#549

THE JOINT STAFF

JOINT ADMINISTRATIVE INSTRUCTION

JOINT ADMINISTRATIVE
INSTRUCTIONS 2511.8J

J-3/STRATOPS
20 April 1989

SAFEGUARDING THE SINGLE INTEGRATED OPERATIONAL PLAN (SIOP)

Reference: MJCS 75-87, 20 May 1987

1. Purpose. To supplement the reference and to establish procedures for the processing and safeguarding of SIOP information within the agencies listed in paragraph 3 below.

2. Cancellation. JAI 2511.8I, 3 October 1983.

3. Applicability. The procedures of this instruction will be followed within the Joint Staff. With the concurrence of the Office of the Secretary of Defense; Federal Emergency Management Agency (FEMA); the Director, Defense Communications Agency (DCA); the Director, Defense Intelligence Agency (DIA); the Director, Defense Mapping Agency (DMA); the Director, Defense Nuclear Agency (DNA); the Director, National Security Agency (NSA); Director, and the Chief, Joint Atomic Information Exchange Group (JAIEG) these procedures will also be applicable to personnel under the jurisdiction of these agencies.

4. Policy. Executive Order 12356, 2 April 1982, DOD Directive 5200.1 and DOD Regulation 5200.1-R provide instructions for the DOD Information Security Program. These documents prescribe measures for classification, reproduction, accountability, safekeeping, storage, dissemination, and transmission of official information and include within their scope the documents which constitute the SIOP. This directive and the reference provide supplemental guidance and apply specifically to that information which is designated as SIOP-Extremely Sensitive Information (SIOP-ESI) in the reference.

93-F-1436 DOC 1 DOCM

5. Responsibilities

a. Each agency listed in paragraph 3 will ensure that the provisions of this instruction and the reference are implemented and followed. Specifically, each agency will assure:

(1) That each person who is authorized access to SIOP-ESI is briefed in accordance with subparagraph 8b(8) of the Appendix to the reference and executes a briefing certificate prior to being granted access, and executes a debriefing certificate after removal from an agency master access roster. For Joint Staff personnel, JCS Form 59, "Security Agreement," will be used. Other agencies may use their own briefing/debriefing forms.

(2) That an agency master SIOP-ESI access listing is maintained in accordance with subparagraph 8b(9) of the reference. Two copies of each agency master roster will be forwarded monthly to the Joint Staff, Attn: Security Division, DIRM. Rosters should arrive not later than the 10th day of the month. JAIEG is requested to provide access roster data to DNA. DNA is requested to include the JAIEG in its master access roster.

(3) That a notice of travel and duty restrictions is forwarded to the person concerned, the appropriate personnel, security, and travel offices in accordance with paragraph 9 of the Appendix to the reference. Joint Staff elements are to use JCS Form 101 (Sample format contained at Enclosures A and B). THIS NOTICE WILL BE FORWARDED AT THE TIME OF ASSIGNMENT TO THE BILLET. The personnel office will forward the notice to the parent Service personnel distribution control point.

b. Personnel granted permanent or temporary access to SIOP-ESI need no further authorization for access to the categories of SIOP-ESI specified; however, holders of SIOP-ESI documents must still exercise prudence when releasing SIOP-ESI information.

6. Information Control Procedures

a. General. The reference states that those portions of the SIOP not designated as "SIOP-ESI" are not considered to require any special control procedures; thus, normal procedures applicable to the degree of classification assigned are to be followed for handling those SIOP documents not considered "SIOP-ESI." This instruction, accordingly, establishes procedures and controls that are applicable only to "SIOP-ESI," as defined in the reference.

b. Document Control. The following procedures are hereby established for control of documents marked 'SIOP-ESI." Internal procedures within each applicable agency and Joint Staff directorate shall provide for a "continuous receipt" system for all SIOP-ESI documents.

(1) Tapes, reproduced in accordance with subparagraph 6b(2) of the Appendix to the reference, shall be controlled as directed by Nuclear Warfare Status Branch, J-3, Joint Staff, in collaboration with recipient.

(2) Messages shall normally be destroyed within 6 MONTHS from date of receipt. Copies of messages that are needed for longer periods of time shall be placed in the normal document control system.

(3) Working papers shall be controlled by the originator in accordance with the procedures for messages specified in subparagraph 6b(2) above.

(4) SIOP-ESI documents shall be returned to the control point established in accordance with the foregoing when no longer required.

(5) All SIOP-ESI documents (including working papers and messages) to be destroyed shall be listed on certificates of destruction forms and destroyed in accordance with security regulations and paragraph 18 of the Appendix to the reference. Within the Joint Staff, the forms to be used are those prescribed in JAI 2511.3 series. Agencies outside the Joint Staff may continue to use their own administrative procedures for this purpose. Handwritten notes and rough drafts should be segregated from other classified trash and disposed of in accordance with this paragraph in a manner which allows access only by authorized personnel.

c. Marking, Distribution, Transmission, and Transportation of Data. The procedures set forth in paragraphs 5, 6, 13, and 14 of the Appendix to the reference are to be followed in all instances.

d. Reproduction of SIOP-ESI. Copies of SIOP-ESI material will be controlled in accordance with the procedures outlined above and paragraph 16 of the Appendix to the reference.

7. Personnel Access Control.

a. General. The Joint Chiefs of Staff consider that distribution of and access to SIOP-ESI must be strictly limited and based on vigorously justified operational requirements or need-to-know. This is especially true for the SIOP decision and execution process. Supervisors should use mechanical means to preclude access and reduce the number of SIOP-ESI billets whenever possible. Examples are: collect and lock SIOP-ESI in one safe versus having SIOP-ESI documents stored in several locations, hold SIOP-ESI discussions only in conference rooms where the audience can be controlled, etc.

b. Delegation of Authority. In accordance with subparagraph 8e of the Appendix to the reference, the Director, Joint Staff has delegated authority to the Director for Operations (J-3) to approve/disapprove requests to establish permanent access billets and grant temporary access for military and civilian personnel of the agencies listed in paragraph 3 above.

c. Permanent Access. Requests to establish permanent SIOP ESI access billets as outlined in subparagraph 8b(2)(a) of the Appendix to the reference should be submitted to the Director for Operations (J-3). Requests must contain the categories of SIOP-ESI for which access is required and a rigorous justification which includes the frequency of anticipated access, the intended use of the information obtained, and a discussion which explains why the number of billets/persons, if any, previously granted access is inadequate.

d. Temporary Access. Requests for temporary access to SIOP-ESI as outlined in subparagraph 8b(2)(b) of the Appendix to the reference should be submitted to the Director for Operations (J-3). Requests must contain the categories of SIOP-ESI for which access is requested and a detailed discussion of why and for how long access is required. Requests must also include the name(s), SSN, and clearance data of personnel for which access is requested.

e. Contractor Access. Civilian personnel not subject to the provisions of the Office of Personnel Management (OPM) or Department of Defense personnel policies (e.g. contractor personnel) shall not be granted PERMANENT ACCESS to SIOP-ESI information. Personnel in this category will be authorized TEMPORARY ACCESS ONLY. Requests for contractor access should be submitted to the Director for Operations (J-3). Requests must contain the name of the contractor, name(s), SSN, categories of SIOP-ESI for which access is required, and a detailed discussion of why and for how long access will be

required. Requests for initial temporary access will be approved by the Director, Joint Staff. Requests to extend the initial period of temporary access may be approved by the Director for Operations or his designee.

f. Waiver of SBI Requirement. In accordance with subparagraphs 8b(5)(b) and 8c of the Appendix to the reference, the Deputy Director, National Military Command System is authorized to waive the SBI requirement for personnel assigned to the organizations listed in paragraph 3 above. Requests for waivers should be submitted to the Director for Operations (J-3), Attention: Strategic Operations Division. The request for waiver should contain a detailed discussion of why the waiver is necessary as well as a certification that the individual qualifies for a waiver as outlined in subparagraph 8b(5)(b) of the Appendix to the reference.

g. Access for Personnel Designated to Relocate to the National Military Command Center (NMCC), Alternate National Military Command Center (ANMCC), and National Emergency Airborne Command Post (NEACP). Access for personnel assigned to relocate under EMERGENCY relocation procedures will be granted as follows:

(1) Relocation rosters shall be submitted to the NMCC and to the carious alternates via the Security Division, DIRM, Joint Staff which will annotate and sign such rosters as follows:

(a) "The personnel listed above meet the criteria for access to SIOP-ESI data as prescribed in MJCS 75-87 and are to be automatically added to their Master Agency SIOP-ESI Access Roster when EMERGENCY relocation is directed."

(b) Any person on such lists who do not meet the criteria for access shall be listed as "Exceptions."

(2) Due to the nature and purpose of the EMERGENCY relocation roster, it is more than probable that a briefing certificate will not be completed on individuals when EMERGENCY relocation is directed. Therefore, a debriefing certificate will be administered by the appropriate directorate or agency security organization at such time as the EMERGENCY no longer exists and the relocatees have returned to the parent organizations.

8. Access for Personnel Designated to Participate in EXERCISES

a. SIOP-ESI access is not normally required for personnel designated to participate in EXERCISES. If it is determined that exercise participants, including Planning Group member and Evaluation Group members, will be required to have access to SIOP-ESI, requests for such access will be processed in accordance with the procedures prescribed in paragraph 7d above.

b. The procedures of this section will not apply to personnel who have been granted permanent access to SIOP-ESI by reason of occupying a permanent SIOP-ESI billet as defined in subparagraph 7c above unless the categories of access required on a temporary basis will exceed the permanent authorization.

c. Exercise temporary access rosters shall be submitted to the NMCC and to the various alternates via the Security Division, DIRM, Joint Staff. Personnel listed on such rosters must be briefed and debriefed as outlined in subparagraph 8b(8) of the Appendix to the reference.

9. Requests for SIOP documents shall be handled in accordance with paragraph 6 of the Appendix to the reference.

10. Visits Requiring Access to SIOP Information, SIOP Briefings, and Visits to Joint Strategic Target Planning Staff (JSTPS)

a. Visits involving SIOP-ESI information and requests for SIOP briefings will be handled in accordance with paragraphs 10 and 11, respectively, of the Appendix to the reference.

b. Visits to the JSTPS will be approved by the Chairman, Joint Chiefs of Staff, or other Joint Staff authority, as appropriate, to minimize the interference with SIOP development and unwarranted dissemination of SIOP information. All requests for visits to JSTPS, except those from individuals directly involved in SIOP development, support, and implementation--see table below, will be forwarded to the Director for Operations, Joint Staff, a minimum of seven working days prior to the proposed visit for a determination of the proper approval authority. The reason for the requests, identity of the visitors, and the briefings/discussions requested will be considered in determining the approval authority. Approval/disapproval authority for visits to JSTPS is as follows:

SOURCE OF REQUEST	APPROVAL/DISAPPROVAL AUTHORITY[1]
Civilian Personnel from White House, Senate or House of Representatives	CJCS
Foreign Personnel other than NATO	JCS
Foreign Members of NATO	DJS
Individuals from the Joint Staff, Services, CINCs, DIA, DMA, or DNA who are directly involved with SIOP development, support, or implementation	DSTP
Services, Agencies subject to JAI (See paragraph 3), and all others	J-3

[1]JCS or other authorities are consulted as appropriate.

c. JSTPS will provide the Director for Operations with informational copies of any messages or documents which may result from approvals/disapprovals processed at JSTPS.

11. Actions in Case of possible or actual compromise shall be handled in accordance with paragraph 15 of the Appendix to the reference.

12. SIOP-ESI Access Categories are defined in Annex A of the Appendix to the reference.

MICHAEL R. DAVENPORT
Colonel, USAF
Director, Information
and Resource Management

Attachments
Enclosure A, JCS Form 101
Enclosure B, Sample Format for Recommendations Pertaining to Travel and Duty Restrictions

SUMMARY OF CHANGES. Administrative update.

ENCLOSURE A

TRAVEL AND DUTY RESTRICTIONS

Name	Rank/Grade	SSAN

Subject individual is assigned to permanent SIOP-ESI access billet _____ in accordance with MJCS 75-87
As a result of this access authorization, the individual will have broad or detailed knowledge and continuing access to SIOP-ESI information. Therefore, he/she is restricted from official of unofficial travel to the countries listed in the Tab to Annex E of MJCS 75-87, while assigned to the Joint Staff unless the restriction is waived by the Director for Operations, the Joint Staff.

Subject individual is restricted from travel to and duty assignment in the countries listed in the Tab to Annex E of MJCS 75-87 for _____ year(s) commencing with the date he/she is detached from the Joint Staff. This restriction may be waived by the Director for Operations, the Joint Staff.

Military Secretary/Executive Officer	Signature

JCS Form 101
APR 89

(W) COPY 1 - Pers Div, J-1
(Y) COPY 2 - Security Div, DIRM
(P) COPY 3 - Travel Sec, Services Div, DIRM
(G) COPY 4 - Individual's Copy

ENCLOSURE B

SAMPLE FORMAT FOR NOTICE OF TRAVEL AND DUTY RESTRICTIONS

MEMORANDUM FOR DISTRIBUTION

Subject: Travel and Duty Restriction Regarding _____
(Rank/Grade, Name, Social Security Number)

1. _____ is assigned to
(Rank/grade, name, SSN)
permanent SIOP-ESI access billet _____ in accordance with reference*.

2. As a result of this access authorization, he/she will have broad or detailed knowledge and continuing access to SIOP-ESI information. Therefore, he/she is restricted from official and unofficial travel to the countries listed in the Tab to Annex E of the reference while assigned to _____ unless the
(Agency)
restriction is waived by the Director for Operations, Joint Staff.

3. Furthermore, _____ is restricted from travel
(Name)
to and duty in the countries listed in the Tab to Annex E of the reference for _____ year(s) commencing with the date he/she is detached from _____. This restriction may be waived
(Agency)
by the Director for Operations, Joint Staff.

_____
(Authorized Signature)

Reference
* MJCS 75-87, dated 20 May 1987

Distribution
J-1, PSD
DIRM, Security Division
DIRM, Services Division
Individual concerned

~~SECRET~~

SAFEGUARDING THE SINGLE INTEGRATED OPERATIONAL PLAN (U)

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

MJCS 75-87

CLASSIFIED BY DIRECTOR, J-3
DECLASSIFY ON OADR

93-FOI-1486
#549
Doc Div R-1

~~SECRET~~

~~SECRET~~

THE JOINT CHIEFS OF STAFF
WASHINGTON, D.C. 20301-5000

MJCS 75-87
20 May 1987

MEMORANDUM FOR: DISTRIBUTION LIST

Subject: Safeguarding the Single Integrated Operational Plan

1. The Appendix contains the policy of the Joint Chiefs of Staff with regard to security of the Single Integrated Operational Plan (SIOP), the basic administrative and handling requirements, and the emphasis that must be placed on control of SIOP-Extremely Sensitive Information (SIOP-ESI).

2. This memorandum supersedes SM-313-83, 10 May 1983, "Safeguarding the Single Integrated Operational Plan."

3. Without enclosure, this memorandum is UNCLASSIFIED.

For the Joint Chiefs of Staff:

Richard A Burpee

RICHARD A. BURPEE
Lieutenant General, USAF
Director for Operations

Enclosure

~~SECRET~~

DISTRIBUTION

	No. of Copies
Secretary of Defense	13*
Director of Central Intelligence	1
Chairman, Joint Chiefs of Staff	1
Chief of Staff, US Army	6
Chief of Naval Operations	4
Chief of Staff, US Air Force	5
Commandant of the Marine Corps	3
Commander in Chief, US Space Command	5
Commander in Chief, US Atlantic Command	4

* Includes copies for distribution to the following:

Assistant to the President for National Security Affairs	1
Director, White House Military Office	1
Director, Federal Emergency Management Agency	1
Director, US Secret Service, Department of the Treasury	1
Deputy Under Secretary of Defense for Policy	1
Director, Emergency Planning, Office of tne Deputy Under Secretary of Defense for Policy	1
Director, Information Security, Office of the Deputy Under Secretary of Defense for Policy	1
Director, Security Plans and Programs, Office of the Deputy Under Secretary of Defense for Policy	1
Deputy Assistant Secretary of Defense (Comptroller) (Administration)	1
Director for Industrial Security Clearance Review, General Counsel	1
Director, Washington Headquarters Services	2

	No. of Copies
Commander in Chief, US Central Command	2
US Commander in Chief, Europe	2
Commander in Chief, Military Airlift Command	2
Commander in Chief, US Pacific Command	9
Commander in Chief, US Readiness Command	3
Commander in Chief, US Southern Command	5
Commander in Chief, Strategic Air Command	5
Director of Strategic Target Planning	8
US Representative to the Military Committee, NATO	1
Director, Defense Communications Agency	4
Director, Defense Intelligence Agency	7
Director, Defense Investigative Service	4
Director, Defense Logistics Agency	2
Director, Defense Mapping Agency	9
Director, Defense Nuclear Agency	3
Director, National Security Agency/Chief, Central Security Service (P-391)	1
Director, Joint Staff	1
Director for Manpower and Personnel, Joint Staff	1
Director for Operations, Joint Staff	13
Director for Logistics, Joint Staff	1

No. of Copies

Director for Strategic Plans and Policy, Joint Staff.....3

Director for Command, Control, and Communications Systems, Joint Staff.....3

US National Military Representative, SHAPE.....1

Commander, Joint Special Operations Command.....1

Director, Force Structure, Resources, and Assessment.....4

Director for Information and Resource Management, OJCS.....7

Chief, Alternate National Military Command Center.....2

Commander, Joint Coordination Center.....1

Chief, National Emergency Airborne Command Post.....4

Chief, Joint Atomic Information Exchange Group.....1

Secretary, Joint Chiefs of Staff.....14

TABLE OF CONTENTS

		Page No.
APPENDIX	SAFEGUARDING THE SINGLE INTEGRATED OPERATIONAL PLAN (U)	1
ANNEX A	CATEGORIES OF SIOP-EXTREMELY SENSITIVE INFORMATION (SIOP-ESI) (U)	A-1
ANNEX B	EXAMPLES OF SIOP-EXTREMELY SENSITIVE INFORMATION ACCESS ROSTERS	B-1
ANNEX C	MINIMUM SECURITY REQUIREMENTS FOR AUTOMATIC DATA PROCESSING SYSTEMS PROCESSING SIOP-EXTREMELY SENSITIVE INFORMATION (SIOP-ESI)	C-1
ANNEX D	DECLASSIFICATION PROCEDURES FOR ADP MEDIA STORING SIOP-EXTREMELY SENSITIVE INFORMATION (SIOP-ESI)	D-1
ANNEX E	SECURITY POLICY CONCERNING TRAVEL AND ASSIGNMENT OF PERSONNEL WITH ACCESS TO SIOP-EXTREMELY SENSITIVE INFORMATION (SIOP-ESI) (U)	E-1
ANNEX F	REFERENCES	F-1

APPENDIX

SAFEGUARDING THE SINGLE INTEGRATED OPERATIONAL PLAN (U)

1. (U) General

a. (U) The guidance 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) (U) Emphasize the need for strict observance of basic security regulations in safeguarding the SIOP.

(2) (U) Emphasize that stringent control must be exercised over SIOP-Extremely Sensitive Information (SIOP-ESI), as defined below.

(3) (U) Provide the basic policy for the identification of SIOP-ESI.

(4) (U) Set forth specific security controls and procedures to ensure that distribution of and access to SIOP-ESI are authorized with utmost discrimination in all cases.

b. (U) Executive Order 12356, DOD 5200.1 and DOD 5200.1-R provide instructions for the DOD Information Security Program. These documents prescribe measures for

CLASSIFIED BY DIRECTOR, J-3
DECLASSIFY ON OADR

classification, reproduction, accountability, safekeeping, storage, dissemination, and transmission of official information and include within their scope the documents that constitute the SIOP. This directive is supplemental to the preceding directives and applies more specifically to SIOP-ESI, as described herein.

c. (U) The Joint Chiefs of Staff consider the information described in subparagraph 3b and paragraph 4 to be an extremely high-level enemy intelligence collection target. Its disclosure to unauthorized persons could clearly result in serious degradation of the effectiveness of the SIOP and therefore, should be designated SIOP-ESI. The Joint Chiefs of Staff consider that distribution of and access to SIOP-ESI must be strictly limited and based on rigorously justified operational requirements or need to know and must be protected under the special access provisions set forth below.

d. (U) DOD 5200.1-R requires all Special Access Programs in the Department of Defense to be reviewed every 5 years to determine continued necessity. The next review of the SIOP-ESI Special Access Program will be accomplished in June 1989.

