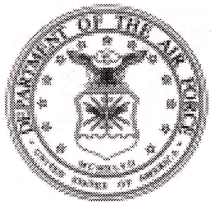
BY ORDER OF THE
SECRETARY OF THE AIR FORCE
BY ORDER OF THE COMMANDER
AIR MOBILITY COMMAND



AIR FORCE INSTRUCTION 10-1102

5 August 1994

AIR MOBILITY COMMAND
Supplement 1

10 May 1995

Operations

SAFEGUARDING THE SINGLE INTEGRATED OPERATIONAL PLAN (SIOP)

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

NOTICE: A copy of this publication can be found digitally at http: www.safb.af.mil:80/hqamc/pa/pubs/pubhome2.htm. If you lack access, contact your Publishing Distribution Office (PDO).

OPR: HQ ACC/SPIP
(Mr. Gerald J. Dvorak)
HQ AMC/SPI
(Ms Sharon Thompson)
Supersedes AFR 205-25(S)/AMC1, 23 April 1992.

Certified by: HQ USAF/XOF
(Col Norton A. Schwartz)
HQ AMC/SPI
(Mr Norman Mitchell)
Pages: 8
Distribution: F

This instruction implements Chairman, Joint Chiefs of Staff Instruction (CJCSI) 3231.01, *Safeguarding the Single Integrated Operational Plan (SIOP)*, November 30,1993, and Air Force Policy Directive (AFPD) 10-11, *Operations Security.* It explains Air Force policies and procedures to ensure authorized personnel have access to, and properly control, SIOP Extremely Sensitive Information (ESI). Use this instruction with CJCSI 3231.01; Department of Defense (DoD) Regulation 5200.1-R, *Information Security Program Regulation,* June 1986; With Change 1, AFPDs 10-11 and 31-4, *Information Security*; AFI 31-401, *Information Security Program Management*; and AFI 31-501, *Personnel Security Program Management.* Send requests for waivers or interpretations, and recommendations to change, add, or delete requirements of this instruction, to HQ ACC/SPI, 220 Sweeney Blvd, Suite 112, Langely AFB VA 23665-2796, with an information copy to HQ USAF/XOFS, 1480 Pentagon, Washington DC 20330-1480.

SUMMARY OF CHANGES

This is the initial publication of AFI 10-1102 and it substantially revises previous Air Force policies and procedures for safeguarding the SIOP.

(AMC) AFI 10-1102, 5 Aug 1994, is supplemented as follows: (This publication requires collecting and maintaining information protected by the Privacy Act of 1974. Executive Order 9397, 22 November 1943, authorizes using the Social Security number (SSN) as a personal identifier. SSN is required for positive identification of personnel. This supplement applies to AMC gained Air National Guard (ANG) and United States Air Force Reserve (USAFR) units.)

Section A— Responsibilities Assigned

1. United States Air Force Air Staff (HQ USAF):

1.1. The Deputy Chief of Staff for Plans and Operations (HQ USAF/XO) is the Office of Primary Responsibility on all policies and procedures for safeguarding the SIOP.

1.2. The Directorate of Forces (HQ USAF/XOF), through the Space and Nuclear Forces Division (HQ USAF/XOFS), is the Air Staff manager for processing SIOP-ESI matters and for reviewing and approving any changes or revisions to SIOP policies, procedures, or instructions.

2. Air Combat Command (ACC):

2.1. The Chief, Information Security Oversight Division (HQ ACC/SPI) is the Air Force executive agent for preparing and keeping this instruction current.

2.2. HQ ACC/SPI, through an assigned Policy Integration and Personnel Security Branch (HQ ACC/SPIP), prepares a handbook with sample illustrations and formats for managing SIOP program requirements.

3. Subordinate Commanders. Major command (MAJCOM), field operating agency (FOA), direct reporting unit (DRU), Numbered Air Force (NAF), center, and wing commanders will appoint an individual as their servicing SIOP Program Manager (SPM) for administering requirements at their level of command.

4. Unit or Staff Agency SPM. Each unit commander or staff agency chief who has SIOP-ESI documents or access authorizations will appoint a unit or staff agency SPM for managing requirements of this instruction.

