIOP-ESI to which each individual is authorized access. This certification is in addition to the requirement to certify appropriate security clearances. If appropriate, any modification to category number imposed by geographical distribution of documents will be added.

(6) Organizational master access lists will be maintained, as appropriate. Such lists, in their entirety, should be classified CONFIDENTIAL. These lists shall be reviewed periodically as an additional measure for assuring access is limited to the minimum numbers of persons required. Correspondence or messages pertaining to access for an individual or small groups of persons shall be marked FOR OFFICIAL USE ONLY or EFTO, as appropriate.

(7) The operational and administrative categories of SIOP-ESI set forth in the Annex are established and shall be used for access control, subject to minor modifications required by the geographical distribution of documents.

(8) Internal inspection procedures will give special and continuing cognizance to safeguards for SIOP-ESI documents.

c. It is intended that control measures for access to SIOP-ESI will provide such access to the following:

(1) The Joint Chiefs of Staff, members of the Organization of the Joint Chiefs of Staff and other Joint Staff agencies, and personnel assigned to the Office of the Secretary of Defense. Authority to grant access is delegated to the Director, Joint Staff.

(2) The Chief of Staff, US Army; Chief of Naval Operations; Chief of Staff, US Air Force; Commandant of the Marine Corps; and members of the Service and departmental staffs. Authority to grant access is delegated to the Chief of Staff, US Army; Chief of Naval Operations; Chief of Staff, US Air Force; and Commandant of the Marine Corps.

(3) Commanders of unified and specified commands having responsibility for planning, preparation, coordination, and/or execution of the SIOP. Authority to grant access is delegated to the commanders concerned.

(4) The DSTP and members of and representatives to the JSTPS. Authority to grant access is delegated to the DSTP.

(5) Other personnel not covered above, as may be authorized by the Joint Chiefs of Staff.

d. The authority to grant access delegated in subparagraph 7c above may be further delegated to appropriate subordinates. Such further delegation shall be held to the minimum appropriately cleared individuals consistent with requirements.

e. It is intended that civilian personnel not subject to the provisions of Federal Civil Service Commission or DOD personnel policies (specifically, industrial contractor personnel) not be granted access to SIOP-ESI. Any requests for such civilian personnel access shall be referred to the Director, Joint Staff, for appropriate action. Personnel in this category will possess a final TOP SECRET clearance, based on criteria established in subparagraph 7b(2) above.

8. (U) Briefings

a. SIOP briefings shall not be given to other than those personnel under the control or military jurisdiction of the Joint Chiefs of Staff or of the Chief of Staff, US Army; Chief of Naval Operations; Chief of Staff, US Air Force; and Commandant of the Marine Corps as essential to review, develop, maintain, or implement the SIOP, without specific approval as indicated below. Attendance at SIOP briefings designated SIOP-ESI shall be governed by approved access lists.

b. The SIOP shall not be used as a vehicle of instruction at Service schools or other instructional institutions. Special SIOP briefings to the joint or Service schools will require approval on a case-by-case basis. The Director for Operations, Joint Staff, will review requests for briefings of joint colleges and make appropriate recommendations to the Director, Joint Staff, who is delegated authority to provide approval. The Chief of Staff, US Army; Chief of Naval Operations; Chief of Staff, US Air Force; and Commandant of the Marine Corps are requested to provide approval of such requests from Service schools. Requests for SIOP briefings will identify the specific information concerning the SIOP that is desired in the briefing and justification showing the purpose served. SIOP-ESI data will not be briefed, unless specifically authorized by the Director, Joint Staff.

c. The Chairman, Joint Chiefs of Staff, consulting the Joint Chiefs of Staff, as appropriate, will review requests for SIOP briefings for the Congress, the White House, and the Office of the Secretary of Defense.

d. SIOP briefings shall not be given to foreign nationals, including members of NATO, SEATO, and CENTO, except as may be approved on a request basis by the Joint Chiefs of Staff or as provided for by other specific action of the Joint Chiefs of Staff.

e. Requests for SIOP briefings not covered above will be submitted to the Director for Operations, Joint Staff, who will review such requests and submit appropriate recommendations to the Director, Joint Staff, for approval.

(U) 9. ~~(C)~~ Correspondence

a. Correspondence, reports, studies, messages, and any other media relaying SIOP-ESI shall include a statement that:

"This (correspondence, memorandum, report, etc.) contains SIOP-ESI data. Access lists govern internal dissemination."

b. Messages containing SIOP-ESI shall include the designator "SPECAT" and the indicator "SIOP-ESI" at the beginning of the message text immediately following the message classification, in accordance with subparagraph 332d, ACP 121 US Supp-1( ), followed by the statement in subparagraph 9a above, as appropriate.