2. (U) References. Documents referenced in this directive are listed in Annex F.

3. (U) Definitions

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

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

(2) (U) Painted or drawn material.

(3) (U) Electronic or magnetic recording, punchcards, or paper tape.

(4) (U) Sound recordings.

(5) (U) Photographs.

(6) (U) Reproductions of the foregoing by whatever process.

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

b. (U) SIOP-ESI. Detailed TOP SECRET information and material of such an extremely sensitive nature that its

compromise would seriously degrade the effectiveness of the SIOP. Paragraph 4 below discusses specific kinds of information that are considered to be SIOP-ESI.

c. (U) JCS SIOP Documents. The JCS SIOP (Basic) and annexes, appendices, and tabs thereto, and associated source data.

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

e. (U) SIOP Briefings. Any briefing that includes detailed extracts of SIOP information derived from material described as SIOP material in subparagraphs 3a through 3d above and paragraph 4 below.

4. (U) Identification of SIOP-ESI

a. (S)

(1) (S)

(2) (S)

(3) (S)

(4) (S)

(5) (S)

(6) (S)

b. (U) The following JCS and JSTPS documents, because the level/amount of detail meets the criteria of subparagraph 4a above, are considered to be extremely sensitive and are

designated, in their entirety, as SIOP-ESI documents.

(1) (U) JSTPS AC&S Consequences of Execution with Tabs and SRF Damage Analysis.

(2) (U) Appendix III to SIOP Annex E (Coordinating Instructions).

(3) (U) SIOP Annex F (Strike Assignments and Force Timing) and Appendices I, II, III, IV, and V thereto.

(4) (U) JCS SIOP Summary, SIOP Annex F (Strike Assignments and Force Timing).

(5) (U) JCS SIOP Decision Handbook (Black Book).

(6) (U) JCS Emergency Action Procedures, Volumes II and IV.

(7) (U) SIOP Revision Reports.

(8) (U) Consolidated SIOP Analysis Document.

NOTE: Information extracted from these or any SIOP-ESI document is considered to be SIOP-ESI until such time as it has been reviewed by an individual who has been designated as an original TOP SECRET classification authority in accordance with DOD 5200.1-R and determined not to meet the criteria for SIOP-ESI stated in subparagraph 3b above.

c. (U) Reconnaissance data are not SIOP-ESI.

d. (S)

e. (U) Agencies responsible for SIOP wargaming and

exercises will consider the following:

(1) (Ø)

[redacted]

(2) (U) The JSTPS and J-8 SIOP war game reports will be classified TOP SECRET and marked SIOP-ESI Category XX when they include information described in subparagraph

*SM-81-77, 1 Feb 77, "Basic Policy Guidance on Wargaming (U)"

4a above. Upon completion, war game reports involving the SIOP will be submitted to the Joint Chiefs of Staff for review and approval. An integral part of the approval procedures for such reports will be the review and approval of the classification assigned by the originator. Reports can be released in accordance with the provisions of JCS MOP 39, subparagraph 2a(2) as JCS papers or paragraph 6 of this directive as appropriate.

(3) (U) The use of SIOP-ESI data in the play of command post exercises and other war plan exercises is not authorized without the approval of the Director, Joint Staff. The Director for Operations, Joint Staff, shall review such requests and submit recommendations to the Director, Joint Staff, for approval.

f. (U) The listing delineated by subparagraphs 4a through 4e above is not to be construed as limiting or all inclusive, nor will the listing be maintained in a current status by changes to this directive.

5. (U) Security Classification and Marking

a. (U) All SIOP documents shall be classified and marked in accordance with DOD 5200.1-R. Documents containing

SIOP-ESI, as defined and described in paragraphs 3 and 4 above, shall bear additional markings, as prescribed herein.

b. (U) SIOP-ESI documents shall be classified TOP SECRET only. In order to permit immediate and positive identification of these documents, the indicator "SIOP-ESI Category XX" (i.e., 01-10) shall be prominently affixed to the front and back cover. This indicator shall also be applied to compilations of documents which, although not SIOP-ESI individually, may, in the aggregate, be so considered.

c. (U) Correspondence, reports, studies, messages, and any other media relaying SIOP-ESI shall include the following statement:

> "This (correspondence, memorandum, report, etc.) contains SIOP-ESI Category XX data. Access lists govern internal distribution."

d. (U) Messages containing SIOP-ESI shall include the designator "SPECAT" and the indicator "SIOP-ESI Category XX" with the Category number spelled out, for example "SPECAT SIOP-ESI CATEGORY ONE," at the beginning of the message text immediately following the message

classification, in accordance with ACP 121 US Supp-1 (Series), followed by the statement in subparagraph 5c above. Supporting telecommunications centers will distribute SIOP-ESI messages based on the SIOP-ESI category number and access/distribution lists provided by recipients of SIOP-ESI message traffic.

e. (S)

* MJCS-273-83, 23 December 1983, "Guidance for the Sanitization and Distribution of SIOP Information to SACEUR and SACLANT"

f. (U) The SIOP-ESI indicator is NOT a separate security classification. This indicator is intended solely as a mechanism for identifying SIOP-extremely sensitive information that must be controlled in accordance with the special access procedures established by this directive. Care must be taken to ensure that the SIOP-ESI indicator is applied to documents only when the contents contain information of the type and quantity set forth in paragraphs 3 and 4 above. 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.

g. (U) SIOP documents, except those sanitized and authorized for release to NATO under the provisions of MJCS-273-83 shall be labeled "Not Releasable to Non-US Agencies Without Permission of the Originator."

6. (U) Distribution of SIOP Material and Extracts

a. (U) The Director for Operations, Joint Staff, OJCS, will review the requirements of all users of the JCS SIOP prior to the publication of each SIOP and report recommended distribution lists will be included in the promulgating directives for each SIOP.

(1) (U) Requests to change approved distribution lists will be submitted, with justification, to the Director for Operations, Joint Staff, OJCS. The Director for Operations, Joint Staff, will forward his consideration and recommendations to the Director, Joint Staff, who is authorized to approve/disapprove such requests. The Director of Strategic Target Planning (DSTP) will be notified of approved changes.

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

b. (U) 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 6a above, with the following stipulations:

(1) (U) Unless an exception is stated in the approved distribution lists, as provided in subparagraph 6a above, or amended under the provisions of subparagraph 6a(1) or 6a(2) above, JCS SIOP materials distributed by the DSTP will contain only those data necessary for the accomplishment of the assigned tasks, missions, and responsibilities of the addressee.

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

(a) (U) The DSTP will forward one copy of each required tape to The Joint Chiefs of Staff, Attention: J-3 Nuclear Warfare Status Branch (NWSB), and one copy to the Joint Coordination Center (JCC), Fort Ritchie, Maryland.

(b) (U) The Director for Operations, Joint Staff, will reproduce tapes, as required, to satisfy the approved requirements of users in the Washington, D.C., area. The JCC will use its copy of tapes provided to support JCS requirements delineated in JCS Pub 6, Volume II, Part 1.

(c) (U) Requests by approved users 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. (U) The DSTP is authorized to make distribution of JSTPS SIOP materials as follows:

(1) (U) All JSTPS SIOP material to:

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

(b) (U) OJCS.

(c) (U) Commands designated by the Joint Chiefs of Staff.

(2) (U) Distribution of JSTPS SIOP materials to the commands or agencies not covered in subparagraphs 6a through 6c(1) will be considered on a case-by-case basis. Requests will be submitted to the DSTP with sufficient justification to complete an appraisal. The DSTP may approve such requests as 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 action.

d. (U) Requests for copies of changes to the distribution schedule for the SIOP publication, "JSTPS Air Defenses Handbook," will be forwarded to the DIA Dissemination Center.

e. (U) The Chairman, Joint Chiefs of Staff, consulting the other Joint Chiefs of Staff, as appropriate, will approve/disapprove requests for SIOP documents from the White House and members of the Senate and House of Representatives.

f. (U) Requests for release of SIOP documents to foreign nationals will be submitted to the Director for Operations, Joint Staff, for review and recommendations to the Joint Chiefs of Staff, except as noted below.

(1) (U) The DSTP is authorized, in coordination with the SACEUR Senior Representative (SACEUR Rep) to the JSTPS, to disclose US classified information, relative to current and subsequent SIOPs, to SACEUR and the SACEUR Rep to JSTPS, pursuant to, and in accordance

with, the policies contained in NDP-1* and JAIEG Case N-15/75F.**

(2) (U) Similarly and in accordance with the same policies, the DSTP is authorized to disclose such SIOP information to SACLANT as is essential for adequate understanding and effective coordination of nuclear forces planning.

(3) (U) Procedures for handling US SIOP information within NATO is contained in Annex B to Attachment 1 of USSAN Instruction 1-69 (DOD 5700.55, Encl 2), "United States Implementation of NATO Security Procedures (U)"

g. (U) 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 accomplishment of assigned tasks, missions, and responsibilities. Reproduction of SIOP document extracts

---

* NDP-1, 9 Sep 81, "National Policy and Procedures for the Disclosure of Classified Military Information to Foreign Governments and International Organizations (National Disclosure Policy)"

** Joint Atomic Information Exchange Group (JAIEG) memorandum JAIEG Case N-15/75F, 10 Dec 75, "Authorization and Release Procedures for SIOP ATOMAL Information to NATO (U)"

shall, in every case, be on a rigidly discriminating basis and shall be controlled in accordance with applicable directives, including this directive.

h. (U) Special procedures for processing extracts from SIOP-ESI documents are as follows:

(1) (U) Release of SIOP data to foreign nationals is prohibited, except as authorized under the NATO Documents Program and as approved by the Joint Chiefs of Staff. The release of SIOP-ESI data to SACEUR/SACLANT is discussed in subparagraph 6f above.

(2) (U) 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 extracts, or portions reproduced, retain characteristics of the type and quantity delineated in paragraphs 3 and 4 above and should be identified as SIOP-ESI.

i. (U) Requests for JCS SIOP documents not covered by subparagraphs 6a through 6h above will be submitted, with justification, to the Director for Operations, Joint

Staff, who will forward the requests and his recommendations to the Director, Joint Staff. The Director, Joint Staff, consulting the Chairman, Joint Chiefs of Staff, as appropriate, will approve/disapprove these requests.

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

7. (U) Inventory and Sighting

a. (U) All SIOP materials defined and identified in paragraphs 3 and 4 above will be inventoried annually, as a minimum, or more frequently, as prescribed by the classified material control procedures of the appropriate Service, joint agency, or command, except as specifically provided in subparagraph 7b below.

b. (U) SIOP documents that are effective for a single SIOP revision cycle 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 security directives of the appropriate Service, joint agency, or unified and specified command. Command internal inspection procedures will be established to ensure rigid adherence to those procedures.

c. (U) The DSTP and other originating agencies shall annually, as of 30 September, provide holders a list of documents as follows:

(1) (U) 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).

(2) (U) All documents not covered in subparagraph 7c(1) above that contain SIOP-ESI.

Documents controlled in accordance with subparagraph 7b above will be exempt from this requirement.

d. (U) Upon receipt of this listing, holders shall verify the listing, sight listed documents, and certify the

sighting to the originator, who in turn will forward a consolidated sighting report of each such annual sighting to the Secretary, Joint Chiefs of Staff. Discrepancies, if any, shall be handled separately in accordance with paragraph 16 below and reported to the Director, Joint Staff.

e. (U) 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.

8. (U) Access Control

a. (U) Control of Access to Non-ESI SIOP Information. Access to SIOP information not identified as SIOP-ESI will be controlled 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. (U) Control of Access to SIOP-ESI Information. Access to SIOP information designated SIOP-ESI shall be subject to special control procedures. Services, joint agencies, and commands holding or authorized to hold SIOP-ESI data are requested to provide implementing instructions for the special control procedures outlined below.

(1) (U) Access to SIOP-ESI shall be highly restricted and granted on a selective and discriminating need-to-know basis in accordance with the guidance set forth in subparagraph 1c above. This is especially true of the SIOP decision and execution process.

(2) (U) There may be two types of access, PERMANENT and TEMPORARY.

(a) (U) Permanent Access. After considering the functions of a given duty position, the frequency of anticipated access, and the categories of SIOP-ESI access required, access granting authorities listed in subparagraph 8c below may establish permanent SIOP-ESI billets. Although a person assigned to a permanent SIOP-ESI billet needs no further authorization for access to the categories of SIOP-ESI specified for the billet, holders of SIOP-ESI information must still verify a valid need-to-know before releasing SIOP-ESI information. PERMANENT ACCESS BILLETS WILL BE REVIEWED AND REAPPROVED BY ACCESS-GRANTING AUTHORITIES LISTED IN SUBPARAGRAPH 8c BELOW NOT LATER THAN 31 DECEMBER IN EACH EVEN-NUMBERED YEAR.

(b) (U) Temporary Access. Access-granting authorities listed in subparagraph 8c below may grant approval for temporary access, up to 1 year, for personnel involved in briefing, studies, or other activities that have a projected end date.

(3) (U) Criteria for Access. Normally, military personnel and civilian personnel subject to the provisions of the personnel policies of the Office of Personnel Management (OPM) and Department of Defense may not be authorized permanent or temporary access to SIOP-ESI unless they meet the basic eligibility criteria set forth below:

(a) (U) The individual shall be a US citizen.

(b) (U) The individual shall have a final TOP SECRET clearance granted in accordance with the policy and criteria prescribed in DOD 5200.2-R.

(c) (U) The individual shall have been the subject of a completed special background investigation (SBI) that meets the criteria set forth in DOD 5200.2-R or other types of background investigations listed in DOD 5200.2-R that are equivalent to an SBI.

Access for these individuals must be essential to the performance of their assigned duties and justified by their direct involvement in the review, development, maintenance, or implementation of the SIOP.

(4) (U) Those personnel previously granted access to SIOP-ESI based upon a background investigation (BI) that did not contain all of the elements of an SBI as set forth in DOD 5200.2-R shall be the subject of an SBI when a reinvestigation is requested for any reason, such as the development of adverse or questionable information or when a break in the period of access or Federal service exceeds 12 months.

(5) (U) Waiver of Access Criteria. When justified by compelling need:

(a) (U) A waiver of the basic eligibility requirement stated in subparagraph 8b(3)(b) above may be authorized by those access-granting authorities listed in subparagraphs 8c(1) through 8c(5) below for military personnel and civilian personnel subject to OPM and DOD personnel policies. This authority may not be delegated. Waivers should be approved only if the individual

concerned meets all the following criteria:

1. (U) Is being assigned to a position for which permanent access to SIOP-ESI is required.

2. (U) Already possesses an interim TOP SECRET clearance granted in accordance with the policy and criteria prescribed in DOD 5200.2-R.

3. (U) Has been administered a screening interview equivalent to that which is used to screen nominees for access to Sensitive Compartmented Information (SCI).

4. (U) Has an SBI initiated.

(b) (U) A waiver of the basic eligibility requirement stated in subparagraph 8b(3)(c) above may be authorized for military personnel and civilian personnel subject to OPM and DOD personnel policies. Such waivers must be approved by flag officer-level, access-granting authorities as authorized in subparagraphs 8c and 8d below. In cases where a flag officer is not routinely available to the unit and delays in processing will result in unacceptable operational delays in assigning personnel to SIOP-related duties, this authority may be delegated in writing to O-6 level operational unit commanders (i.e. Submarine

Squadron Commanders, Wing commanders, or equivalent). To be granted a waiver, the individual concerned must meet all of the following criteria:

1. (U) Is being assigned to a position for which permanent access to SIOP-ESI is required.

2. (U) Already possesses a final TOP SECRET clearance that was based on a standard BI that meets the investigative standards of paragraph 2, Appendix B, DOD 5200.2-R.

3. (U) Has an SBI initiated.

(c) (U) Approval of waivers for contractor personnel will be made only by the Chairman, Joint Chiefs of Staff.

(6) (U) Flag-officer level, access-granting authorities, as authorized in subparagraphs 8c and 8d below, may approve temporary access to SIOP-ESI information for briefings, working meetings, etc., for personnel who do not have a completed SBI as required by subparagraph 8b(2), provided all of the following criteria are met:

(a) (U) Access is essential to the performance of duty and the individual is directly involved in the review, development, maintenance, or implementation of the SIOP.

(b) (U) The individual meets the other basic eligibility criteria specified in subparagraphs 8b(3)(a) and 8b(3)(b) above.

(c) (U) The individual is subject to military, OPM, or DOD personnel policies.

(7) (U) Civilian personnel not subject to provisions of OPM or DOD personnel policies (i.e., contractor personnel) will not normally be granted access to SIOP-ESI. Such civilian personnel shall not be granted permanent access to SIOP-ESI but may be granted temporary access for periods not to exceed 1 year. Requests for temporary access for such civilian personnel shall be referred to the Director, Joint Staff, for appropriate action. Personnel in this category for whom temporary access is approved shall possess a final TOP SECRET clearance and shall meet the basic security eligibility requirements of DOD Instruction 5220.28.

(8) (U) Prior to being granted permanent access, all personnel will be briefed on the contents of this directive and any supplemental directives considered appropriate. Once granted, continued access by individuals will be based on security assurance measures established by the granting authority. Upon termination of access, appropriate debriefing must be

accomplished. These briefings will emphasize 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 permanent SIOP-ESI access will execute an appropriate briefing/debriefing certificate, which will be maintained for a minimum of 1 year after the debriefing of an individual by the command granting access. These same requirements apply to personnel granted temporary access to SIOP-ESI, except as noted in subparagraph 12h below.

(9) (U) OJCS, Services, unified and specified commands, Defense agencies, and JSTPS will:

(a) (U) Develop procedures to maintain, at an appropriate level, SIOP-ESI access listings of personnel categorized by military, DOD civilian, and industrial contractor personnel. These listings will be current as of the last day of each quarter and will contain, at a minimum: billet number, name, rank/grade, social security number (SSN), office/activity/unit designator, category of

access, travel/duty restrictions (if applicable), and authorization document. Annex B is an example of a personnel access roster. Such lists shall be marked: "Subject to the Privacy Act of 1974 (5 USC, Section 552a)."

(b) (U) Be prepared to provide a numerical count of personnel having SIOP-ESI access within 5 working days after request, in the categories specified in subparagraph 8b(9)(a) above, to the Directorate for Information and Resource Management, OJCS, ATTN: Security Division. In any case, such a numerical report will be provided by 31 January of each calendar year. Close-out date for the report will be 31 December of the preceding year. To preclude duplication in recording, the following instructions apply:

1. (U) Services will record all personnel not assigned to the OJCS, Defense agencies, or to the staffs of unified and specified commands.

2. (U) Unified commands will record assigned headquarters personnel only.

3. (U) US Element NORAD and the specified

commands (US Space Command, MAC, and SAC) will divide personnel into two categories: headquarters and all others.

4. (U) JSTPS will record single-status and Scientific Advisory Group personnel.

5. (U) Guidance for recording of personnel in OSD, OJCS, non-DOD agencies, and the Defense agencies will be provided by a Joint Administrative Instruction.

(10) (U) The categories of SIOP-ESI listed in Annex A shall be used for access control.

(11) (U) Internal inspection procedures will give special and continuing attention to safeguards for SIOP-ESI.

c. (U) Authority to establish billets and grant access to SIOP-ESI is delegated to:

(1) (U) The Director, Joint Staff, for civilian personnel of the White House, members of the Senate and House of Representatives, and their staffs. Requests must be submitted to the Director a minimum of 7 work days prior to the date the access is required.

(2) (U) The Director, Joint Staff, for the Joint Chiefs

of Staff, members of the OJCS, other Joint Staff agencies, Defense agencies, military personnel assigned to the White House and National Security Council Staffs, OSD, civilian personnel not subject to the provisions of OPM or DOD policies (i.e., contractor personnel), and others as may be authorized by the Joint Chiefs of Staff. These requests must be submitted to the Director for Operations, Joint Staff, a minimum of 7 work days prior to the date the access is required.