4. (AMC) All AMC Directorates, staff agencies, and subordinate units that maintain SIOP-ESI material will appoint a properly cleared person as the SIOP program manager (SPM). Submit the name, grade, office symbol, and phone number of each SPM to HQ AMC/SPI and updated as changes occur. In addition, field units will provide a copy of the appointment letter to the servicing security police office.

Section B— Access Requirements

5. Access Granting Authorities:

5.1. The Air Force has approved the Chief of Staff, Vice Chief of Staff, Assistant Vice Chief of Staff, and Deputy Chiefs of Staff for SIOP-ESI access and has designated them as SIOP-ESI access granting authorities. These officials may further delegate their access granting authority within a MAJCOM, DRU, NAF and Center Headquarters to no lower than division chief or equivalent in the grade of at least O-6.

5.2. The Air Force has approved subordinate commanders and vice commanders tasked to execute the SIOP for SIOP-ESI access and has designated them as SIOP-ESI access granting authorities. These officials may further delegate their access granting authority:

5.2.1. Within a MAJCOM, DRU, NAF, and center headquarters to no lower than director or equivalent level.

5.2.1. (AMC) AMC/CC/CV, AMC directors and their assistants, and staff agency chiefs and their deputies; NAF commanders and vice commanders; unit commanders for ANG and USAFR units; and wing commanders and vice commander are authorized to grant SIOP-ESI access to their personnel for all SIOP-ESI categories.

5.2.2. Within a wing to no lower than a group commander or equivalent level.

5.3. Delegated access granting officials must have access to the required categories of SIOP-ESI before exercising their authority.

6. Documenting Access, Briefings, and Debriefings:

6.1. Document access on AF Form 2583, **Request for Personnel Security Action.** In the "Remarks" section of this form, show the briefing date and signature of the individual briefed.

6.2. Access granting authorities whose missions require access to SIOP-ESI are authorized access as an inherent part of their duty function. For these individuals, signature is not required in block 29 of the AF Form 2583.

6.2. (AMC) Individuals assigned to positions in paragraph **5.2.1.**, this supplement, are authorized SIOP-ESI access after appropriate briefing to affected categories.

6.3. Use AF Form 2587, **Security Termination Statement**, when debriefing an individual from SIOP-ESI access.

6.3. (AMC) AF Forms 2587 will be annotated with the SIOP-ESI categories of access terminated. A copy of the AF Form 2587 terminating permanent SIOP-ESI access will be sent to the SIOP Special Access Program Manager (SSAPM) who is responsible for maintenance of the SIOP-ESI access list.

7. Industrial Operations. When classified contract efforts require access to or generation of

SIOP-ESI, program and project managers will coordinate DD Forms 254, **DoD Contract Security Classification Specification**, and contractual statements of work, with the servicing SPM.

7. (AMC) Requests for temporary access for industrial contractors must be sent through HQ AMC/SPI to HQ USAF/XOFS. Request will include the name and duty phone of a point of contact in the requesting office. Sample format is at **Attachment 2 (Added)**, this supplement.

7.1. Security requirements for contracts requiring SIOP-ESI access must be identified early in the acquisition phase to ensure requirements can be stated to the contractor in both the statement of work (SOW) and the DD Form 254, **Contract Security Classification Specification**. See **Attachment 3 (Added)**, this supplement, for sample security requirements to be included in the SOW. DD Forms 254 for contracts requiring SIOP-ESI access will be annotated as follows:

7.1.1. Item 10b. Mark "yes."

7.1.2. Item 13. Add the following: Reference item 10b. This contract requires access to SIOP-ESI. SIOP-ESI material remains under US government control at all times. Access to SIOP-ESI by contractor personnel will be limited to US government facilities. See contract statement of work for SIOP-ESI security requirements and access processing instructions.

7.2. **(Added)** AF Forms 2583 must be prepared for contractors granted temporary SIOP-ESI access. Complete sections I, II, and VI. SSAPMs may complete items 27, 28, and 29. In section VII,

remarks, indicate the JCS authorization letter that granted access (i.e. J-3M 5-92, 10 February 1992) and show inclusive dates for which access was authorized. Update AF Form 2583 as required by a reference to the JCS letter which authorizes extension of temporary access (i.e. "Temporary SIOP-ESI access extended through 30 May 1992 by J-3M 6-92, 1 May 1992").