10. (U) Courier Instructions

a. SIOP material not identified as SIOP-ESI will be handled in accordance with applicable directives.

b. SIOP-ESI material not transmitted electrically shall be dispatched only by courier. The Armed Forces Courier Service (ARFCOS) may be utilized. SIOP-ESI material being transported or processed outside military installations will be accompanied by two appropriately cleared couriers assigned the primary responsibility for surveillance and security of the material. When utilizing air transportation, one courier may be used during flight so long as two couriers are used to transport the SIOP-ESI material to and from the aircraft and maintain surveillance until the aircraft is airborne. US military air transportation is the desired mode of transporting SIOP-ESI material. US Military Airlift Command commercial contract aircraft, where the passenger list is under US military control or US commercial non-passenger cargo aircraft may be used in lieu of military air.

c. SIOP-ESI material transmitted by ARFCOS will be processed and transported in accordance with subparagraph 10b above. Dispatching officials will designate the material SIOP-ESI when entering it into the ARFCOS system. Special handling within the ARFCOS system will be as prescribed by the Director, ARFCOS. Commanders supporting ARFCOS are responsible for providing arrangements for the transportation of SIOP-ESI material by military air. Priority will be provided to the transmission or deadline delivery date SIOP-ESI material.

d. All SIOP-ESI material being transported by ARFCOS will have the following statement affixed to the outside of the package or container in addition to the normal addressees and markings:

RESTRICTED HANDLING REQUIRED

(1) Air transportation of this package will be by US military aircraft; US Military Airlift Command commercial contract aircraft, where the passenger list is under US military control; or US commercial nonpassenger cargo aircraft only.

(2) TWO COURIERS ARE REQUIRED BETWEEN US MILITARY INSTALLATIONS. COURIERS AND GUARDS MUST POSSESS TOP SECRET CLEARANCE, BASED ON A COMPLETED FAVORABLE BACKGROUND INVESTIGATION. ONE COURIER CAN BE USED DURING FLIGHT SO LONG AS TWO COURIERS DELIVER AND PICK UP MATERIAL AT PLANESIDE OFF MILITARY BASES.

(3) When not attended by qualified couriers, the minimum security required for storage of this package is in a secure room supplemented by guards or an intrusion detection alarm system or a Class A vault constructed in accordance with individual Service directives.

11. (U) Actions in Case of Possible or Actual Compromise. The Joint Chiefs of Staff and the DCTP shall be informed by the most expeditious means available, consistent with security requirements, of any actual or suspected compromise of any portion of SIOP material. Such reports will include specific identification of the document, whether or not SIOP-ESI is involved, opinion as to probability of compromise, and details of how, when, and where the data were compromised or possibly compromised. The DSTP will recommend appropriate actions required, with regard to modification of the plan and/or related procedures as a result of the compromise or possible compromise, for consideration by the Joint Chiefs of Staff.

[redacted]

[ ]

13. (U) Electronic Data Processing Media. The facility of data reproduction by electronic means presents a special need for attention to security precautions where such means are used in processing classified material. This need is more pressing in instances where distribution and access must be strictly controlled, as in the case of SIOP-ESI material. Commands and agencies which possess the means of machine reproduction of SIOP-ESI material, or which are authorized to release such materials to other agencies for similar reproduction, shall establish suitable and adequate means for controlling, accounting, and access. In every case, such means shall provide that numbers of copies, extracts, or information derivatives shall be limited to those required to serve valid needs. Access to documents and reproduction equipment shall be limited to the minimum numbers of proper, cleared personnel. Accountability systems shall insure that all documents produced by electronic means are properly identified, marked, distributed, and safeguarded.

a. Safeguarding SIOP-ESI in an automatic data processing environment requires special precautions, since the recording media used to store or process SIOP-ESI must be protected and must retain the TOP SECRET classification and be controlled as SIOP-ESI until one of the procedures below

is carried out (i.e., the procedures have been designed for, but are not limited to, releasing the recording media for maintenance of equipment, return of parts to contractor, release of computer to contractors, etc.):

(1) Clear Memory Procedures. When SIOP-ESI has been processed using electronic data processing equipment, internal memory (i.e., core) in the central processing unit may be cleared by alternately setting each addressable memory location to all "1s" and all "0s" for 100 cycles, such that the state is changed at least 99 times. The successful application of this procedure must be verified after the 100th cycle. Internal memory, other than thin film and plated wire, may then be declassified. The ability to clear internal memory of thin film or plated wire completely for declassification purposes is uncertain; therefore, such media must retain the TOP SECRET classification and be controlled as SIOP-ESI until destroyed.