(3) (U) The Chief of Staff, US Army; the Chief of Naval Operations; the Chief of Staff, US Air Force; and the Commandant of the Marine Corps for members of their respective Services and departmental staffs, and personnel assigned to the offices of the Secretaries of the Military Departments.

(4) (U) Commanders of unified and specified commands having responsibility for planning, preparation, coordination, and execution of the SIOP, for members of their staffs and subordinate command, and military personnel assigned to agencies directly supporting the CINC's SIOP-related missions.

(5) (U) The Director of Strategic Target Planning for members of the JSTPS.

d. (U) Access to SIOP data, including SIOP-ESI, normally shall not be given to foreign nationals, including members of NATO, except as authorized by the Joint Chiefs of Staff. Procedures for access to US SIOP data released to NATO in accordance with subparagraph 6f above are contained in Annex B to Attachment 1 of USSAN Instruction 1069 (DOD 5100.55, Enclosure 2). Access to SIOP-ESI data by US personnel assigned to NATO military organizations/ agencies normally will be restricted to those sanitized data allowed to be provided under the provisions of MJCS 273-83. US personnel assigned to NATO military organizations/agencies who are also members of USEUCOM or LANTCOM may be authorized access to other SIOP-ESI by USCINCEUR or USCINCLANT. US personnel assigned to NATO military organizations/agencies who are not also members of USEUCOM or LANTCOM may be authorized access to other SIOP-ESI by USCINCEUR.

e. (U) The authority to grant access delegated in sub-paragraph 8c above may be further delegated to

appropriate subordinates. Such further delegation shall be held at the highest rank and restricted to the minimum number of appropriately cleared individuals, consistent with operational requirements.

f. (U) Requests for SIOP-ESI access not covered above will be submitted to the Director for Operations, Joint Staff, who will forward the request and his recommendations to the Director, Joint Staff. The Director, Joint Staff, consulting the Chairman, Joint Chiefs Staff, as appropriate, will approve/disapprove these requests.

9. (U) Travel: Persons granted access to SIOP-ESI incur a special security obligation and must be aware of the risks associated with travel to or through hostile countries. SIOP-ESI-cleared personnel must be warned of the risks associated with capture, interrogations, harassment, entrapment, or exploitation by hostile nations or groups. Hazardous activities comprise assignments, visits to, travel through, and use of vessels owned or controlled by hostile countries, as well as assignment or travel in combat zones or other areas where hostilities or terrorist activities are taking place, duties behind hostile lines, and duties or

travel in isolated or exposed areas where individuals cannot reasonably be protected against hostile action. Individuals also must be advised of the potential for terrorism and the active and passive measures to avoid becoming a target or inadvertent victim of a terrorist act.

a. (U) Official Travel: All SIOP-ESI cleared personnel performing official travel outside the United States must receive a security/anti-terrorist briefing and or risk of capture briefing.

b. (U) Unofficial Travel: All SIOP-ESI-cleared personnel performing unofficial travel to or through hostile countries must comply with the provisions below. Failure to comply with these provisions may result in the withdrawal of approval for continued access to SIOP-ESI.

(1) (U) Give advance notice of such planned travel to local security officer.

(2) (U) Obtain anti-terrorism briefing from the security officer prior to performing such travel.

(3) (U) Immediately contact the nearest US Consul, Attache, or Embassy Regional Security Officer or Post Duty Officer if detained or subjected to significant

harassment or provocation while traveling.

(4) (U) Report to the specified official upon return from travel any unusual incidents, including incidents of potential security concern, encountered during such travel.

c. (U) SIOP-cleared individuals whose access is being terminated will be officially reminded of their continuing obligation to protect SIOP-ESI and will be informed of the risks associated with hazardous activities. After SIOP-ESI access is terminated, provisions of paragraph b no longer apply.

10. (U) Visits Requiring Access to SIOP-ESI. Prior to visits by personnel who will require access to SIOP-ESI data, the headquarters to be visited 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.

11. (U) Visits to JSTPS

a. (U) Requests for visits to JSTPS by civilian personnel of the White House, members of Congress, and Congressional Staff members will be submitted to and be reviewed and approved by the Director, Joint Staff.

All other requests for visits, except working level, will be sent to the Director for Operations, Joint Staff, for approval. The Director for Operations, Joint Staff, will approve/disapprove or forward as appropriate to the Director, Joint Staff, visit requests for individuals possessing appropriate clearances and a valid need-to-know.

b. (U) All requests for visits should be submitted a minimum of 7 working days prior to the visit. The timely submission of requests is necessary to provide sufficient time for adequate staffing within the Joint Staff. Requests should contain a detailed justification for the visit, type of information/briefing requested, point of contact at JSTPS, and recommendations on the appropriate type/classification of briefing to be given.

c. (U) Members of the Service or CINC staffs who are directly involved with SIOP development/support/implementation should contact the Joint Secretariat, JSTPS, directly for working-level visit approval. Other individuals from outside agencies possessing appropriate SIOP clearances who wish to visit JSTPS for working-level

meetings need only to notify J-3, Strategic Operations Division, of visit intentions.

12. (U) SIOP Briefings

a. (U) SIOP briefings may be given to those personnel under the control or military jurisdiction of the Joint Chiefs of Staff or of the Chief of Staff, US Army; the Chief of Naval Operations; the Chief of Staff, US Air Force; or the Commandant of the Marine Corps. Access for these individuals must be essential to the performance of their assigned duties and justified by their direct involvement in the review, development, maintenance, or implementation of the SIOP. Personnel who do not fall into this category require specific approval as indicated below.

b. (U) The SIOP shall not be used as a vehicle of instruction at joint or Service schools or other similar instructional institutions. Special SIOP briefings given to joint or Service schools shall not contain SIOP-ESI and will be classified TOP SECRET. Attendance of foreign personnel at these briefings is prohibited. SIOP briefings for the joint colleges may be scheduled and

conducted on a mutually acceptable basis through direct coordination between DSTP and the cognizant commandant. The Chiefs of the Services will provide approval of such requests from Service schools over which they exercise cognizance.

c. (U) SIOP briefings normally shall not be given to foreign nationals, including members of NATO. The Director, Joint Staff, may approve briefings for military members of NATO, provided the briefing is sanitized in accordance with MJCS 273-83. Other requests for SIOP briefings for foreign nationals may be approved by the Joint Chiefs of Staff.

d. (U) The Chairman, Joint Chiefs of Staff, consulting the other Joint Chiefs of Staff, as appropriate, will approve/disapprove requests for SIOP briefings for civilian personnel of the White House and members of the Senate and House of Representatives.

e. (U) Briefings on the SIOP Revision Report and War Games Report or briefings based on these reports may not be given except as provided in the foregoing subparagraphs or as approved in accordance with the provisions of JCS MOP 39 and this directive, as appropriate.

f. (U) Requests for SIOP briefings not covered above will be submitted to the Director for Operations, Joint Staff, who will forward the request and his recommendations to the Director, Joint Staff. The Director, Joint Staff, consulting the Chairman, Joint Chiefs of Staff, as appropriate, will approve/disapprove these requests.

g. (U) An approved attendance list will be prepared to control entry to SIOP briefings containing SIOP-ESI.

h. (U) Persons attending SIOP briefings containing SIOP-ESI must meet the criteria for eligibility for access to SIOP-ESI as specified in subparagraphs 8b(3), (5), and (6) above. Persons granted temporary access to SIOP-ESI to attend a briefing need not complete a briefing/debriefing certificate as required by subparagraph 8b(8) above, provided the briefing contains appropriate oral and visual warning regarding the sensitivity of the data in the briefing.

13. (U) Training. It is recognized that operational commands must conduct SIOP training in order to accomplish their strategic operational missions effectively. In this context, SIOP indoctrination is required by many operational personnel.

The policy guidelines for SIOP indoctrination are as follows:

a. (U) Access shall be strictly controlled on a need-to-know basis.

b. (U) Attendance at indoctrination briefings will be restricted to those personnel actually assigned to or en route to operational billets that require access to SIOP information.

c. (U) Indoctrination courses may be conducted at operational commands that hold SIOP documents or at those appropriate training facilities that are under the direct supervision/control of the component commanders of the several unified and specified commands. Curricula and associated material shall be approved by these commanders.

d. (U) The SIOP may be used as a vehicle of instruction provided that the precise area of indoctrination is correlated with billet requirements.

14. (U) Telecommunications System Processing of SIOP-ESI

a. (U) Special Category (SPECAT) SIOP-ESI Special Handling Designator. To preclude delivery of SIOP-ESI message traffic to a SPECAT terminal that is not specifically approved to receive SIOP-ESI messages, communications

systems shall apply a special handling designator in the security field of the communications heading of all electrically transmitted SIOP-ESI messages to enable automatic switch comparison of the SIOP-ESI designator against the destination security level authorization. A designator indicating SIOP-ESI has been established and is promulgated in ACP 121 US Supp-1 (Series). Message originators must include this designator in all SIOP-ESI messages (see paragraph 5d). Commanders having responsibility for terminals authorized to receive SPECAT (less SIOP-ESI) messages will ensure that adequate debriefing procedures are established in the event of inadvertent delivery of a SIOP-ESI message to the terminal affected.

b. (U) Connection of an ADP System that Processes SIOP-ESI to a Telecommunications System. An ADP system processing SIOP-ESI in accordance with the provisions of Annex C may be connected to telecommunications systems such as AUTODIN or other nondedicated telecommunications systems only when approved by the Joint Chiefs of Staff. Requests for approval to make such connections should be forwarded to

the Director for Operations, Joint Staff, OJCS. Requests should address as a minimum:

(1) (U) The procedures to be followed to ensure the safeguarding of SIOP-ESI.

(2) (U) Interface design features that will ensure the safeguarding of SIOP-ESI.

(3) (U) The results of evaluations of the interface design.

(4) (U) The results of tests of the interface.

(5) (U) Security findings and remaining vulnerabilities of security concern.

(6) (U) How reapproval will be handled if significant interface redesign is required in the future.

(7) (U) Conclusions and recommendations regarding security and the use of the interface to interconnect the ADP system to a telecommunications system.

c. (U) Accreditation of Telecommunications Systems To Process SIOP-ESI.

(1) (U) Telecommunications systems such as AUTODIN may process and transmit SIOP-ESI data only after the system has been accredited by the Joint Chiefs of

Staff. Requests to accredit telecommunications systems to handle SIOP-ESI should be addressed to the Director for Operations, Joint Staff, OJCS. Requests for accreditation should include details regarding implementation of a security certification/accreditation plan and adhere to guidance outlined in: Defense Intelligence Agency Manuals (DIAM) 50-3, "Physical Security Standards for Sensitive Compartmented Information Facilities"; DIAM 50-4, "Security of Compartmented Computer Operations;" and DIAM 50-5, "Sensitive Compartmented Information Contractor Administration Security." Upon development of the Security Certification/Accreditation Plan, it should be submitted to the Director for Operations, Joint Staff, OJCS, for review and comment by OJCS personnel. The plan will outline the procedures to be followed to ensure the safeguarding of SIOP-ESI. The plan should address how information security will be achieved at the outset and how reaccreditation will be achieved whenever significant portions of system hardware or software are changed. The plan will also address the

protective features outlined in subparagraph 5g(9) of Annex C. A suggested outline of the plan's contents is as follows:

(a) (U) Introduction - includes brief description of system, purpose, and scope of plan.

(b) (U) Responsibilities - identifies agencies participating in certification and accreditation activity and their roles and responsibilities.

(c) (U) System Overview - includes a functional description of the system with appropriate definitions of system components, interfaces, etc. Additionally, should address security concept, operational concept, maintenance concept, and procurement process.

(d) (U) Security Problem - identifies potential system security weaknesses.

(e) (U) Security Approach - describes computer security features and communications security considerations.

(f) Security Activities - describes actions and features implemented to ensure security.

(g) (U) Description of the Accommodation Package - describes documents comprising recommendation package to include the security certification evaluation.

(2) (U) Upon completion of system security activities, the final accreditation/certification request should be submitted for approval. The request should be accompanied by a security certification evaluation which addresses the following as a minimum:

(a) (U) System security design and mode of operation.

(b) (U) System security tests conducted.

(c) (U) Security findings and remaining vulnerabilities.

(d) (U) Conclusions and recommendations regarding security.

15. (U) Transportation of SIOP-ESI Material

a. (U) SIOP-ESI material not electrically transmitted via secured circuits shall be dispatched only by courier. The Armed Forces Courier Service (ARFCOS) should be utilized to the maximum extent feasible. Special handling

instructions within the ARFCOS system will be as prescribed by the Director, ARFCOS. Dispatching officials will designate the material SIOP-ESI when entering it into the ARFCOS system and will have the following statement affixed to the outside of the package or container in addition to the normal addresses and markings:

"RESTRICTED HANDLING REQUIRED"

(1) (U) Air transportation of this package will be in the following priority: military aircraft, regularly scheduled US commercial cargo aircraft, government-chartered commercial aircraft, regularly scheduled US commercial passenger aircraft (ARFCOS only).

(2) (U) TWO COURIERS ARE REQUIRED BETWEEN US MILITARY INSTALLATIONS/FACILITIES. ONE COURIER CAN BE USED DURING FLIGHT SO LONG AS TWO COURIERS DELIVER AND PICK UP MATERIAL AT PLANESIDE OFF MILITARY BASES.

(3) (U) 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.

(4) (U) COURIERS AND GUARDS MUST POSSESS TOP SECRET CLEARANCES BASED ON A COMPLETED BACKGROUND INVESTIGATION.

b. (U) Commanders supporting ARFCOS are responsible for providing arrangements for the transportation of SIOP-ESI material by military air. Priority will be provided to the shipment of SIOP-ESI material to meet the deadline delivery date.

c. (U) When not transported via ARFCOS, SIOP-ESI material being transported or processed outside military installations/facilities will be accompanied by two appropriately cleared couriers (in accordance with the handling restrictions delineated in subparagraph 15b above) assigned the primary responsibility for surveillance and security of the material. When utilizing authorized air transportation, as delineated in subparagraph 15c(1) and (2) below, 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 to maintain surveillance until the aircraft is airborne.

(1) (U) The following types of air transportation are authorized for movement of SIOP-ESI material:

(a) (U) Military aircraft.

(b) (U) US contract commercial aircraft when the manifest is under US military control.

(c) (U) US commercial nonpassenger cargo aircraft.

(2) (U) SIOP-ESI material WILL NOT be transported by any of the following means:

(a) (U) Commercial passenger aircraft (except for ARFCOS, as described above).

(b) (U) Department of State Diplomatic Courier Service.

(c) (U) Foreign or combined courier service (such as NATO).

(3) (U) Ground transportation of SIOP-ESI material will be, in order of priority, by US Government sedan, US Government bus, US Government chartered bus, commercial transportation.

16. (U) Actions in Case of Possible or Actual Compromise. The Joint Chiefs of Staff and the DSTP shall be informed by the most expeditious means available, consistent with security requirements, of any compromise or suspected compromise of any portion of any SIOP material. Such reports

will include specific identification of the document, whether or not SIOP-ESI is involved, and an opinion as to probability or possibility of compromise. The DSTP will recommend appropriate actions required with regard to modification of the plan or related procedures as a result of the actual or possible compromise for consideration by the Joint Chiefs of Staff. The provisions of Chapter VI, DOD 5200.1-R also apply.

17. (U) Machine Reproduction of SIOP-ESI. The capability of data reproduction by electronic means presents a special need for attention to security precautions where such means are used in processing classified material. The 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 that possess the means for 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 accounting for and controlling access to SIOP-ESI. In every case, such means shall ensure that numbers of copies, extracts, or information derivatives are limited to those required to serve valid needs. Access to documents and

reproduction equipment shall be limited to the minimum numbers of properly cleared personnel. Accountability systems shall ensure that all documents produced by electronic means, including ADP systems, are properly identified, marked, distributed, and safeguarded.

18. (U) ADP

a. (U) Safeguarding SIOP-ESI in an ADP environment requires special precautions achieved by using a combination of conventional security procedures and new automated techniques. Annex C delineates the minimum security requirements for ADP systems. ADP systems security should include the following:

(1) (U) ADP hardware features.

(2) (U) ADP software features.

(3) (U) Communications security.

(4) (U) Emanations security.

(5) (U) Physical security measures.

(6) (U) Personnel security measures.

(7) (U) Procedural safeguards (management, administrative, and operational procedures).

b. (U) Recording media used to store or process SIOP-ESI must retain the TOP SECRET classification and be

controlled as SIOP-ESI until one of the declassification procedures delineated in Annex D is carried out. The declassification procedures in Annex D apply to release of the recording media for maintenance of equipment, return of parts to contractor, and release of computers to contractors.

c. (U) The provisions of Annexes C and D may differ from the requirements of communications security (COMSEC) materials and information. Refer to appropriate COMSEC directives for security requirements and declassification procedures for COMSEC items when COMSEC and SIOP-ESI are being processed.

19. (U) Destruction. As a matter of policy, in order to ensure 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 and witnessing the destruction of material containing SIOP-ESI must have authorization for access to the category(ies) of SIOP-ESI contained in the material being destroyed.

ANNEX A

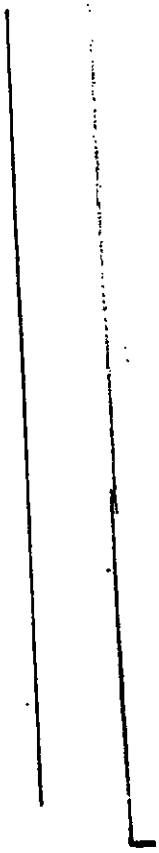
CATEGORIES OF SIOP-EXTREMELY SENSITIVE INFORMATION (SIOP-ESI) (U)

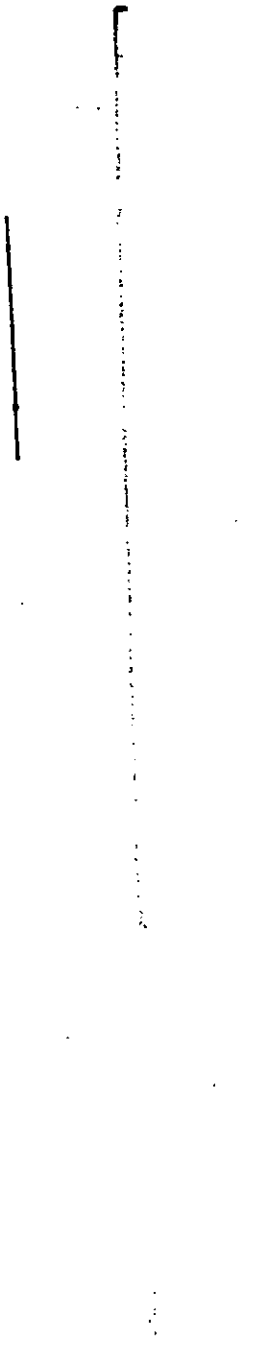
1. (U) Scrupulous discrimination must be used when granting access to Categories 01, 02, 04, 09, and 10. Use of one, or more, of Category 03, 05, 06, 07, or 08 is preferable to granting access to Category 01, 02, 04, 09, or 10. Access categories are not meant to be a list of greater or lesser sensitivity or exposure; they are meant to be subject restrictive. The categories are intended to limit access to the specific area of duty responsibility. Personnel granted permanent or temporary access to SIOP-ESI need no further authorization for access to the specific categories of SIOP-ESI specified for a billet; however, holders of SIOP-ESI information must still verify a valid need-to-know before releasing SIOP-ESI.