8. Foreign National SIOP-ESI Access. Send requests for release of SIOP-ESI to a foreign national through SPM channels to HQ USAF/XOFS.

9. Adverse Access Removal and Administrative Due Process . An individual disagreeing with the adverse removal of SIOP-ESI access may appeal in writing to the access granting authority. The access granting authority will appoint a disinterested person to review merits of the appeal. If the access granting authority denies the appeal, the individual has 30 calendar days from the date of the denial letter to request the final appellate review of this determination by the MAJCOM, DRU, or FOA SIOP Program Manager. For Headquarters USAF, and MAJCOMs, DRUs, or FOAs without a SIOP Program Manager, send these requests to the Air Force SIOP Access Program Executive Agent (HQ ACC/SPI). This further appellate determination is final and not reviewable.

10. Report Requirements, RCS: HAF-XOF(A) 8901, SIOP-ESI Numerical Re port . Not later than 15 January of each year, MAJCOM, FOA, and DRU SPMs send a numerical report to HQ ACC/SPI of all persons approved for SIOP-ESI access, with a close-out date of 31 December of the preceding year. Submit the report by type of access (permanent and temporary), personnel status (military, civilian and contractor) and by access category. The Air Force designates this report emergency status code D. Immediately discontinue reporting data requirements during emergency conditions.

10.1. Each SPM will be responsible for maintaining listing of all persons approved for SIOP-ESI access. Update the list as changes occur and maintain at the unit or agency. Also, send copy of the changes to HQ AMC/SPI as they occur.

Section C— Control Procedures

11. Marking Standards:

11.1. Interior Page Markings. Mark the bottom of each interior page containing SIOP-ESI with the indicator "SIOP-ESI."

11.2. Portion Markings. Each section, part, paragraph, subparagraph or similar portion of a classified document that has SIOP-ESI will include the abbreviated symbols "(TS)(SIOP-ESI)."

11.3. File Folders. Apply the indicator "SIOP-ESI" on the file folder tab and once on the back of the folder.

11.4. Classified Cover Sheets. In the "Remarks" section of AF Form 144, **Top Secret Access Record and Cover Sheet**, enter the notice "This (correspondence, memorandum, report, etc.) contains SIOP-ESI Category (XX) data. Access lists govern internal distribution."

11.5. Inner Wrappings . The inner wrapping of packages, envelopes or containers with SIOP-ESI will reflect the notice "This (correspondence, memorandum, report, etc.) contains SIOP-ESI Category (XX) data. Access lists govern internal distribution."

12. Safekeeping and Storage. Keep SIOP-ESI documents separate from other classified materials. The use of guidecards, file folders, or separate drawers of multi-drawer security containers suffice for this purpose.

13. Loss or Compromise of SIOP-ESI. The responsible commander will notify HQ USAF/XOFS through SPM channels of any loss or compromise of SIOP-ESI. Upon completion of the inquiry or investigation, send a final report through SPM channels to HQ USAF/XOFS.

Section D— "For Cause" Administrative Discharges, Courts-Martials, and Civilian Removal Actions

14. Requesting Permission to Proceed . Unit commanders considering disciplinary or administrative action against military members or civilian employees that could lead to a discharge or removal must first get written permission to proceed. See AFI 31-501 for more guidance.

15. SIOP "For Cause" Decision Authorities . SIOP-ESI access granting authorities are also designated as decision authorities to approve or deny requests to proceed with "for cause" actions.

16. Damage Assessment . If a decision authority does not approve a request to proceed due to extenuating circumstances, send the case to the AF executive agent (HQ ACC/SPI) for further processing.

EDWIN E TENOSO, Major General, USAF
Acting Deputy Chief of Staff for Plans and Operations

ATTACHMENT 1 (ADDED) (ADDED-AMC)

SAMPLE SIOP-ESI BRIEFING

1. This briefing is conducted under the authority of AFI 10-1102, *Safeguarding the Single Integrated Operational Plan (SIOP)*, and AMC Supplement 1. The purpose is to acquaint you with how to identify SIOP material and your responsibilities toward its protection.