(2) Magnetic discs, disc packs, disc files, drums, and other storage devices (excluding tapes that are discussed in subparagraph 13b below) that use either a nickel cobalt or oxide coating as the digital recording medium may be declassified after using one or more of the following procedures, as appropriate:

(a) Providing that SIOP-ESI has been recorded undisturbed no longer than 72 consecutive hours, all data tracks will be overwritten a minimum of three times using maximum current that will not damage or impair the recording equipment. The binary digit 1 or 0 will be overwritten in all bit locations

and overwrite verified. Then, a single numeric, alphabetic, or special character will be overwritten in all address positions. Finally, alphanumeric data which is known to be UNCLASSIFIED can be overwritten in all positions, and this UNCLASSIFIED text should be left on the device. This, too, should be verified. If doubt exists that all data tracks have been overwritten, then procedures of subparagraph 13a(2)(a)2 below will be used.

1. When the capability exists as an integral part of the storage subsystem, an AC/DC erase will be applied to all data tracks. The tracks will then be overwritten as in subparagraph 13a(2)(a) above and verified that the overwrite has been accomplished.

2. In the event a storage unit fails or has a mechanical failure which inhibits normal operation, a hand erase bar or portable permanent/AC magnet will be used to wipe all data tracks, including the permanent data tracks such as clock, address and word mark, or message tracks. The erase bar or magnet must produce at least 1500 Oersted field intensity at the recording surface.

(b) If SIOP-ESI has been recorded and remains undisturbed for over 72 hours or is subjected to excessive heating, it can only be considered declassified if the recording surface is completely removed. Unavailability of appropriate facilities for surface removal will necessitate shipment of the material to a suitably equipped depot or manufacturer. Such transportation must be in accordance with paragraph 10 above. Damaged or inoperative drums and discs which cannot be treated as prescribed in subparagraph 13a(2)(a) above fall under the provisions of this paragraph.

(3) When the disc, disc pack, disc file, or drum is treated as prescribed in subparagraph 13a(2)(a) above, it may be declassified and released to the commercial contractor if it is to be returned to a military user. The military user will establish those procedures necessary to insure that the same disc, disc pack, disc file, or drum is returned. Their transportation and movement will be handled to insure timely receipt by the contractor (i.e., contractor furnish receipt to sender upon arrival and no extensive delays have occurred). They will not be permanently released to commercial contractors without specific approval by the Director, Joint Staff, on a case-by-case basis.

(4) When the disc, disc pack, disc file, or drum is treated as prescribed in subparagraph 13a(2)(b) above, it is UNCLASSIFIED and released without restrictions to the commercial contractor.

b. Magnetic tapes used to record SIOP-ESI may be degaussed, using approved bulk degaussing equipment which meets technical specifications promulgated by the National Security Agency. Tapes may be subsequently declassified but must be retained by a military user.

c. Magnetic wire used to record SIOP-ESI will not be declassified and will continue to retain the TOP SECRET classification, under SIOP-ESI control, until destroyed.

d. Personnel clearing SIOP-ESI information from magnetic drums, discs, and tapes will execute certificates of destruction as indicated in paragraph 14 below.

14. (U) Destruction. As a matter of policy, in order to insure control and minimize the possibility of compromise, SIOP material will be destroyed promptly when superseded by new editions or when no longer required for operational use. Archive copies are authorized to be established by JSTPS, as prescribed by the Joint Chiefs of Staff. Officials certifying to the destruction of material containing SIOP-ESI will be commissioned officers, warrant officers, or civilians in grade GS-9 or above. Witnessing officials will be commissioned officers, warrant officers, or noncommissioned officers in grade E-7 or above or civilians in grade GS-7 or above.

ANNEX

SIOP-ESI OPERATIONAL AND ADMINISTRATIVE CATEGORIES

(U) 1. (C) The following operational categories provide access to full and detailed knowledge:

Operational Category	
01	[redacted]
02	
03	
04	
05	
06	

2. (U) The following administrative categories provide access only as necessary for administrative handling and processing in a routine manner:

Administrative Category	Access Authorized
21	To category 01
22	To category 02
23	To category 03
24	To category 04
25	To category 05
26	To category 06

GROUP 3
DOWNGRADED AT 12 YEAR INTERVALS;
NOT AUTOMATICALLY DECLASSIFIED