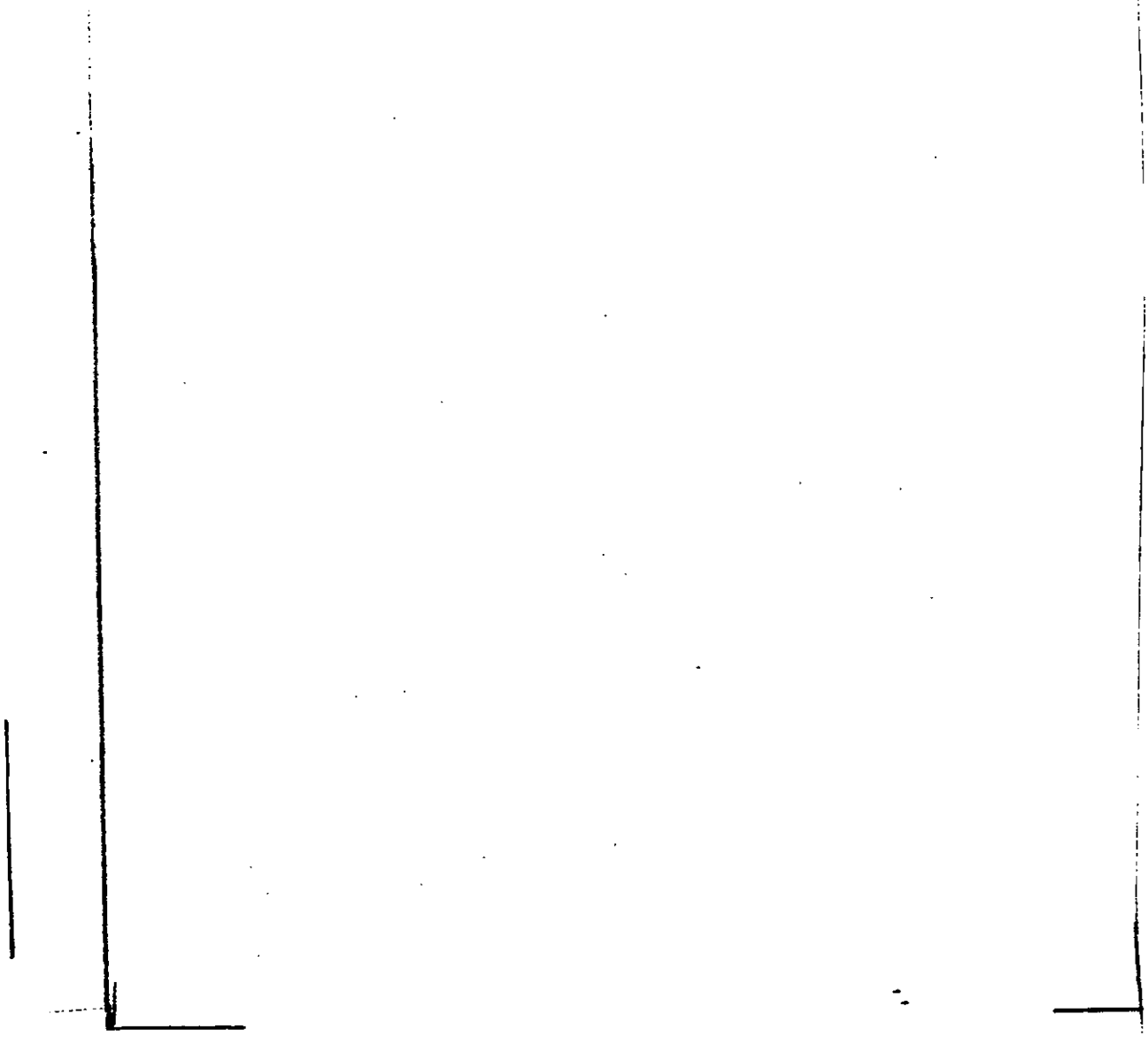
2. (U) Category numbers are unclassified. When associated with their definitions, they are CONFIDENTIAL.

3. (Ø)

CLASSIFIED BY DIRECTOR, J-3
DECLASSIFY ON OADR







UNCLASSIFIED

ANNEX B

EXAMPLES OF SIOP-EXTREMELY SENSITIVE INFORMATION ACCESS ROSTERS

SIOP-ESI PERMANENT ACCESS ROSTER FOR (AGENCY)
(Subject to Privacy Act of 1974)(5 USC 552a))

Billet No/SSN	Title/Name	Rank/Grade	Service	SIOP Categories	Authorization Document
XY000001 123-45-6789	Dir, XYZ Staff Doe, John Q.	GS-06	Civ	02 03 05 07	DJSM 1234-40, 28 Sep 1940
XY000002 987-65-4321	Dir, ABC Staff Tree, Tall F.	LTC	USA	01 04 09	J3M 4567-45 14 Jan 1945

SIOP-ESI TEMPORARY ACCESS ROSTER FOR (AGENCY)
(Subject to Privacy Act of 1974)(5 USC 552a))

Company	Name	SSN	SIOP Categories	Authorization Document	Expiration Date
ADPS	Doe, John Q.	123-45-6789	02 03 05 07	DJSM 1234-40 28 Sep 1940	28 Sep 1941
AIS	Tree, Tall F.	987-65-4321	01 04	J3M 4567-45 14 Jan 1945	14 Jul 1945

* Category of access does not automatically determine need for travel/duty restriction. Determination must be made on case-by-case basis, depending on an individual's frequency/degree of access (see Annex E).

UNCLASSIFIED

ANNEX C

MINIMUM SECURITY REQUIREMENTS FOR AUTOMATIC DATA PROCESSING SYSTEMS PROCESSING SIOP-EXTREMELY SENSITIVE INFORMATION (SIOP-ESI)

1. An Automatic Data Processing System (ADPS) is defined in DOD Directive 7920.1 as an interacting assembly of procedures, processes, methods, personnel, communications, and automatic data processing equipment to perform a series of data processing operations--a combination of automatic data processing resources and automated data systems. This definition is interpreted as including all peripheral devices used in performing data processing operations located within or remote to the central ADPS facility.

2. Authorities listed in subparagraphs 8c(1) through 8c(5) of the Appendix may approve the processing of data containing SIOP-ESI on an ADPS when operations are controlled as indicated below.

a. The preferred mode of operation is the Dedicated Security Mode as defined by paragraph 1-211, DOD 5200.28-M.

"All portions of this annex are UNCLASSIFIED"

b. In exceptional cases where the Dedicated Security Mode of Operations is not reasonably practicable, the System High Security Mode as defined by paragraph 1-227, DOD 5200.28-M may be used.

c. Regardless of whether the Dedicated Security Mode or the System High Security Mode is used, the ADPS including all of its connected peripheral devices and remote terminals, must be dedicated to the processing of SIOP-related and/or SIOP-ESI and be under the exclusive control of persons who are authorized access to SIOP-ESI.

d. All peripheral devices in areas not manned by personnel cleared for SIOP-ESI must be disconnected from the ADPS by either a manually thrown switch or by unplugging at a patch panel.

3. Efficient utilization of the ADPS is important but should not be used as a criterion for determining the need-to-know and access to SIOP-ESI.

4. Appropriate procedures will be established for debriefing persons not authorized access to SIOP-ESI should inadvertent disclosures of SIOP-ESI occur while processing under the modes of operation delineated in subparagraphs 2a and 2b above. Paragraph 16 of the Appendix will only apply in the

case of possible or actual compromise.

5. Requirements for ADPS containing SIOP-ESI are stated below:

a. ADPS Security Officer. A Security Officer properly cleared for access to SIOP-ESI will be appointed for each ADPS that will process data bases containing SIOP-ESI. The designated approving authority (DAA) for commands having operational responsibility for the ADPS will ensure such appointment. The responsibilities of the ADPS Security Officer will include:

(1) Ensuring that each site has written procedures that outline operator actions required for known fault/security events. These procedures should include operating restrictions, if required, and delineate reporting and investigation requirements.

(2) Ensuring continued compliance with all requirements for processing and storing data containing SIOP-ESI including the requirements of this directive.

(3) Ensuring that security deficiencies that occur in the operation of the ADPS are expeditiously reported to the command DAA.

(4) Curtailing system processing, pending investigation

when continued operation could lead to compromise.

(5) Conducting a review of audit trails for security-related activities.

Command DAAs will immediately forward to the Director for Operations, Joint Staff, all security deficiencies they consider significant and will forward annual certification that the system complies with all requirements for processing and storing data containing SIOP-ESI. If systems do not comply with all requirements for processing and storing data containing SIOP-ESI, command DAAs will list deficiencies and proposed corrective actions in their annual reports.

b. Personnel Security and Access Control Measures

(1) Unescorted access to any portion of the ADPS processing SIOP-ESI will be limited to personnel authorized access to SIOP-ESI. All other personnel requiring access to such areas must be escorted by personnel authorized access to SIOP-ESI. The area will be inspected prior to such visits to ensure that no SIOP-ESI is visible. Escorts are responsible for ensuring that no disclosure of SIOP-ESI occurs.

(2) A personnel access control system will be

maintained at the central site and at the remote terminal areas to permit ready identification of those persons authorized access to the ADPS.

(3) A record will be maintained of all persons that are escorted into the areas identified in subparagraph 5b(1) above. The ADPS Security Officer will ensure that this record is retained for a minimum of 12 months from the date of the last entry in the log.

c. Physical Security Protection. Physical security will be in accordance with DOD Directive 5200.1, DOD Regulation 5200.1-R, DOD Directive 5200.28, and DOD Manual 5200.28-M.

d. Communications Links. All communications links will be secured in accordance with DOD Directive C-5200.5 for the classification of information transmitted. When connection is approved by the Joint Chiefs of Staff (see subparagraph 14b of the Appendix) and is connected in accordance with subparagraph 5g(9) of this annex, and ADPS that processes data containing SIOP-ESI may be conducted to nondedicated telecommunications systems that have been accredited for the transmission of SIOP-ESI (see subparagraph 14c of the Appendix).

e. Emanations Security. All equipment associated with an

ADPS, including remote terminals, modems, multiplexers, crypto devices, patch panel, etc., that is used to process data containing SIOP-ESI must meet the objectives of DOD Directive S-5200.19. ADPS equipment processing SIOP-ESI, and not previously TEMPEST tested, will be tested and evaluated at the earliest possible date. If the ADPS equipment is found to be deficient, appropriate counter-measures will be implemented immediately and a plan will be developed to phase in equipment that will meet TEMPEST standards at the earliest possible date.

f. Security Classification Responsibilities. The user is responsible for verifying that no extraneous data are included in his output product and that the security classification indicated on the product is consistent with the data contained therein. He is also responsible for reporting all discrepancies.

g. Software/Hardware Controls. The following features will be implemented in each ADPS that is to be used to process data containing SIOP-ESI. Special controls will be implemented governing access to, and modifications of, these features. Where implementation of the following features is not feasible because of equipment configuration

or other legitimate reason, other compensating controls will be developed and approved for implementation by command DAA.

(1) Security Markings and Special Access Labels

(a) All printed material produced from ADPS containing SIOP-ESI and operating in accordance with paragraph 2 above will have machine-produced security markings and special access labels at the top and bottom of each page equivalent to the highest classification of the data contained in the product. In addition, the front covers will be marked with a SAFEGUARD statement (see Tab).

(b) Removable storage media; i.e., tapes, card decks, discs, and similar devices used to store data bases containing SIOP-ESI will contain TOP SECRET classification markings in accordance with DOD 5200.1-R, with the SIOP-ESI label appropriately affixed to the storage media. These security markings/labels will be retained until the device is declassified by approved procedures described in Annex D.

(2) User Identification/Authentication. Operation of the ADPS will include a mechanism that identifies and authenticates user personnel accessing it remotely. This mechanism will consist of software and/or hardware devices, manual control procedures at terminal sites, or other appropriate measures designed to validate the identity and access authority of system users.

(3) Memory Protection. System hardware and software features will exercise control over the addresses to which a user program has access.

(4) Separation of User/Executive Modes of Operation. The user and executive modes of an ADPS will be separated so that a program operating in user mode is prevented from performing unauthorized executive functions. Controls will be implemented to maintain continued separation of these modes.

(5) Memory Residue Clean-Out. Measures will be implemented to ensure that memory residue from terminated user programs is made inaccessible to other users. This will be accomplished as required by DOD 5200.28-M.

(6) Access Control. Effective controls will be implemented to limit user and terminal access to authorized information and programs as well as to control read and/or write capability. In addition to software, positive disconnection of hardware can also be used to control remote terminals. Each individual user of the system will have a unique unclassified user identification (ID) assigned. Access attempts from remote terminals will be limited to TWO attempts, after which the terminal will automatically be locked-out and the ADP Security Officer notified.

(7) Audit Trail Capability. Each ADPS will produce an audit trail as defined in DOD 5200.28-M containing sufficient information to permit a regular security review of system activity. Audit trail information will be controlled closely by the ADPS Security Officer and, since SIOP-ESI may be contained therein, should be marked and handled as SIOP-ESI until actual classification is determined.

(8) Changing into and out of SIOP-ESI Operations

(a) Before starting to process SIOP-ESI, the area

must be cleared of all unauthorized personnel and unauthorized peripheral devices must be disconnected. The point of disconnect must be under the control of personnel cleared for SIOP-ESI.

(b) After processing is completed, all removable storage media containing files and/or programs used during SIOP-ESI processing will be disconnected from the ADPS. If any SIOP-related files or programs were used and those files or programs are to be used in a non-SIOP-ESI processing environment, they must contain no SIOP-ESI or must be purged of any SIOP-ESI prior to such use. All nonremovable storage media and memory must be cleared of all SIOP-ESI. Erase and overwrite procedures delineated in Annex D apply if the ADPS is to be used in an unclassified mode.

(9) Communication Connectivity. If an ADPS that has been approved for processing SIOP-ESI is also approved for interface with an external telecommunications system, such as AUTODIN or other telecommunication systems, while processing SIOP-ESI, the following

additional protective features are required:

(a) All interfacing telecommunications channels will be protected by cryptographic equipment or approved protective wireline distribution system.

(b) Specific measures will be implemented to prevent remote programming of the ADPS via external telecommunications.

(c) Procedures will be implemented to protect against accidental spillage of the data base into external telecommunications.

(d) Procedures will be implemented for fault monitoring that will detect malfunctions and halt processing when such malfunctions degrade any protective feature.

(e) Authentication procedures will be employed when telecommunications are used for ADPS-to-ADPS operations and/or ADPS-to-Remote user operations to limit access to SIOP-ESI to those network terminals and ADPS authorized to handle the data.

h. Individual Security Responsibilities. All users of the ADPS will be briefed on the need for exercising sound

security practices in protecting the information stored, processed, and produced by the system. Users will be informed when the system is operating in accordance with paragraph 2 above. Receipt of any information not specifically requested and of an unknown source shall be reported immediately to the ADPS Security Officer.

i. Civilian Contractor ADP Maintenance Personnel. These personnel will not be granted access to computer centers where data containing SIOP-ESI is resident in the ADPS unless the provisions of subparagraphs 8b(7) and 8b(8) of the Appendix have been met.

j. Reports. When an inadvertent disclosure occurs involving an ADPS processing SIOP-ESI, the report required in paragraph 16 of the Appendix shall be expanded to include at a minimum:

(1) An abstract of the problem.

(2) The type and source (e.g., Annex F data from disc pack) of the data involved.

(3) The ADP equipment involved.

(4) The number of people inadvertently exposed to the data.

(5) An assessment of the risk of compromise of the data.

(6) Immediate action taken (e.g., system processing curtailed as authorized by subparagraph 5a above).

(7) Steps being taken to preclude a recurrence of the problem.

(8) Comments and recommendations regarding problems considered to be of concern to the SIOP community and not restricted to the reporting site. This information is essential in order to determine the disclosure risk level of SIOP-ESI throughout the SIOP community and to determine whether similar problems exist on a community-wide basis. Reports will be submitted on an "as-occurring" basis.

k. Exceptions. Requests for exceptions to the security measures stated above will be submitted to the Director, Joint Staff.

TAB TO ANNEX C

SAFEGUARD STATEMENT

SAFEGUARD

This ADP product was produced during a TOP SECRET SIOP-ESI period. Handle as TOP SECRET SIOP-ESI until this statement has been signed by an individual who is designated to determine that the security classification of this document is appropriately marked and that the document can assume the handling requirements for that classification. Report any unusual or unrequested output discrepancies immediately to: _____
Printed/Typed Name

Signature: _____, Date: _____

ADPS Security Officer

Room Number _____

Phone Number _____

This ADP product has been reviewed by the undersigned. The correct security classification of this document is _____.

Signature: _____, Date: _____

_____

Printed/Typed Name

Room Number _____

Phone Number _____

Tab to
Annex C

ANNEX D

DECLASSIFICATION PROCEDURES FOR ADP MEDIA-STORING SIOP-EXTREMELY SENSITIVE INFORMATION (SIOP-ESI) (U)

1. General. Safeguarding classified information in a computer or computer system requires special precautions because of the types of storage media and devices (magnetic drums, discs, disc packs, and tapes) used to store, record, or manipulate data that must be protected by appropriate classification and security controls until procedures in paragraph 2 below are carried out.

2. Declassification. The eventual temporary or outright release of the storage device or a system including storage media should be anticipated. Procedures to be used in the event a decision is made to release or deploy the storage media are as follows:

a. Magnetic Tapes. Tapes used to store magnetically recorded digital data may be degaussed and declassified by erasing with approved tape degaussers that meet technical specifications promulgated by the Department of Defense.

b. Magnetic Discs, Dics Packs, Drums, and Other Similar Rigid Magnetic Storage Devices (e.g., Core Memory).

"All portions of this annex are UNCLASSIFIED"

The equipment will be checked immediately prior to beginning or after (whichever is appropriate to the particular computer) the overwrite procedures to ensure that malfunctions do/did not occur that will prevent the classified information from being effectively overwritten. Further, when the capability exists, as an integral part of the storage subsystem, an a.c./d.c. erase will be applied to all data tracks before the tracks are overwritten and the overwrite verified. Thereafter, all storage locations will be overwritten minimum of three times: once with all binary ones; once with all binary zeros; and once with a single numeric, alphabetic, or special character. Such alphanumeric or other unclassified data shall be left on the device. The current used in overwriting must be equal to or greater than that used in recording the information but of a strength that will not damage or impair the equipment.

c. Inoperative Magnetic Drums, Discs, Disc Packs, and Similar Rigid Storage Devices. If the storage device has failed in such a manner that it cannot be overwritten, the device may be declassified by exposing the recording surface(s) to a magnet having a field strength at the

recording surface of at least 1,500 Oersted. Care must be taken to ensure that the entire surface is wiped at least three times by a nonuniform motion of the magnet. Care must be taken to ensure that all tracks are covered by the center of the magnet. A thin sheet of clear plastic (a 1-5 mil sheet) should be used to prevent damage to the recording surfaces.

d. Internal Memory. Detailed memory erase or clearing programs or routines should be prepared by qualified automatic data processing programmers and approved and controlled by the Automatic Data Processing System (ADPS) Security Officer. Declassification procedures for main or internal memories depend on the type and characteristics of the memory.

(1) Ferrite Core Memory. Ferrite core memory used in processing information classified SECRET and below must be declassifed by setting each addressable memory location alternately to binary high values and binary low values for 100 cycles until the state is changed at least 99 times. The same procedure applies for declassifying core memory used for processing

TOP SECRET information, except that the state must be changed at least 999 times.

(2) Plated Wire Memory. Plated wire memory used to continuously store classified information undisturbed more than 8 hours may not be declassified. Such media will continue to retain their classification until physically destroyed. If the classified information is stored less than 8 hours and unclassified data is later stored for at least an equal time, the memory may be declassified according to the procedures for magnetic ferrite core memory.

(3) Semiconductor Memory. Semiconductor memory may be declassified according to the procedures for magnetic ferrite core, except for volatile semiconductor memory. Volatile semiconductor memory may be declassified by setting "0" or "1" in all memory locations.

e. Magnetic Storage Media Used To Store Analog, Video, or Similar Nondigital Information. Magnetic tape used to record analog, video, or similar types of nondigital information may be declassified by degaussing as in subparagraph 2a above. There is no approved overwrite

method for declassifying rigid magnetic storage media used for nondigital information; specific guidance may be obtained as stated in paragraph 5 below. In the case of a failure of the tape degausser or in the absence of an approved overwrite method for rigid surfaces, a magnet may be used, as described in subparagraph 2c above.

3. Disposition Approval. With the specific approval in each case of the designated (systems) approving authority (DAA) within the DOD component that is responsible for the security features of the ADPS, storage media treated as above may be handled as unclassified and released as necessary.

4. Records. A record of the procedures used to declassify each storage media device shall be maintained for a period of 2 years after disposition of the media or device.

5. Specific Guidance

a. Guidance for eradication of storage media not covered above may be obtained by submission of all pertinent details to the Director, Joint Staff, for consideration on a case-by-case basis.

b. In the absence of eradication by approved equipment or procedures or at the direction of the designated official

responsible for the security features of the ADPS, magnetic information storage media will be safeguarded in the manner prescribed for the highest classification ever recorded thereon until it is destroyed.

ANNEX E

SECURITY POLICY CONCERNING TRAVEL AND ASSIGNMENT OF PERSONNEL WITH ACCESS TO SIOP-EXTREMELY SENSITIVE INFORMATION (SIOP-ESI) (U)

1. (S)

2. (U) Purpose. This policy is based upon the need to protect SIOP-ESI from possible compromise resulting from the capture, interrogation, exploitation, or entrapment of personnel who have or have had access to SIOP-ESI.

CLASSIFIED BY DIRECTOR, J-3
DECLASSIFY ON OADR

3. (U) Definitions

a. (U) SIOP-ESI. SIOP-ESI is defined in subparagraph 3b of the Appendix.

b. (U) Hazardous Activities. Hazardous activities include assignments or visits to and travel through countries listed in the Tab. Hazardous activities also include assignment or travel in combat zones or other areas where hostilities are taking place, duty behind hostile lines, and duty or travel in isolated or exposed areas where individuals cannot reasonably be protected against hostile action.

c. (U) Foreign Travel Briefings. These briefings alert traveling personnel to the potential for harassment, provocation, or entrapment by foreign intelligence services in overseas areas and in other environments of an international nature, such as conferences, scientific and technical meetings, seminars, and symposiums. They examine foreign intelligence service methods of operation and suggest precautions designed to minimize the risk of direct foreign intelligence exploitation of personnel during periods of temporary duty or leave.

d. (U) Antiterrorist Briefings. These briefings advise personnel of a variety of measures that may be employed to safeguard oneself against terrorist threats in overseas areas.

4. (U) Policy. Personnel who have detailed knowledge and continuing access to SIOP-ESI information at Service, joint agency, or unified and specified command level may be subject to travel and assignment restrictions, as determined by the authority granting access.

a. (U) Official Assignment/Travel

(1) (U) To the extent practicable, personnel with detailed knowledge and continuing access to SIOP-ESI should not be assigned to or directed to participate in hazardous activities. Regardless of the degree of access, all personnel who have access to SIOP-ESI must be appropriately briefed prior to participation in any hazardous activity or visit as defined in subparagraph 3b above.

(2) (U) Prior to official visits to or travel through the countries listed in the Tab, personnel who have access to SIOP-ESI must:

(a) (U) Give their supporting security office advance notice of such planned travel.

(b) (U) Obtain foreign travel and antiterrorist briefings before traveling to such countries.

(c) (U) Immediately contact the nearest US Consul Attache, or Embassy Regional Security Officer or Post Duty Officer if detained or subjected to significant harassment or provocation while traveling.

(d) (U) Report to the specified official upon return from travel any unusual incidents, including incidents of potential security concern, encountered during such travel.

NOTE: Individuals who frequently travel, or attend or host meetings of foreign visitors of the types described in subparagraphs 3c above, need not be briefed for each such occasion, but shall be provided a thorough briefing at least once each 6-month period and a general reminder of their security responsibilities prior to each such activity.

b. (U) Unofficial Travel

(1) (U) Prior to unofficial visits to or travel through the countries listed in the Tab, personnel who have access to SIOP-ESI must take the actions outlined in

subparagraph 4a(2) above.

(2) (U) Access-granting authorities may deny unofficial travel by notifying the requester in writing of the specific conditions upon which the denial is based.

c. (U) Actions Required of All Persons Traveling to or Through Designated Countries (see Tab).

(1) (U) During official or unofficial visits to or travel through the countries listed in the Tab, persons who have access to SIOP-ESI MUST immediately contact the nearest US consular, attache, or Embassy official if they have been detained or subjected to significant harassment or provocation while traveling.

(2) (U) Persons who have access to SIOP-ESI must be reminded annually of the foregoing obligations through security education programs.

d. (U) Individuals With Previous Access. Persons whose access to SIOP-ESI is being terminated will be officially reminded if their obligation to ensure continued protection of SIOP-ESI and reminded of the risks associated with hazardous activities as defined herein.

5. (U) Responsibilities

a. (U) The Directorate for Information and Resource Management, OJCS, will prepare and disseminate to the holders of this document an updated list of countries (Tab) identified as posing a security risk bearing on this policy as changes occur.

b. (U) Access-granting authorities will issue implementing directives concerning travel and assignment of personnel under their cognizance.

TAB TO ANNEX E

COUNTRIES AND AREAS IN WHICH VISITS, TRAVEL, AND ASSIGNMENT ARE CONSIDERED TO BE A HAZARDOUS ACTIVITY (U)

(~~C~~)

CLASSIFIED BY DIRECTOR, J-3
DECLASSIFY ON OADR

ANNEX F

REFERENCES

1. Executive Order 12356, 2 April 1982, "National Security Information"

2. Public Law, 93-579, Title 5, United States Code, Section 552a, (Privacy Act of 1974)

3. DOD Directive 5100.55, 21 April 1982, "United States Security Authority for North Atlantic Treaty Organization Affairs" (USSAN Instruction 1-69)

4. DOD Directive 5200.1, 7 June 1982, "DOD Information Security Program"

5. DOD Regulation 5200.1-R, June 1986, "Information Security Program Regulation"

6. DOD Regulation 5200.2-R, January 1987, "DOD Personnel Security Program"

7. DOD Directive C-5200.5, 6 October 1981, "Communications Security (COMSEC) (U)"

8. DOD Directive S-5200.19, 10 February 1968, "Control of Compromising Emanations (U)"

9. DOD Directive 5200.28, 29 April 1978, "Security Requirements for Automatic Data Processing (ADP) Systems"

10. DOD Manual 5200.28-M, 25 June 1979, "ADP Security Manual" 1

11. DOD Instruction 5220.28, 8 March 1978, "Application of 2
Special Eligibility and Clearance Requirements in the SIOP- 3
ESI Program for Contractor Employees" 4

12. DOD Directive 7920.1, 17 October 1978, "Life Cycle 5
Management of Automated Information Systems (AIS)" 6

13. JCS MOP 39, 28 September 1983, "Release Procedures for 7
JCS Papers" 8

14. JCS Pub 6, Volume II, Part 1, 1 October 1985, "Standing 9
Operating Procedures for the Coordination of Atomic 10
Operations (CAO SOP) (U)" 11

15. MJCS-273-83, 20 December 1983, "Guidance for the 12
Sanitization and Distribution of SIOP Information to SACEUR 13
and SACLANT" 14

16. SM-81-77, 1 February 1977, "Basic Policy Guidance on 15
Wargaming (U)" 16

17. SM-283-81, 24 April 1981, "Emergency Action Procedures of 17
the Joint Chiefs of Staff (EAP-JCS), Volume II - SIOP 18
Instructions (U)" 19

18. J3M-2061-83, 1 August 1983, "Emergency Action Procedures 20
of the Joint Chiefs of Staff, Volume IV - Alternate 21
Procedures (U)" 22

19. NDP-1, 9 September 1981, "National Policy and Procedures for the Disclosure of Classified Military Information to Foreign Governments and International Organizations (National Disclosure Policy)"

20. Joint Atomic Information Exchange Group (JAIEG) memorandum, JAIEG Case N-15/75F, 10 December 1975, "Authorization and Release Procedures for SIOP ATOMAL Information to NATO (U)"

21. JSTPS Air Defenses Handbook, October 1980

22. ACP 121 US Supp-1(Series), June 1981, "Communications Instructions-General"

23. USSAN Instruction 1-69 (DOD 5100.55, Encl 2), 1982, "United States Implementation of NATO Security Procedures (U)"

SECRET

1 December 1987

FIRST CORRIGENDUM TO MJCS 75-87

"Safeguarding the Single Integrated Operational Plan"

Note by the Secretaries

Holders are requested to substitute the attached revised pages and to destroy the superseded pages in accordance with security regulations.

Secretaries

INTERNAL STAFF PAPER
RELEASE COVERED BY
JCS MOP 39

Regraded UNCLASSIFIED
Without Attachment

OFFICE OF THE CHAIRMAN
THE JOINT CHIEFS OF STAFF
WASHINGTON, D.C. 20318-0001

Reply ZIP Code:
20318-0300

MCM-98-90
13 June 1990

MEMORANDUM FOR HOLDERS OF MJCS 75-87

Subject: First Note to Holders on "Safeguarding the Single Integrated Operational Plan"

1. The Appendix to MJCS 75-87 has been revised to reflect changes in the special background investigation waiver authority. Holders are requested to substitute the attached revised pages 26, 27, and 28, and to destroy the superseded pages in accordance with security regulations.

2. Holders of MJCS 75-87 are requested to attach a copy of this memorandum to the document for record purposes.

3. This memorandum and the enclosure are UNCLASSIFIED.

For the Chairman, Joint Chiefs of Staff:

GENE A. DEEGAN
Major General, USMC
Vice Director, Joint Staff

Enclosure

~~SECRET~~

SAFEGUARDING THE SINGLE INTEGRATED OPERATIONAL PLAN (U)

This is a sanitized copy.

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

MJCS 75-87

CLASSIFIED BY DIRECTOR, J-3
DECLASSIFY ON OADR

93-F-1436 #549

~~SECRET~~ DOCID

~~SECRET~~

THE JOINT CHIEFS OF STAFF
WASHINGTON, D.C. 20301-5000

MJCS 75-87
20 May 1987

MEMORANDUM FOR: DISTRIBUTION LIST

Subject: Safeguarding the Single Integrated Operational Plan

1. The Appendix contains the policy of the Joint Chiefs of Staff with regard to security of the Single Integrated Operational Plan (SIOP), the basic administrative and handling requirements, and the emphasis that must be placed on control of SIOP-Extremely Sensitive Information (SIOP-ESI).

2. This memorandum supersedes SM-313-83, 10 May 1983, "Safeguarding the Single Integrated Operational Plan."

3. Without enclosure, this memorandum is UNCLASSIFIED.

For the Joint Chiefs of Staff:

Richard A Burpee

RICHARD A. BURPEE
Lieutenant General, USAF
Director for Operations

Enclosure

~~SECRET~~

OFFICE OF THE CHAIRMAN
THE JOINT CHIEFS OF STAFF
WASHINGTON, D.C. 20318-0001

Reply ZIP Code:
20318-0300

MCM-98-90
13 June 1990

MEMORANDUM FOR HOLDERS OF MJCS 75-87

Subject: First Note to Holders on "Safeguarding the Single Integrated Operational Plan"

1. The Appendix to MJCS 75-87 has been revised to reflect changes in the special background investigation waiver authority. Holders are requested to substitute the attached revised pages 26, 27, and 28, and to destroy the superseded pages in accordance with security regulations.

2. Holders of MJCS 75-87 are requested to attach a copy of this memorandum to the document for record purposes.

3. This memorandum and the enclosure are UNCLASSIFIED.

For the Chairman, Joint Chiefs of Staff:

GENE A. DEEGAN
Major General, USMC
Vice Director, Joint Staff

Enclosure

[redacted]

1 December 1987

FIRST CORRIGENDUM TO MJCS 75-87

"Safeguarding the Single Integrated Operational Plan"

Note by the Secretaries

Holders are requested to substitute the attached revised pages and to destroy the superseded pages in accordance with security regulations.

Secretaries

INTERNAL STAFF PAPER
RELEASE COVERED BY
JCS MOP 39

Regraded UNCLASSIFIED
Without Attachment

[redacted]

DISTRIBUTION

	No. of Copies
Secretary of Defense	13*
Director of Central Intelligence	1
Chairman, Joint Chiefs of Staff	1
Chief of Staff, US Army	6
Chief of Naval Operations	4
Chief of Staff, US Air Force	5
Commandant of the Marine Corps	3
Commander in Chief, US Space Command	5
Commander in Chief, US Atlantic Command	4

* Includes copies for distribution to the following:

Assistant to the President for National Security Affairs	1
Director, White House Military Office	1
Director, Federal Emergency Management Agency	1
Director, US Secret Service, Department of the Treasury	1
Deputy Under Secretary of Defense for Policy	1
Director, Emergency Planning, Office of the Deputy Under Secretary of Defense for Policy	1
Director, Information Security, Office of the Deputy Under Secretary of Defense for Policy	1
Director, Security Plans and Programs, Office of the Deputy Under Secretary of Defense for Policy	1
Deputy Assistant Secretary of Defense (Comptroller) (Administration)	1
Director for Industrial Security Clearance Review, General Counsel	1
Director, Washington Headquarters Services	2

	No. of Copies
Commander in Chief, US Central Command	2
US Commander in Chief, Europe	2
Commander in Chief, Military Airlift Command	2
Commander in Chief, US Pacific Command	9
Commander in Chief, US Readiness Command	3
Commander in Chief, US Southern Command	5
Commander in Chief, Strategic Air Command	5
Director of Strategic Target Planning	8
US Representative to the Military Committee, NATO	1
Director, Defense Communications Agency	4
Director, Defense Intelligence Agency	7
Director, Defense Investigative Service	4
Director, Defense Logistics Agency	2
Director, Defense Mapping Agency	9
Director, Defense Nuclear Agency	3
Director, National Security Agency/Chief, Central Security Service (P-391)	1
Director, Joint Staff	1
Director for Manpower and Personnel, Joint Staff	1
Director for Operations, Joint Staff	13
Director for Logistics, Joint Staff	1

No. of Copies

Director for Strategic Plans and Policy, Joint Staff.....3

Director for Command, Control, and Communications Systems, Joint Staff.....3

US National Military Representative, SHAPE.....1

Commander, Joint Special Operations Command.....1

Director, Force Structure, Resources, and Assessment.....4

Director for Information and Resource Management, OJCS.....7

Chief, Alternate National Military Command Center.....2

Commander, Joint Coordination Center.....1

Chief, National Emergency Airborne Command Post.....4

Chief, Joint Atomic Information Exchange Group.....1

Secretary, Joint Chiefs of Staff.....14

TABLE OF CONTENTS

		Page No.
APPENDIX	SAFEGUARDING THE SINGLE INTEGRATED OPERATIONAL PLAN (U)	1
ANNEX A	CATEGORIES OF SIOP-EXTREMELY SENSITIVE INFORMATION (SIOP-ESI) (U)	A-1
ANNEX B	EXAMPLES OF SIOP-EXTREMELY SENSITIVE INFORMATION ACCESS ROSTERS	B-1
ANNEX C	MINIMUM SECURITY REQUIREMENTS FOR AUTOMATIC DATA PROCESSING SYSTEMS PROCESSING SIOP-EXTREMELY SENSITIVE INFORMATION (SIOP-ESI)	C-1
ANNEX D	DECLASSIFICATION PROCEDURES FOR ADP MEDIA STORING SIOP-EXTREMELY SENSITIVE INFORMATION (SIOP-ESI)	D-1
ANNEX E	SECURITY POLICY CONCERNING TRAVEL AND ASSIGNMENT OF PERSONNEL WITH ACCESS TO SIOP-EXTREMELY SENSITIVE INFORMATION (SIOP-ESI) (U)	E-1
ANNEX F	REFERENCES	F-1

[redacted]

APPENDIX

SAFEGUARDING THE SINGLE INTEGRATED OPERATIONAL PLAN (U)

1. (U) General

a. (U) The guidance 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) (U) Emphasize the need for strict observance of basic security regulations in safeguarding the SIOP.

(2) (U) Emphasize that stringent control must be exercised over SIOP-Extremely Sensitive Information (SIOP-ESI), as defined below.

(3) (U) Provide the basic policy for the identification of SIOP-ESI.

(4) (U) Set forth specific security controls and procedures to ensure that distribution of and access to SIOP-ESI are authorized with utmost discrimination in all cases.

b. (U) Executive Order 12356, DOD 5200.1 and DOD 5200.1-R provide instructions for the DOD Information Security Program. These documents prescribe measures for

CLASSIFIED BY DIRECTOR, J-3
DECLASSIFY ON OADR

classification, reproduction, accountability, safekeeping, storage, dissemination, and transmission of official information and include within their scope the documents that constitute the SIOP. This directive is supplemental to the preceding directives and applies more specifically to SIOP-ESI, as described herein.

c. (U) The Joint Chiefs of Staff consider the information described in subparagraph 3b and paragraph 4 to be an extremely high-level enemy intelligence collection target. Its disclosure to unauthorized persons could clearly result in serious degradation of the effectiveness of the SIOP and therefore, should be designated SIOP-ESI. The Joint Chiefs of Staff consider that distribution of and access to SIOP-ESI must be strictly limited and based on rigorously justified operational requirements or need to know and must be protected under the special access provisions set forth below.

d. (U) DOD 5200.1-R requires all Special Access Programs in the Department of Defense to be reviewed every 5 years to determine continued necessity. The next review of the SIOP-ESI Special Access Program will be accomplished in June 1989.

2. (U) References. Documents referenced in this directive are listed in Annex F.

3. (U) Definitions

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

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

(2) (U) Painted or drawn material.

(3) (U) Electronic or magnetic recording, punchcards, or paper tape.

(4) (U) Sound recordings.

(5) (U) Photographs.

(6) (U) Reproductions of the foregoing by whatever process.

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

b. (U) SIOP-ESI. Detailed TOP SECRET information and material of such an extremely sensitive nature that its

compromise would seriously degrade the effectiveness of the SIOP. Paragraph 4 below discusses specific kinds of information that are considered to be SIOP-ESI.

c. (U) JCS SIOP Documents. The JCS SIOP (Basic) and annexes, appendices, and tabs thereto, and associated source data.

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

e. (U) SIOP Briefings. Any briefing that includes detailed extracts of SIOP information derived from material described as SIOP material in subparagraphs 3a through 3d above and paragraph 4 below.

4. (U) Identification of SIOP-ESI

b. (U) The following JCS and JSTPS documents, because the level/amount of detail meets the criteria of subparagraph 4a above, are considered to be extremely sensitive and are

designated, in their entirety, as SIOP-ESI documents.

(1) (U) JSTPS AC&S Consequences of Execution with Tabs and SRF Damage Analysis.

(2) (U) Appendix III to SIOP Annex E (Coordinating Instructions).

(3) (U) SIOP Annex F (Strike Assignments and Force Timing) and Appendices I, II, III, IV, and V thereto.

(4) (U) JCS SIOP Summary, SIOP Annex F (Strike Assignments and Force Timing).

(5) (U) JCS SIOP Decision Handbook (Black Book).

(6) (U) JCS Emergency Action Procedures, Volumes II and IV.

(7) (U) SIOP Revision Reports.

(8) (U) Consolidated SIOP Analysis Document.

NOTE: Information extracted from these or any SIOP-ESI document is considered to be SIOP-ESI until such time as it has been reviewed by an individual who has been designated as an original TOP SECRET classification authority in accordance with DOD 5200.1-R and determined not to meet the criteria for SIOP-ESI stated in subparagraph 3b above.

c. (U) Reconnaissance data are not SIOP-ESI.

e. (U) Agencies responsible for SIOP wargaming and

exercises will consider the following:

(2) (U) The JSTPS and J-8 SIOP war game reports will be classified TOP SECRET and marked SIOP-ESI Category XX when they include information described in subparagraph

*SM-81-77, 1 Feb 77, "Basic Policy Guidance on Wargaming (U)"

4a above. Upon completion, war game reports involving the SIOP will be submitted to the Joint Chiefs of Staff for review and approval. An integral part of the approval procedures for such reports will be the review and approval of the classification assigned by the originator. Reports can be released in accordance with the provisions of JCS MOP 39, subparagraph 2a(2) as JCS papers or paragraph 6 of this directive as appropriate.

(3) (U) The use of SIOP-ESI data in the play of command post exercises and other war plan exercises is not authorized without the approval of the Director, Joint Staff. The Director for Operations, Joint Staff, shall review such requests and submit recommendations to the Director, Joint Staff, for approval.

f. (U) The listing delineated by subparagraphs 4a through 4e above is not to be construed as limiting or all inclusive, nor will the listing be maintained in a current status by changes to this directive.

5. (U) Security Classification and Marking

a. (U) All SIOP documents shall be classified and marked in accordance with DOD 5200.1-R. Documents containing

SIOP-ESI, as defined and described in paragraphs 3 and 4 above, shall bear additional markings, as prescribed herein.

b. (U) SIOP-ESI documents shall be classified TOP SECRET only. In order to permit immediate and positive identification of these documents, the indicator "SIOP-ESI Category XX" (i.e., 01-10) shall be prominently affixed to the front and back cover. This indicator shall also be applied to compilations of documents which, although not SIOP-ESI individually, may, in the aggregate, be so considered.

c. (U) Correspondence, reports, studies, messages, and any other media relaying SIOP-ESI shall include the following statement:

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

d. (U) Messages containing SIOP-ESI shall include the designator "SPECAT" and the indicator "SIOP-ESI Category XX" with the Category number spelled out, for example "SPECAT SIOP-ESI CATEGORY ONE," at the beginning of the message text immediately following the message

[redacted]

classification, in accordance with ACP 121 US Supp-1 (Series), followed by the statement in subparagraph 5c above. Supporting telecommunications centers will distribute SIOP-ESI messages based on the SIOP-ESI category number and access/distribution lists provided by recipients of SIOP-ESI message traffic.

* MJCS-273-83, 23 December 1983, "Guidance for the Sanitization and Distribution of SIOP Information to SACEUR and SACLANT"

[redacted]

[redacted]

f. (U) The SIOP-ESI indicator is NOT a separate security classification. This indicator is intended solely as a mechanism for identifying SIOP-extremely sensitive information that must be controlled in accordance with the special access procedures established by this directive. Care must be taken to ensure that the SIOP-ESI indicator is applied to documents only when the contents contain information of the type and quantity set forth in paragraphs 3 and 4 above. 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.

g. (U) SIOP documents, except those sanitized and authorized for release to NATO under the provisions of MJCS-273-83 shall be labeled "Not Releasable to Non-US Agencies Without Permission of the Originator."

6. (U) Distribution of SIOP Material and Extracts

a. (U) The Director for Operations, Joint Staff, OJCS, will review the requirements of all users of the JCS SIOP prior to the publication of each SIOP and report recommended distribution lists will be included in the promulgating directives for each SIOP.

(1) (U) Requests to change approved distribution lists will be submitted, with justification, to the Director for Operations, Joint Staff, OJCS. The Director for Operations, Joint Staff, will forward his consideration and recommendations to the Director, Joint Staff, who is authorized to approve/disapprove such requests. The Director of Strategic Target Planning (DSTP) will be notified of approved changes.

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

b. (U) 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 6a above, with the following stipulations:

(1) (U) Unless an exception is stated in the approved distribution lists, as provided in subparagraph 6a above, or amended under the provisions of subparagraph 6a(1) or 6a(2) above, JCS SIOP materials distributed by the DSTP will contain only those data necessary for the accomplishment of the assigned tasks, missions, and responsibilities of the addressee.

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

(a) (U) The DSTP will forward one copy of each required tape to The Joint Chiefs of Staff, Attention: J-3 Nuclear Warfare Status Branch (NWSB), and one copy to the Joint Coordination Center (JCC), Fort Ritchie, Maryland.

(b) (U) The Director for Operations, Joint Staff, will reproduce tapes, as required, to satisfy the approved requirements of users in the Washington, D.C., area. The JCC will use its copy of tapes provided to support JCS requirements delineated in JCS Pub 6, Volume II, Part 1.

(c) (U) Requests by approved users 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. (U) The DSTP is authorized to make distribution of JSTPS SIOP materials as follows:

(1) (U) All JSTPS SIOP material to:

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

(b) (U) OJCS.

(c) (U) Commands designated by the Joint Chiefs of Staff.

(2) (U) Distribution of JSTPS SIOP materials to the commands or agencies not covered in subparagraphs 6a through 6c(1) will be considered on a case-by-case basis. Requests will be submitted to the DSTP with sufficient justification to complete an appraisal. The DSTP may approve such requests as 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 action.

d. (U) Requests for copies of changes to the distribution schedule for the SIOP publication, "JSTPS Air Defenses Handbook," will be forwarded to the DIA Dissemination Center.

e. (U) The Chairman, Joint Chiefs of Staff, consulting the other Joint Chiefs of Staff, as appropriate, will approve/disapprove requests for SIOP documents from the White House and members of the Senate and House of Representatives.

f. (U) Requests for release of SIOP documents to foreign nationals will be submitted to the Director for Operations, Joint Staff, for review and recommendations to the Joint Chiefs of Staff, except as noted below.

(1) (U) The DSTP is authorized, in coordination with the SACEUR Senior Representative (SACEUR Rep) to the JSTPS, to disclose US classified information, relative to current and subsequent SIOPs, to SACEUR and the SACEUR Rep to JSTPS, pursuant to, and in accordance

with, the policies contained in NDP-1* and JAIEG Case N-15/75F.**

(2) (U) Similarly and in accordance with the same policies, the DSTP is authorized to disclose such SIOP information to SACLANT as is essential for adequate understanding and effective coordination of nuclear forces planning.

(3) (U) Procedures for handling US SIOP information within NATO is contained in Annex B to Attachment 1 of USSAN Instruction 1-69 (DOD 5700.55, Encl 2), "United States Implementation of NATO Security Procedures (U)"

g. (U) 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 accomplishment of assigned tasks, missions, and responsibilities. Reproduction of SIOP document extracts

---

* NDP-1, 9 Sep 81, "National Policy and Procedures for the Disclosure of Classified Military Information to Foreign Governments and International Organizations (National Disclosure Policy)"

** Joint Atomic Information Exchange Group (JAIEG) memorandum JAIEG Case N-15/75F, 10 Dec 75, "Authorization and Release Procedures for SIOP ATOMAL Information to NATO (U)"

shall, in every case, be on a rigidly discriminating basis and shall be controlled in accordance with applicable directives, including this directive.

h. (U) Special procedures for processing extracts from SIOP-ESI documents are as follows:

(1) (U) Release of SIOP data to foreign nationals is prohibited, except as authorized under the NATO Documents Program and as approved by the Joint Chiefs of Staff. The release of SIOP-ESI data to SACEUR/SACLANT is discussed in subparagraph 6f above.

(2) (U) 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 extracts, or portions reproduced, retain characteristics of the type and quantity delineated in paragraphs 3 and 4 above and should be identified as SIOP-ESI.

i. (U) Requests for JCS SIOP documents not covered by subparagraphs 6a through 6h above will be submitted, with justification, to the Director for Operations, Joint

Staff, who will forward the requests and his recommendations to the Director, Joint Staff. The Director, Joint Staff, consulting the Chairman, Joint Chiefs of Staff, as appropriate, will approve/disapprove these requests.

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

7. (U) Inventory and Sighting

a. (U) All SIOP materials defined and identified in paragraphs 3 and 4 above will be inventoried annually, as a minimum, or more frequently, as prescribed by the classified material control procedures of the appropriate Service, joint agency, or command, except as specifically provided in subparagraph 7b below.

b. (U) SIOP documents that are effective for a single SIOP revision cycle 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 security directives of the appropriate Service, joint agency, or unified and specified command. Command internal inspection procedures will be established to ensure rigid adherence to those procedures.

c. (U) The DSTP and other originating agencies shall annually, as of 30 September, provide holders a list of documents as follows:

(1) (U) 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).

(2) (U) All documents not covered in subparagraph 7c(1) above that contain SIOP-ESI.

Documents controlled in accordance with subparagraph 7b above will be exempt from this requirement.

d. (U) Upon receipt of this listing, holders shall verify the listing, sight listed documents, and certify the

sighting to the originator, who in turn will forward a consolidated sighting report of each such annual sighting to the Secretary, Joint Chiefs of Staff. Discrepancies, if any, shall be handled separately in accordance with paragraph 16 below and reported to the Director, Joint Staff.

e. (U) 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.

8. (U) Access Control

a. (U) Control of Access to Non-ESI SIOP Information. Access to SIOP information not identified as SIOP-ESI will be controlled 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. (U) Control of Access to SIOP-ESI Information. Access to SIOP information designated SIOP-ESI shall be subject to special control procedures. Services, joint agencies, and commands holding or authorized to hold SIOP-ESI data are requested to provide implementing instructions for the special control procedures outlined below.

3.b. (1) (U) Access to SIOP-ESI shall be highly restricted and granted on a selective and discriminating need-to-know basis in accordance with the guidance set forth in subparagraph 1c above. This is especially true of the SIOP decision and execution process.

(2) (U) There may be two types of access, PERMANENT and TEMPORARY.

(a) (U) Permanent Access. After considering the functions of a given duty position, the frequency of anticipated access, and the categories of SIOP-ESI access required, access granting authorities listed in subparagraph 8c below may establish permanent SIOP-ESI billets. Although a person assigned to a permanent SIOP-ESI billet needs no further authorization for access to the categories of SIOP-ESI specified for the billet, holders of SIOP-ESI information must still verify a valid need-to-know before releasing SIOP-ESI information. PERMANENT ACCESS BILLETS WILL BE REVIEWED AND REAPPROVED BY ACCESS-GRANTING AUTHORITIES LISTED IN SUBPARAGRAPH 8c BELOW NOT LATER THAN 31 DECEMBER IN EACH EVEN-NUMBERED YEAR.

(b) (U) Temporary Access. Access-granting authorities listed in subparagraph 8c below may grant approval for temporary access, up to 1 year, for personnel involved in briefing, studies, or other activities that have a projected end date.

8.b. (3) (U) Criteria for Access. Normally, military personnel and civilian personnel subject to the provisions of the personnel policies of the Office of Personnel Management (OPM) and Department of Defense may not be authorized permanent or temporary access to SIOP-ESI unless they meet the basic eligibility criteria set forth below:

(a) (U) The individual shall be a US citizen.

(b) (U) The individual shall have a final TOP SECRET clearance granted in accordance with the policy and criteria prescribed in DOD 5200.2-R.

(c) (U) The individual shall have been the subject of a completed special background investigation (SBI) that meets the criteria set forth in DOD 5200.2-R or other types of background investigations listed in DOD 5200.2-R that are equivalent to an SBI.

(U) Access for these individuals must be essential to the performance of their assigned duties and justified by their direct involvement in the review, development, maintenance, or implementation of the SIOP.

8.b. (4) (U) Those personnel previously granted access to SIOP-ESI based upon a background investigation (BI) that did not contain all of the elements of an SBI as set forth in DOD 5200.2-R shall be the subject of an SBI when a reinvestigation is requested for any reason, such as the development of adverse or questionable information or when a break in the period of access or Federal service exceeds 12 months.

(5) (U) Waiver of Access Criteria. When justified by compelling need:

(a) (U) A waiver of the basic eligibility requirement stated in subparagraph 8b(3)(b) above may be authorized by those access-granting authorities listed in subparagraphs 8c(1) through 8c(5) below for military personnel and civilian personnel subject to OPM and DOD personnel policies. This authority may not be delegated. Waivers should be approved only if the individual

concerned meets all the following criteria:

1. (U) Is being assigned to a position for which permanent access to SIOP-ESI is required.

2. (U) Already possesses an interim TOP SECRET clearance granted in accordance with the policy and criteria prescribed in DOD 5200.2-R.

3. (U) Has been administered a screening interview equivalent to that which is used to screen nominees for access to Sensitive Compartmented Information (SCI).

4. (U) Has an SBI initiated.

(b) (U) A waiver of the basic eligibility requirement stated in subparagraph 8b(3)(c) above may be authorized for military personnel and civilian personnel subject to OPM and DOD personnel policies. Such waivers must be approved by flag officer-level, access-granting authorities as authorized in subparagraphs 8c and 8d below. In cases where a flag officer is not routinely available to the unit and delays in processing will result in unacceptable operational delays in assigning personnel to SIOP-related duties, this authority may be delegated in writing to O-6 level operational unit commanders (i.e. Submarine

Squadron Commanders, Wing commanders, or equivalent). To be granted a waiver, the individual concerned must meet all of the following criteria:

1. (U) Is being assigned to a position for which permanent access to SIOP-ESI is required.

2. (U) Already possesses a final TOP SECRET clearance that was based on a standard BI that meets the investigative standards of paragraph 2, Appendix B, DOD 5200.2-R.

3. (U) Has an SBI initiated.

(c) (U) Approval of waivers for contractor personnel will be made only by the Chairman, Joint Chiefs of Staff.

(6) (U) Flag-officer level, access-granting authorities, as authorized in subparagraphs 8c and 8d below, may approve temporary access to SIOP-ESI information for briefings, working meetings, etc., for personnel who do not have a completed SBI as required by subparagraph 8b(2), provided all of the following criteria are met:

(a) (U) Access is essential to the performance of duty and the individual is directly involved in the review, development, maintenance, or implementation of the SIOP.

(b) (U) The individual meets the other basic eligibility criteria specified in subparagraphs 8b(3)(a) and 8b(3)(b) above.

(c) (U) The individual is subject to military, OPM, or DOD personnel policies.

(7) (U) Civilian personnel not subject to provisions of OPM or DOD personnel policies (i.e., contractor personnel) will not normally be granted access to SIOP-ESI. Such civilian personnel shall not be granted permanent access to SIOP-ESI but may be granted temporary access for periods not to exceed 1 year. Requests for temporary access for such civilian personnel shall be referred to the Director, Joint Staff, for appropriate action. Personnel in this category for whom temporary access is approved shall possess a final TOP SECRET clearance and shall meet the basic security eligibility requirements of DOD Instruction 5220.28.

(8) (U) Prior to being granted permanent access, all personnel will be briefed on the contents of this directive and any supplemental directives considered appropriate. Once granted, continued access by individuals will be based on security assurance measures established by the granting authority. Upon termination of access, appropriate debriefing must be

(U) accomplished. These briefings will emphasize 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 permanent SIOP-ESI access will execute an appropriate briefing/debriefing certificate, which will be maintained for a minimum of 1 year after the debriefing of an individual by the command granting access. These same requirements apply to personnel granted temporary access to SIOP-ESI, except as noted in subparagraph 12h below.

8b. (9) (U) OJCS, Services, unified and specified commands, Defense agencies, and JSTPS will:

(a) (U) Develop procedures to maintain, at an appropriate level, SIOP-ESI access listings of personnel categorized by military, DOD civilian, and industrial contractor personnel. These listings will be current as of the last day of each quarter and will contain, at a minimum: billet number, name, rank/grade, social security number (SSN), office/activity/unit designator, category of

(U) access, travel/duty restrictions (if applicable), and authorization document. Annex B is an example of a personnel access roster. Such lists shall be marked: "Subject to the Privacy Act of 1974 (5 USC, Section 552a)."

8b.(9) (b) (U) Be prepared to provide a numerical count of personnel having SIOP-ESI access within 5 working days after request, in the categories specified in subparagraph 8b(9)(a) above, to the Directorate for Information and Resource Management, OJCS, ATTN: Security Division. In any case, such a numerical report will be provided by 31 January of each calendar year. Close-out date for the report will be 31 December of the preceding year. To preclude duplication in recording, the following instructions apply:

1. (U) Services will record all personnel not assigned to the OJCS, Defense agencies, or to the staffs of unified and specified commands.

2. (U) Unified commands will record assigned headquarters personnel only.

3. (U) US Element NORAD and the specified

(U) commands (US Space Command, MAC, and SAC) will divide personnel into two categories: headquarters and all others.

4. (U) JSTPS will record single-status and Scientific Advisory Group personnel.

5. (U) Guidance for recording of personnel in OSD, OJCS, non-DOD agencies, and the Defense agencies will be provided by a Joint Administrative Instruction.

3.b. (10) (U) The categories of SIOP-ESI listed in Annex A shall be used for access control.

(11) (U) Internal inspection procedures will give special and continuing attention to safeguards for SIOP-ESI.

3. c. (U) Authority to establish billets and grant access to SIOP-ESI is delegated to:

(1) (U) The Director, Joint Staff, for civilian personnel of the White House, members of the Senate and House of Representatives, and their staffs. Requests must be submitted to the Director a minimum of 7 work days prior to the date the access is required.

(2) (U) The Director, Joint Staff, for the Joint Chiefs

(U) of Staff, members of the OJCS, other Joint Staff agencies, Defense agencies, military personnel assigned to the White House and National Security Council Staffs, OSD, civilian personnel not subject to the provisions of OPM or DOD policies (i.e., contractor personnel), and others as may be authorized by the Joint Chiefs of Staff. These requests must be submitted to the Director for Operations, Joint Staff, a minimum of 7 work days prior to the date the access is required.

B.C. (3) (U) The Chief of Staff, US Army; the Chief of Naval Operations; the Chief of Staff, US Air Force; and the Commandant of the Marine Corps for members of their respective Services and departmental staffs, and personnel assigned to the offices of the Secretaries of the Military Departments.

(4) (U) Commanders of unified and specified commands having responsibility for planning, preparation, coordination, and execution of the SIOP, for members of their staffs and subordinate command, and military personnel assigned to agencies directly supporting the CINC's SIOP-related missions.

(5) (U) The Director of Strategic Target Planning for members of the JSTPS.

8. d. (U) Access to SIOP data, including SIOP-ESI, normally shall not be given to foreign nationals, including members of NATO, except as authorized by the Joint Chiefs of Staff. Procedures for access to US SIOP data released to NATO in accordance with subparagraph 6f above are contained in Annex B to Attachment 1 of USSAN Instruction 1069 (DOD 5100.55, Enclosure 2). Access to SIOP-ESI data by US personnel assigned to NATO military organizations/ agencies normally will be restricted to those sanitized data allowed to be provided under the provisions of MJCS 273-83. US personnel assigned to NATO military organizations/agencies who are also members of USEUCOM or LANTCOM may be authorized access to other SIOP-ESI by USCINCEUR or USCINCLANT. US personnel assigned to NATO military organizations/agencies who are not also members of USEUCOM or LANTCOM may be authorized access to other SIOP-ESI by USCINCEUR.

e. (U) The authority to grant access delegated in subparagraph 8c above may be further delegated to

(U) appropriate subordinates. Such further delegation shall be held at the highest rank and restricted to the minimum number of appropriately cleared individuals, consistent with operational requirements.

8. f. (U) Requests for SIOP-ESI access not covered above will be submitted to the Director for Operations, Joint Staff, who will forward the request and his recommendations to the Director, Joint Staff. The Director, Joint Staff, consulting the Chairman, Joint Chiefs Staff, as appropriate, will approve/disapprove these requests.

9. (U) Travel: Persons granted access to SIOP-ESI incur a special security obligation and must be aware of the risks associated with travel to or through hostile countries. SIOP-ESI-cleared personnel must be warned of the risks associated with capture, interrogations, harassment, entrapment, or exploitation by hostile nations or groups. Hazardous activities comprise assignments, visits to, travel through, and use of vessels owned or controlled by hostile countries, as well as assignment or travel in combat zones or other areas where hostilities or terrorist activities are taking place, duties behind hostile lines, and duties or

travel in isolated or exposed areas where individuals cannot reasonably be protected against hostile action. Individuals also must be advised of the potential for terrorism and the active and passive measures to avoid becoming a target or inadvertent victim of a terrorist act.

7. a. (U) Official Travel: All SIOP-ESI cleared personnel performing official travel outside the United States must receive a security/anti-terrorist briefing and or risk of capture briefing.

b. (U) Unofficial Travel: All SIOP-ESI-cleared personnel performing unofficial travel to or through hostile countries must comply with the provisions below. Failure to comply with these provisions may result in the withdrawal of approval for continued access to SIOP-ESI.

(1) (U) Give advance notice of such planned travel to local security officer.

(2) (U) Obtain anti-terrorism briefing from the security officer prior to performing such travel.

(3) (U) Immediately contact the nearest US Consul, Attache, or Embassy Regional Security Officer or Post Duty Officer if detained or subjected to significant

(U) harassment or provocation while traveling.

(4) (U) Report to the specified official upon return from travel any unusual incidents, including incidents of potential security concern, encountered during such travel.

c. (U) SIOP-cleared individuals whose access is being terminated will be officially reminded of their continuing obligation to protect SIOP-ESI and will be informed of the risks associated with hazardous activities. After SIOP-ESI access is terminated, provisions of paragraph b no longer apply.

10. (U) Visits Requiring Access to SIOP-ESI. Prior to visits by personnel who will require access to SIOP-ESI data, the headquarters to be visited 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.

11. (U) Visits to JSTPS

a. (U) Requests for visits to JSTPS by civilian personnel of the White House, members of Congress, and Congressional Staff members will be submitted to and be reviewed and approved by the Director, Joint Staff.

(U) All other requests for visits, except working level, will be sent to the Director for Operations, Joint Staff, for approval. The Director for Operations, Joint Staff, will approve/disapprove or forward as appropriate to the Director, Joint Staff, visit requests for individuals possessing appropriate clearances and a valid need-to-know.

b. (U) All requests for visits should be submitted a minimum of 7 working days prior to the visit. The timely submission of requests is necessary to provide sufficient time for adequate staffing within the Joint Staff. Requests should contain a detailed justification for the visit, type of information/briefing requested, point of contact at JSTPS, and recommendations on the appropriate type/classification of briefing to be given.

c. (U) Members of the Service or CINC staffs who are directly involved with SIOP development/support/implementation should contact the Joint Secretariat, JSTPS, directly for working-level visit approval. Other individuals from outside agencies possessing appropriate SIOP clearances who wish to visit JSTPS for working-level

meetings need only to notify J-3, Strategic Operations Division, of visit intentions.

12. (U) SIOP Briefings

a. (U) SIOP briefings may be given to those personnel under the control or military jurisdiction of the Joint Chiefs of Staff or of the Chief of Staff, US Army; the Chief of Naval Operations; the Chief of Staff, US Air Force; or the Commandant of the Marine Corps. Access for these individuals must be essential to the performance of their assigned duties and justified by their direct involvement in the review, development, maintenance, or implementation of the SIOP. Personnel who do not fall into this category require specific approval as indicated below.

b. (U) The SIOP shall not be used as a vehicle of instruction at joint or Service schools or other similar instructional institutions. Special SIOP briefings given to joint or Service schools shall not contain SIOP-ESI and will be classified TOP SECRET. Attendance of foreign personnel at these briefings is prohibited. SIOP briefings for the joint colleges may be scheduled and

(U) conducted on a mutually acceptable basis through direct coordination between DSTP and the cognizant commandant. The Chiefs of the Services will provide approval of such requests from Service schools over which they exercise cognizance.

12. c. (U) SIOP briefings normally shall not be given to foreign nationals, including members of NATO. The Director, Joint Staff, may approve briefings for military members of NATO, provided the briefing is sanitized in accordance with MJCS 273-83. Other requests for SIOP briefings for foreign nationals may be approved by the Joint Chiefs of Staff.

d. (U) The Chairman, Joint Chiefs of Staff, consulting the other Joint Chiefs of Staff, as appropriate, will approve/disapprove requests for SIOP briefings for civilian personnel of the White House and members of the Senate and House of Representatives.

e. (U) Briefings on the SIOP Revision Report and War Games Report or briefings based on these reports may not be given except as provided in the foregoing subparagraphs or as approved in accordance with the provisions of JCS MOP 39 and this directive, as appropriate.

12. f. (U) Requests for SIOP briefings not covered above will be submitted to the Director for Operations, Joint Staff, who will forward the request and his recommendations to the Director, Joint Staff. The Director, Joint Staff, consulting the Chairman, Joint Chiefs of Staff, as appropriate, will approve/disapprove these requests.

g. (U) An approved attendance list will be prepared to control entry to SIOP briefings containing SIOP-ESI.

h. (U) Persons attending SIOP briefings containing SIOP-ESI must meet the criteria for eligibility for access to SIOP-ESI as specified in subparagraphs 8b(3), (5), and (6) above. Persons granted temporary access to SIOP-ESI to attend a briefing need not complete a briefing/debriefing certificate as required by subparagraph 8b(8) above, provided the briefing contains appropriate oral and visual warning regarding the sensitivity of the data in the briefing.

13. (U) Training. It is recognized that operational commands must conduct SIOP training in order to accomplish their strategic operational missions effectively. In this context, SIOP indoctrination is required by many operational personnel.

The policy guidelines for SIOP indoctrination are as follows:

a. (U) Access shall be strictly controlled on a need-to-know basis.

b. (U) Attendance at indoctrination briefings will be restricted to those personnel actually assigned to or en route to operational billets that require access to SIOP information.

c. (U) Indoctrination courses may be conducted at operational commands that hold SIOP documents or at those appropriate training facilities that are under the direct supervision/control of the component commanders of the several unified and specified commands. Curricula and associated material shall be approved by these commanders.

d. (U) The SIOP may be used as a vehicle of instruction provided that the precise area of indoctrination is correlated with billet requirements.

14. (U) Telecommunications System Processing of SIOP-ESI

a. (U) Special Category (SPECAT) SIOP-ESI Special Handling Designator. To preclude delivery of SIOP-ESI message traffic to a SPECAT terminal that is not specifically approved to receive SIOP-ESI messages, communications

systems shall apply a special handling designator in the security field of the communications heading of all electrically transmitted SIOP-ESI messages to enable automatic switch comparison of the SIOP-ESI designator against the destination security level authorization. A designator indicating SIOP-ESI has been established and is promulgated in ACP 121 US Supp-1 (Series). Message originators must include this designator in all SIOP-ESI messages (see paragraph 5d). Commanders having responsibility for terminals authorized to receive SPECAT (less SIOP-ESI) messages will ensure that adequate debriefing procedures are established in the event of inadvertent delivery of a SIOP-ESI message to the terminal affected.

b. (U) Connection of an ADP System that Processes SIOP-ESI to a Telecommunications System. An ADP system processing SIOP-ESI in accordance with the provisions of Annex C may be connected to telecommunications systems such as AUTODIN or other nondedicated telecommunications systems only when approved by the Joint Chiefs of Staff. Requests for approval to make such connections should be forwarded to

[redacted]

the Director for Operations, Joint Staff, OJCS. Requests should address as a minimum:

(1) (U) The procedures to be followed to ensure the safeguarding of SIOP-ESI.

(2) (U) Interface design features that will ensure the safeguarding of SIOP-ESI.

(3) (U) The results of evaluations of the interface design.

(4) (U) The results of tests of the interface.

(5) (U) Security findings and remaining vulnerabilities of security concern.

(6) (U) How reapproval will be handled if significant interface redesign is required in the future.

(7) (U) Conclusions and recommendations regarding security and the use of the interface to interconnect the ADP system to a telecommunications system.

c. (U) Accreditation of Telecommunications Systems To Process SIOP-ESI.

(1) (U) Telecommunications systems such as AUTODIN may process and transmit SIOP-ESI data only after the system has been accredited by the Joint Chiefs of

Staff. Requests to accredit telecommunications systems to handle SIOP-ESI should be addressed to the Director for Operations, Joint Staff, OJCS. Requests for accreditation should include details regarding implementation of a security certification/accreditation plan and adhere to guidance outlined in: Defense Intelligence Agency Manuals (DIAM) 50-3, "Physical Security Standards for Sensitive Compartmented Information Facilities"; DIAM 50-4, "Security of Compartmented Computer Operations;" and DIAM 50-5, "Sensitive Compartmented Information Contractor Administration Security." Upon development of the Security Certification/Accreditation Plan, it should be submitted to the Director for Operations, Joint Staff, OJCS, for review and comment by OJCS personnel. The plan will outline the procedures to be followed to ensure the safeguarding of SIOP-ESI. The plan should address how information security will be achieved at the outset and how reaccreditation will be achieved whenever significant portions of system hardware or software are changed. The plan will also address the

protective features outlined in subparagraph 5g(9) of Annex C. A suggested outline of the plan's contents is as follows:

(a) (U) Introduction - includes brief description of system, purpose, and scope of plan.

(b) (U) Responsibilities - identifies agencies participating in certification and accreditation activity and their roles and responsibilities.

(c) (U) System Overview - includes a functional description of the system with appropriate definitions of system components, interfaces, etc. Additionally, should address security concept, operational concept, maintenance concept, and procurement process.

(d) (U) Security Problem - identifies potential system security weaknesses.

(e) (U) Security Approach - describes computer security features and communications security considerations.

(f) Security Activities - describes actions and features implemented to ensure security.

(g) (U) Description of the Accommodation Package - describes documents comprising recommendation package to include the security certification evaluation.

(2) (U) Upon completion of system security activities, the final accreditation/certification request should be submitted for approval. The request should be accompanied by a security certification evaluation which addresses the following as a minimum:

(a) (U) System security design and mode of operation.

(b) (U) System security tests conducted.

(c) (U) Security findings and remaining vulnerabilities.

(d) (U) Conclusions and recommendations regarding security.

15. (U) Transportation of SIOP-ESI Material

a. (U) SIOP-ESI material not electrically transmitted via secured circuits shall be dispatched only by courier. The Armed Forces Courier Service (ARFCOS) should be utilized to the maximum extent feasible. Special handling

instructions within the ARFCOS system will be as prescribed by the Director, ARFCOS. Dispatching officials will designate the material SIOP-ESI when entering it into the ARFCOS system and will have the following statement affixed to the outside of the package or container in addition to the normal addresses and markings:

"RESTRICTED HANDLING REQUIRED"

(1) (U) Air transportation of this package will be in the following priority: military aircraft, regularly scheduled US commercial cargo aircraft, government-chartered commercial aircraft, regularly scheduled US commercial passenger aircraft (ARFCOS only).

(2) (U) TWO COURIERS ARE REQUIRED BETWEEN US MILITARY INSTALLATIONS/FACILITIES. ONE COURIER CAN BE USED DURING FLIGHT SO LONG AS TWO COURIERS DELIVER AND PICK UP MATERIAL AT PLANESIDE OFF MILITARY BASES.

(3) (U) 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.

(4) (U) COURIERS AND GUARDS MUST POSSESS TOP SECRET CLEARANCES BASED ON A COMPLETED BACKGROUND INVESTIGATION.

b. (U) Commanders supporting ARFCOS are responsible for providing arrangements for the transportation of SIOP-ESI material by military air. Priority will be provided to the shipment of SIOP-ESI material to meet the deadline delivery date.

c. (U) When not transported via ARFCOS, SIOP-ESI material being transported or processed outside military installations/facilities will be accompanied by two appropriately cleared couriers (in accordance with the handling restrictions delineated in subparagraph 15b above) assigned the primary responsibility for surveillance and security of the material. When utilizing authorized air transportation, as delineated in subparagraph 15c(1) and (2) below, 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 to maintain surveillance until the aircraft is airborne.

(1) (U) The following types of air transportation are authorized for movement of SIOP-ESI material:

(a) (U) Military aircraft.

(b) (U) US contract commercial aircraft when the manifest is under US military control.

(c) (U) US commercial nonpassenger cargo aircraft.

(2) (U) SIOP-ESI material WILL NOT be transported by any of the following means:

(a) (U) Commercial passenger aircraft (except for ARFCOS, as described above).

(b) (U) Department of State Diplomatic Courier Service.

(c) (U) Foreign or combined courier service (such as NATO).

(3) (U) Ground transportation of SIOP-ESI material will be, in order of priority, by US Government sedan, US Government bus, US Government chartered bus, commercial transportation.

16. (U) Actions in Case of Possible or Actual Compromise. The Joint Chiefs of Staff and the DSTP shall be informed by the most expeditious means available, consistent with security requirements, of any compromise or suspected compromise of any portion of any SIOP material. Such reports

will include specific identification of the document, whether or not SIOP-ESI is involved, and an opinion as to probability or possibility of compromise. The DSTP will recommend appropriate actions required with regard to modification of the plan or related procedures as a result of the actual or possible compromise for consideration by the Joint Chiefs of Staff. The provisions of Chapter VI, DOD 5200.1-R also apply.

17. (U) Machine Reproduction of SIOP-ESI. The capability of data reproduction by electronic means presents a special need for attention to security precautions where such means are used in processing classified material. The 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 that possess the means for 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 accounting for and controlling access to SIOP-ESI. In every case, such means shall ensure that numbers of copies, extracts, or information derivatives are limited to those required to serve valid needs. Access to documents and

[redacted]

reproduction equipment shall be limited to the minimum numbers of properly cleared personnel. Accountability systems shall ensure that all documents produced by electronic means, including ADP systems, are properly identified, marked, distributed, and safeguarded.

18. (U) ADP

a. (U) Safeguarding SIOP-ESI in an ADP environment requires special precautions achieved by using a combination of conventional security procedures and new automated techniques. Annex C delineates the minimum security requirements for ADP systems. ADP systems security should include the following:

(1) (U) ADP hardware features.

(2) (U) ADP software features.

(3) (U) Communications security.

(4) (U) Emanations security.

(5) (U) Physical security measures.

(6) (U) Personnel security measures.

(7) (U) Procedural safeguards (management, administrative, and operational procedures).

b. (U) Recording media used to store or process SIOP-ESI must retain the TOP SECRET classification and be

controlled as SIOP-ESI until one of the declassification procedures delineated in Annex D is carried out. The declassification procedures in Annex D apply to release of the recording media for maintenance of equipment, return of parts to contractor, and release of computers to contractors.

c. (U) The provisions of Annexes C and D may differ from the requirements of communications security (COMSEC) materials and information. Refer to appropriate COMSEC directives for security requirements and declassification procedures for COMSEC items when COMSEC and SIOP-ESI are being processed.

19. (U) Destruction. As a matter of policy, in order to ensure 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 and witnessing the destruction of material containing SIOP-ESI must have authorization for access to the category(ies) of SIOP-ESI contained in the material being destroyed.

[redacted]

ANNEX A

CATEGORIES OF SIOP-EXTREMELY SENSITIVE INFORMATION (SIOP-ESI) (U)

1. (U) Scrupulous discrimination must be used when granting access to Categories 01, 02, 04, 09, and 10. Use of one, or more, of Category 03, 05, 06, 07, or 08 is preferable to granting access to Category 01, 02, 04, 09, or 10. Access categories are not meant to be a list of greater or lesser sensitivity or exposure; they are meant to be subject restrictive. The categories are intended to limit access to the specific area of duty responsibility. Personnel granted permanent or temporary access to SIOP-ESI need no further authorization for access to the specific categories of SIOP-ESI specified for a billet; however, holders of SIOP-ESI information must still verify a valid need-to-know before releasing SIOP-ESI.

2. (U) Category numbers are unclassified. When associated with their definitions, they are CONFIDENTIAL.

CLASSIFIED BY DIRECTOR, J-3
DECLASSIFY ON OADR

[redacted]

ANNEX B

EXAMPLES OF SIOP-EXTREMELY SENSITIVE INFORMATION ACCESS ROSTERS

SIOP-ESI PERMANENT ACCESS ROSTER FOR (AGENCY)
(Subject to Privacy Act of 1974)(5 USC 552a))

Billet No/SSN	Title/Name	Rank/Grade	Service	SIOP Categories	Authorization Document
XY000001 123-45-6789	Dir, XYZ Staff Doe, John Q.	GS-06	Civ	02 03 05 07	DJSM 1234-40, 28 Sep 1940
XY000002 987-65-4321	Dir, ABC Staff Tree, Tall F.	LTC	USA	01 04 09	J3M 4567-45 14 Jan 1945

SIOP-ESI TEMPORARY ACCESS ROSTER FOR (AGENCY)
(Subject to Privacy Act of 1974)(5 USC 552a))

Company	Name	SSN	SIOP Categories	Authorization Document	Expiration Date
ADPS	Doe, John Q.	123-45-6789	02 03 05 07	DJSM 1234-40 28 Sep 1940	28 Sep 1941
AIS	Tree, Tall F.	987-65-4321	01 04	J3M 4567-45 14 Jan 1945	14 Jul 1945

* Category of access does not automatically determine need for travel/duty restriction. Determination must be made on case-by-case basis, depending on an individual's frequency/degree of access (see Annex E).

ANNEX C

MINIMUM SECURITY REQUIREMENTS FOR AUTOMATIC DATA PROCESSING SYSTEMS PROCESSING SIOP-EXTREMELY SENSITIVE INFORMATION (SIOP-ESI)

1. An Automatic Data Processing System (ADPS) is defined in DOD Directive 7920.1 as an interacting assembly of procedures, processes, methods, personnel, communications, and automatic data processing equipment to perform a series of data processing operations--a combination of automatic data processing resources and automated data systems. This definition is interpreted as including all peripheral devices used in performing data processing operations located within or remote to the central ADPS facility.

2. Authorities listed in subparagraphs 8c(1) through 8c(5) of the Appendix may approve the processing of data containing SIOP-ESI on an ADPS when operations are controlled as indicated below.

a. The preferred mode of operation is the Dedicated Security Mode as defined by paragraph 1-211, DOD 5200.28-M.

"All portions of this annex are UNCLASSIFIED"

b. In exceptional cases where the Dedicated Security Mode of Operations is not reasonably practicable, the System High Security Mode as defined by paragraph 1-227, DOD 5200.28-M may be used.

c. Regardless of whether the Dedicated Security Mode or the System High Security Mode is used, the ADPS including all of its connected peripheral devices and remote terminals, must be dedicated to the processing of SIOP-related and/or SIOP-ESI and be under the exclusive control of persons who are authorized access to SIOP-ESI.

d. All peripheral devices in areas not manned by personnel cleared for SIOP-ESI must be disconnected from the ADPS by either a manually thrown switch or by unplugging at a patch panel.

3. Efficient utilization of the ADPS is important but should not be used as a criterion for determining the need-to-know and access to SIOP-ESI.

4. Appropriate procedures will be established for debriefing persons not authorized access to SIOP-ESI should inadvertent disclosures of SIOP-ESI occur while processing under the modes of operation delineated in subparagraphs 2a and 2b above. Paragraph 16 of the Appendix will only apply in the

case of possible or actual compromise.

5. Requirements for ADPS containing SIOP-ESI are stated below:

a. ADPS Security Officer. A Security Officer properly cleared for access to SIOP-ESI will be appointed for each ADPS that will process data bases containing SIOP-ESI. The designated approving authority (DAA) for commands having operational responsibility for the ADPS will ensure such appointment. The responsibilities of the ADPS Security Officer will include:

(1) Ensuring that each site has written procedures that outline operator actions required for known fault/security events. These procedures should include operating restrictions, if required, and delineate reporting and investigation requirements.

(2) Ensuring continued compliance with all requirements for processing and storing data containing SIOP-ESI including the requirements of this directive.

(3) Ensuring that security deficiencies that occur in the operation of the ADPS are expeditiously reported to the command DAA.

(4) Curtailing system processing, pending investigation

when continued operation could lead to compromise.

(5) Conducting a review of audit trails for security-related activities.

Command DAAs will immediately forward to the Director for Operations, Joint Staff, all security deficiencies they consider significant and will forward annual certification that the system complies with all requirements for processing and storing data containing SIOP-ESI. If systems do not comply with all requirements for processing and storing data containing SIOP-ESI, command DAAs will list deficiencies and proposed corrective actions in their annual reports.

b. Personnel Security and Access Control Measures

(1) Unescorted access to any portion of the ADPS processing SIOP-ESI will be limited to personnel authorized access to SIOP-ESI. All other personnel requiring access to such areas must be escorted by personnel authorized access to SIOP-ESI. The area will be inspected prior to such visits to ensure that no SIOP-ESI is visible. Escorts are responsible for ensuring that no disclosure of SIOP-ESI occurs.

(2) A personnel access control system will be

maintained at the central site and at the remote terminal areas to permit ready identification of those persons authorized access to the ADPS.

(3) A record will be maintained of all persons that are escorted into the areas identified in subparagraph 5b(1) above. The ADPS Security Officer will ensure that this record is retained for a minimum of 12 months from the date of the last entry in the log.

c. Physical Security Protection. Physical security will be in accordance with DOD Directive 5200.1, DOD Regulation 5200.1-R, DOD Directive 5200.28, and DOD Manual 5200.28-M.

d. Communications Links. All communications links will be secured in accordance with DOD Directive C-5200.5 for the classification of information transmitted. When connection is approved by the Joint Chiefs of Staff (see subparagraph 14b of the Appendix) and is connected in accordance with subparagraph 5g(9) of this annex, and ADPS that processes data containing SIOP-ESI may be conducted to nondedicated telecommunications systems that have been accredited for the transmission of SIOP-ESI (see subparagraph 14c of the Appendix).

e. Emanations Security. All equipment associated with an

ADPS, including remote terminals, modems, multiplexers, crypto devices, patch panel, etc., that is used to process data containing SIOP-ESI must meet the objectives of DOD Directive S-5200.19. ADPS equipment processing SIOP-ESI, and not previously TEMPEST tested, will be tested and evaluated at the earliest possible date. If the ADPS equipment is found to be deficient, appropriate counter-measures will be implemented immediately and a plan will be developed to phase in equipment that will meet TEMPEST standards at the earliest possible date.

f. Security Classification Responsibilities. The user is responsible for verifying that no extraneous data are included in his output product and that the security classification indicated on the product is consistent with the data contained therein. He is also responsible for reporting all discrepancies.

g. Software/Hardware Controls. The following features will be implemented in each ADPS that is to be used to process data containing SIOP-ESI. Special controls will be implemented governing access to, and modifications of, these features. Where implementation of the following features is not feasible because of equipment configuration

or other legitimate reason, other compensating controls will be developed and approved for implementation by command DAA.

(1) Security Markings and Special Access Labels

(a) All printed material produced from ADPS containing SIOP-ESI and operating in accordance with paragraph 2 above will have machine-produced security markings and special access labels at the top and bottom of each page equivalent to the highest classification of the data contained in the product. In addition, the front covers will be marked with a SAFEGUARD statement (see Tab).

(b) Removable storage media; i.e., tapes, card decks, discs, and similar devices used to store data bases containing SIOP-ESI will contain TOP SECRET classification markings in accordance with DOD 5200.1-R, with the SIOP-ESI label appropriately affixed to the storage media. These security markings/labels will be retained until the device is declassified by approved procedures described in Annex D.

(2) User Identification/Authentication. Operation of the ADPS will include a mechanism that identifies and authenticates user personnel accessing it remotely. This mechanism will consist of software and/or hardware devices, manual control procedures at terminal sites, or other appropriate measures designed to validate the identity and access authority of system users.

(3) Memory Protection. System hardware and software features will exercise control over the addresses to which a user program has access.

(4) Separation of User/Executive Modes of Operation. The user and executive modes of an ADPS will be separated so that a program operating in user mode is prevented from performing unauthorized executive functions. Controls will be implemented to maintain continued separation of these modes.

(5) Memory Residue Clean-Out. Measures will be implemented to ensure that memory residue from terminated user programs is made inaccessible to other users. This will be accomplished as required by DOD 5200.28-M.

(6) Access Control. Effective controls will be implemented to limit user and terminal access to authorized information and programs as well as to control read and/or write capability. In addition to software, positive disconnection of hardware can also be used to control remote terminals. Each individual user of the system will have a unique unclassified user identification (ID) assigned. Access attempts from remote terminals will be limited to TWO attempts, after which the terminal will automatically be locked-out and the ADP Security Officer notified.

(7) Audit Trail Capability. Each ADPS will produce an audit trail as defined in DOD 5200.28-M containing sufficient information to permit a regular security review of system activity. Audit trail information will be controlled closely by the ADPS Security Officer and, since SIOP-ESI may be contained therein, should be marked and handled as SIOP-ESI until actual classification is determined.

(8) Changing into and out of SIOP-ESI Operations

(a) Before starting to process SIOP-ESI, the area

must be cleared of all unauthorized personnel and unauthorized peripheral devices must be disconnected. The point of disconnect must be under the control of personnel cleared for SIOP-ESI.

(b) After processing is completed, all removable storage media containing files and/or programs used during SIOP-ESI processing will be disconnected from the ADPS. If any SIOP-related files or programs were used and those files or programs are to be used in a non-SIOP-ESI processing environment, they must contain no SIOP-ESI or must be purged of any SIOP-ESI prior to such use. All nonremovable storage media and memory must be cleared of all SIOP-ESI. Erase and overwrite procedures delineated in Annex D apply if the ADPS is to be used in an unclassified mode.

(9) Communication Connectivity. If an ADPS that has been approved for processing SIOP-ESI is also approved for interface with an external telecommunications system, such as AUTODIN or other telecommunication systems, while processing SIOP-ESI, the following

additional protective features are required:

(a) All interfacing telecommunications channels will be protected by cryptographic equipment or approved protective wireline distribution system.

(b) Specific measures will be implemented to prevent remote programming of the ADPS via external telecommunications.

(c) Procedures will be implemented to protect against accidental spillage of the data base into external telecommunications.

(d) Procedures will be implemented for fault monitoring that will detect malfunctions and halt processing when such malfunctions degrade any protective feature.

(e) Authentication procedures will be employed when telecommunications are used for ADPS-to-ADPS operations and/or ADPS-to-Remote user operations to limit access to SIOP-ESI to those network terminals and ADPS authorized to handle the data.

h. Individual Security Responsibilities. All users of the ADPS will be briefed on the need for exercising sound

security practices in protecting the information stored, processed, and produced by the system. Users will be informed when the system is operating in accordance with paragraph 2 above. Receipt of any information not specifically requested and of an unknown source shall be reported immediately to the ADPS Security Officer.

i. Civilian Contractor ADP Maintenance Personnel. These personnel will not be granted access to computer centers where data containing SIOP-ESI is resident in the ADPS unless the provisions of subparagraphs 8b(7) and 8b(8) of the Appendix have been met.

j. Reports. When an inadvertent disclosure occurs involving an ADPS processing SIOP-ESI, the report required in paragraph 16 of the Appendix shall be expanded to include at a minimum:

(1) An abstract of the problem.

(2) The type and source (e.g., Annex F data from disc pack) of the data involved.

(3) The ADP equipment involved.

(4) The number of people inadvertently exposed to the data.

(5) An assessment of the risk of compromise of the data.

(6) Immediate action taken (e.g., system processing curtailed as authorized by subparagraph 5a above).

(7) Steps being taken to preclude a recurrence of the problem.

(8) Comments and recommendations regarding problems considered to be of concern to the SIOP community and not restricted to the reporting site. This information is essential in order to determine the disclosure risk level of SIOP-ESI throughout the SIOP community and to determine whether similar problems exist on a community-wide basis. Reports will be submitted on an "as-occurring" basis.

k. Exceptions. Requests for exceptions to the security measures stated above will be submitted to the Director, Joint Staff.

TAB TO ANNEX C

SAFEGUARD STATEMENT

SAFEGUARD

This ADP product was produced during a TOP SECRET SIOP-ESI period. Handle as TOP SECRET SIOP-ESI until this statement has been signed by an individual who is designated to determine that the security classification of this document is appropriately marked and that the document can assume the handling requirements for that classification. Report any unusual or unrequested output discrepancies immediately to: _____
Printed/Typed Name

Signature: _____, Date: _____

ADPS Security Officer

Room Number _____

Phone Number _____

This ADP product has been reviewed by the undersigned. The correct security classification of this document is _____.

Signature: _____, Date: _____

_____

Printed/Typed Name

Room Number _____

Phone Number _____

ANNEX D

DECLASSIFICATION PROCEDURES FOR ADP MEDIA-STORING SIOP-EXTREMELY SENSITIVE INFORMATION (SIOP-ESI) (U)

1. General. Safeguarding classified information in a computer or computer system requires special precautions because of the types of storage media and devices (magnetic drums, discs, disc packs, and tapes) used to store, record, or manipulate data that must be protected by appropriate classification and security controls until procedures in paragraph 2 below are carried out.

2. Declassification. The eventual temporary or outright release of the storage device or a system including storage media should be anticipated. Procedures to be used in the event a decision is made to release or deploy the storage media are as follows:

a. Magnetic Tapes. Tapes used to store magnetically recorded digital data may be degaussed and declassified by erasing with approved tape degaussers that meet technical specifications promulgated by the Department of Defense.

b. Magnetic Discs, Dics Packs, Drums, and Other Similar Rigid Magnetic Storage Devices (e.g., Core Memory).

"All portions of this annex are UNCLASSIFIED"

TOP SECRET information, except that the state must be changed at least 999 times.

(2) Plated Wire Memory. Plated wire memory used to continuously store classified information undisturbed more than 8 hours may not be declassified. Such media will continue to retain their classification until physically destroyed. If the classified information is stored less than 8 hours and unclassified data is later stored for at least an equal time, the memory may be declassified according to the procedures for magnetic ferrite core memory.

(3) Semiconductor Memory. Semiconductor memory may be declassified according to the procedures for magnetic ferrite core, except for volatile semiconductor memory. Volatile semiconductor memory may be declassified by setting "0" or "1" in all memory locations.

e. Magnetic Storage Media Used To Store Analog, Video, or Similar Nondigital Information. Magnetic tape used to record analog, video, or similar types of nondigital information may be declassified by degaussing as in subparagraph 2a above. There is no approved overwrite

method for declassifying rigid magnetic storage media used for nondigital information; specific guidance may be obtained as stated in paragraph 5 below. In the case of a failure of the tape degausser or in the absence of an approved overwrite method for rigid surfaces, a magnet may be used, as described in subparagraph 2c above.

3. Disposition Approval. With the specific approval in each case of the designated (systems) approving authority (DAA) within the DOD component that is responsible for the security features of the ADPS, storage media treated as above may be handled as unclassified and released as necessary.

4. Records. A record of the procedures used to declassify each storage media device shall be maintained for a period of 2 years after disposition of the media or device.

5. Specific Guidance

a. Guidance for eradication of storage media not covered above may be obtained by submission of all pertinent details to the Director, Joint Staff, for consideration on a case-by-case basis.

b. In the absence of eradication by approved equipment or procedures or at the direction of the designated official

responsible for the security features of the ADPS, magnetic information storage media will be safeguarded in the manner prescribed for the highest classification ever recorded thereon until it is destroyed.

ANNEX E

SECURITY POLICY CONCERNING TRAVEL AND ASSIGNMENT OF PERSONNEL WITH ACCESS TO SIOP-EXTREMELY SENSITIVE INFORMATION (SIOP-ESI) (U)

2. (U) Purpose. This policy is based upon the need to protect SIOP-ESI from possible compromise resulting from the capture, interrogation, exploitation, or entrapment of personnel who have or have had access to SIOP-ESI.

CLASSIFIED BY DIRECTOR, J-3
DECLASSIFY ON OADR

[redacted]

3. (U) Definitions

a. (U) SIOP-ESI. SIOP-ESI is defined in subparagraph 3b of the Appendix.

b. (U) Hazardous Activities. Hazardous activities include assignments or visits to and travel through countries listed in the Tab. Hazardous activities also include assignment or travel in combat zones or other areas where hostilities are taking place, duty behind hostile lines, and duty or travel in isolated or exposed areas where individuals cannot reasonably be protected against hostile action.

c. (U) Foreign Travel Briefings. These briefings alert traveling personnel to the potential for harassment, provocation, or entrapment by foreign intelligence services in overseas areas and in other environments of an international nature, such as conferences, scientific and technical meetings, seminars, and symposiums. They examine foreign intelligence service methods of operation and suggest precautions designed to minimize the risk of direct foreign intelligence exploitation of personnel during periods of temporary duty or leave.

[redacted]

d. (U) Antiterrorist Briefings. These briefings advise personnel of a variety of measures that may be employed to safeguard oneself against terrorist threats in overseas areas.

4. (U) Policy. Personnel who have detailed knowledge and continuing access to SIOP-ESI information at Service, joint agency, or unified and specified command level may be subject to travel and assignment restrictions, as determined by the authority granting access.

a. (U) Official Assignment/Travel

(1) (U) To the extent practicable, personnel with detailed knowledge and continuing access to SIOP-ESI should not be assigned to or directed to participate in hazardous activities. Regardless of the degree of access, all personnel who have access to SIOP-ESI must be appropriately briefed prior to participation in any hazardous activity or visit as defined in subparagraph 3b above.

(2) (U) Prior to official visits to or travel through the countries listed in the Tab, personnel who have access to SIOP-ESI must:

[redacted]

(a) (U) Give their supporting security office advance notice of such planned travel.

(b) (U) Obtain foreign travel and antiterrorist briefings before traveling to such countries.

(c) (U) Immediately contact the nearest US Consul Attache, or Embassy Regional Security Officer or Post Duty Officer if detained or subjected to significant harassment or provocation while traveling.

(d) (U) Report to the specified official upon return from travel any unusual incidents, including incidents of potential security concern, encountered during such travel.

NOTE: Individuals who frequently travel, or attend or host meetings of foreign visitors of the types described in subparagraphs 3c above, need not be briefed for each such occasion, but shall be provided a thorough briefing at least once each 6-month period and a general reminder of their security responsibilities prior to each such activity.

b. (U) Unofficial Travel

(1) (U) Prior to unofficial visits to or travel through the countries listed in the Tab, personnel who have access to SIOP-ESI must take the actions outlined in

subparagraph 4a(2) above.

(2) (U) Access-granting authorities may deny unofficial travel by notifying the requester in writing of the specific conditions upon which the denial is based.

c. (U) Actions Required of All Persons Traveling to or Through Designated Countries (see Tab).

(1) (U) During official or unofficial visits to or travel through the countries listed in the Tab, persons who have access to SIOP-ESI MUST immediately contact the nearest US consular, attache, or Embassy official if they have been detained or subjected to significant harassment or provocation while traveling.

(2) (U) Persons who have access to SIOP-ESI must be reminded annually of the foregoing obligations through security education programs.

d. (U) Individuals With Previous Access. Persons whose access to SIOP-ESI is being terminated will be officially reminded if their obligation to ensure continued protection of SIOP-ESI and reminded of the risks associated with hazardous activities as defined herein.

5. (U) Responsibilities

a. (U) The Directorate for Information and Resource Management, OJCS, will prepare and disseminate to the holders of this document an updated list of countries (Tab) identified as posing a security risk bearing on this policy as changes occur.

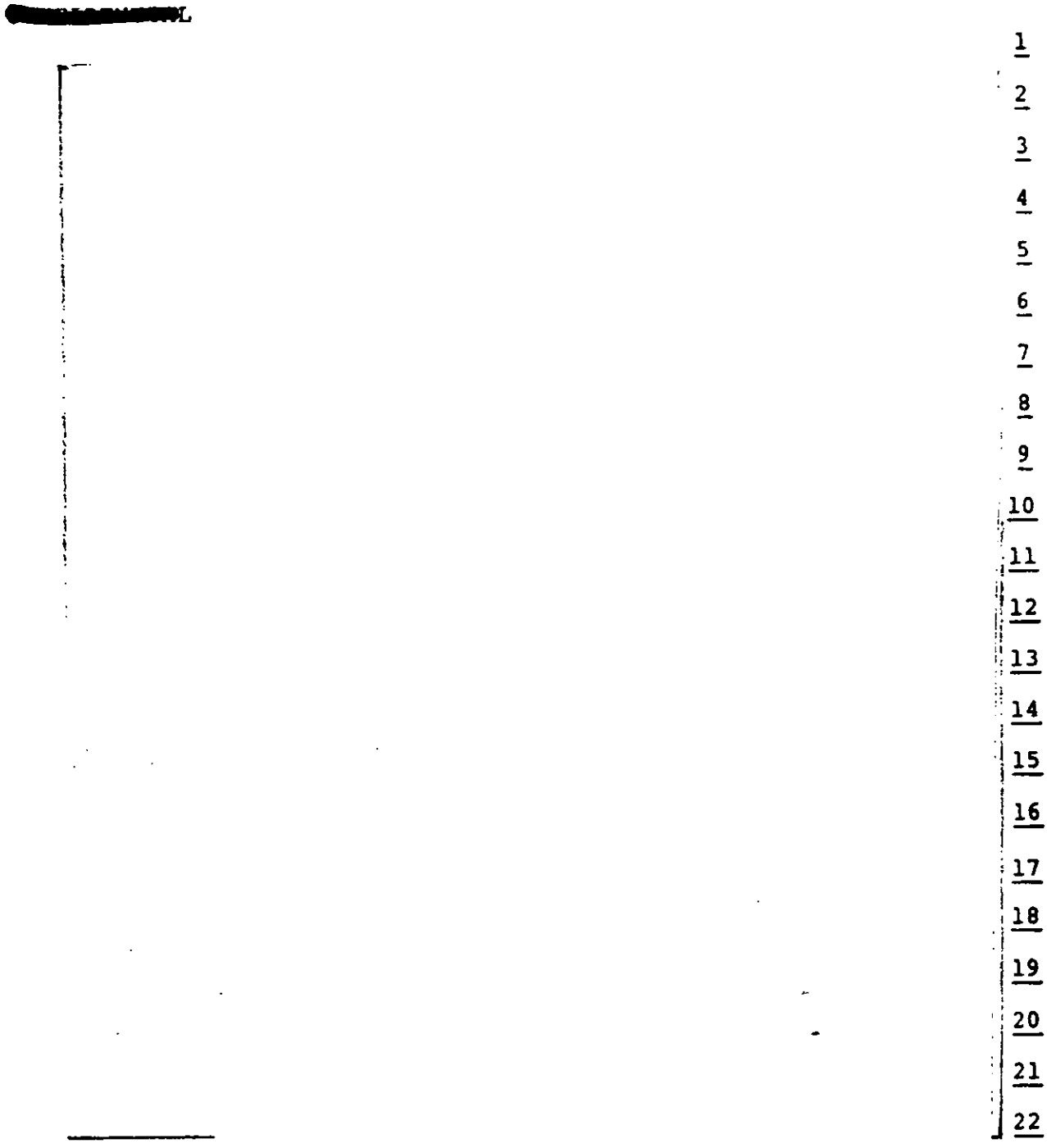
b. (U) Access-granting authorities will issue implementing directives concerning travel and assignment of personnel under their cognizance.

[redacted]

TAB TO ANNEX E

COUNTRIES AND AREAS IN WHICH VISITS, TRAVEL, AND ASSIGNMENT ARE CONSIDERED TO BE A HAZARDOUS ACTIVITY (U)

CLASSIFIED BY DIRECTOR, J-3
DECLASSIFY ON OADR



ANNEX F

REFERENCES

1. Executive Order 12356, 2 April 1982, "National Security Information"

2. Public Law, 93-579, Title 5, United States Code, Section 552a, (Privacy Act of 1974)

3. DOD Directive 5100.55, 21 April 1982, "United States Security Authority for North Atlantic Treaty Organization Affairs" (USSAN Instruction 1-69)

4. DOD Directive 5200.1, 7 June 1982, "DOD Information Security Program"

5. DOD Regulation 5200.1-R, June 1986, "Information Security Program Regulation"

6. DOD Regulation 5200.2-R, January 1987, "DOD Personnel Security Program"

7. DOD Directive C-5200.5, 6 October 1981, "Communications Security (COMSEC) (U)"

8. DOD Directive S-5200.19, 10 February 1968, "Control of Compromising Emanations (U)"

9. DOD Directive 5200.28, 29 April 1978, "Security Requirements for Automatic Data Processing (ADP) Systems"

10. DOD Manual 5200.28-M, 25 June 1979, "ADP Security Manual"

11. DOD Instruction 5220.28, 8 March 1978, "Application of Special Eligibility and Clearance Requirements in the SIOP-ESI Program for Contractor Employees"

12. DOD Directive 7920.1, 17 October 1978, "Life Cycle Management of Automated Information Systems (AIS)"

13. JCS MOP 39, 28 September 1983, "Release Procedures for JCS Papers"

14. JCS Pub 6, Volume II, Part 1, 1 October 1985, "Standing Operating Procedures for the Coordination of Atomic Operations (CAO SOP) (U)"

15. MJCS-273-83, 20 December 1983, "Guidance for the Sanitization and Distribution of SIOP Information to SACEUR and SACLANT"

16. SM-81-77, 1 February 1977, "Basic Policy Guidance on Wargaming (U)"

17. SM-283-81, 24 April 1981, "Emergency Action Procedures of the Joint Chiefs of Staff (EAP-JCS), Volume II - SIOP Instructions (U)"

18. J3M-2061-83, 1 August 1983, "Emergency Action Procedures of the Joint Chiefs of Staff, Volume IV - Alternate Procedures (U)"

19. NDP-1, 9 September 1981, "National Policy and Procedures for the Disclosure of Classified Military Information to Foreign Governments and International Organizations (National Disclosure Policy)"

20. Joint Atomic Information Exchange Group (JAIEG) memorandum, JAIEG Case N-15/75F, 10 December 1975, "Authorization and Release Procedures for SIOP ATOMAL Information to NATO (U)"

21. JSTPS Air Defenses Handbook, October 1980

22. ACP 121 US Supp-1(Series), June 1981, "Communications Instructions-General"

23. USSAN Instruction 1-69 (DOD 5100.55, Encl 2), 1982, "United States Implementation of NATO Security Procedures (U)"