2. What is the SIOP? It is a single plan that provides for coordinated attack on targets by all military commands. It consists of Joint Chiefs of Staff documents, developed and maintained by the United States Strategic Command (USSTRATCOM) and HQ AMC/DO. SIOP-ESI is extremely sensitive information that is part of the SIOP, consisting of detailed TOP SECRET information and material of such an extremely sensitive nature that its disclosure to unauthorized persons could seriously degrade the execution of the SIOP. SIOP-ESI information can be found, but is not limited to, the following forms:

- Written material, including printed, typed, or handwritten
- Painted or drawn material
- Data processed by electronic means
- Sound recordings
- Data processed by photographic media
- Reproductions of the above by whatever process
- Materials used in reproducing the above (i.e. typewriter and printer ribbons, copying machine belts, etc.)

3. Access to SIOP-ESI. The following criteria must be met for permanent access can be granted to military or DoD civilian personnel:

- Be a US citizen
- Be assigned to a position requiring access
- Possess a final TOP SECRET clearance based on an SBI or SSBI current within the last 5 years

4. SIOP access is defined by category in CJCSI 3231.01. Each category contains information specific to a particular function. Individuals will be granted access to the categories necessary to complete their jobs. Before releasing SIOP information to anyone, ensure the person has access to the appropiate category.

5. SIOP access authorization is a formal act required to certify that an individual, who has been determined to be eligible, has been granted access to SIOP-ESI information. Access granting authorities are in AFI 10-1102/AMC Supplement 1. This authorization is recorded on an AF Form 2583, and your SIOP program manager (SPM) maintains a list of all personnel in your unit with this access.

ATTACHMENT 2 (ADDED) (ADDED-AMC)

CONTRACTOR SIOP-ESI BILLET REQUEST

Name:

SSN:

Company Name:

Date of Birth:

Place of Birth:

Citizenship of Applicant:

Citizenship of Spouse:

SIOP-ESI Category of Access Required:

TOP SECRET clearance based on a favorably completed SBI or SSBI, dated_____.

Inclusive dates SIOP-ESI access will be required.

Contract Number:

Justification: (State specifically why individual cannot complete his or her job without SIOP-ESI access):

Also include:

a. Whether the request is in addition to personnel already supporting HQ AMC requirements with extensive rationale as to why additional personnel are needed.

b. Whether the request is for replacement personnel, to include the names of the individuals being debriefed.

c. Whether the request is to support new or expanded contracts with appropriate justification for SIOP access. Job Description:

Project Officer Information: Name, grade, office symbol, phone number, date prepared

ATTACHMENT 3 (ADDED) (ADDED-AMC)

SECURITY REQUIREMENTS FOR CONTRACTS REQUIRING ACCESS TO SIOP-ESI

1. This contract will require contractor personnel to have access to TOP SECRET SIOP-ESI information. Access to SIOP-ESI will be limited to US government installations.

2. In order to be considered for access to SIOP-ESI, applicant and spouse, if any, must be United States citizens. No waivers will be considered. In addition, applicant must have a TOP SECRET clearance based on a favorable Special Background Investigation (SBI) or Single Scope Background Investigation (SSBI) current within the past 5 years. Again, no waivers will be considered.

3. Contractor will nominate personnel to (AMC OPR for the contract). Contractor will nominate only technically qualified personnel who meet citizenship and clearance requirements stated above.

4. Nominations will contain full identifying data on the nominee, statement that he or she and spouse meet the above citizenship requirements, description of the applicant's duties under the contract which will require access to SIOP-ESI, applicant's current clearance and the basis for the clearance.

4.1. If the applicant does not have a favorable current SBI or SSBI within the past 5 years, (AMC OPR) will provide an endorsement to Defense Industrial Security Clearance Office (DISCO) on a copy of the nomination. Endorsement will advise DISCO that SSBI is required for SIOP-ESI access. Endorsement and nomination will be returned to the contractor for inclusion in the SSBI request which the contractor sends to DISCO.

4.2. If applicant meets the clearance and investigation criteria, nomination must be received by the contract project office 60 days in advance of anticipated date SIOP-ESI access is required.

4.3. If applicant does not meet the clearance or investigation criteria, nominatioin must be received 6 months before anticipated date SIOP-ESI access is required.

5. SIOP-ESI access will require a briefing and debriefing to be accomplished by AMC. Contractor will cooperate with AMC in making personnel available with sufficient lead time to permit AMC to arrange for required briefings and debriefings.

6. Contractor will advise (AMC OPR) of any adverse information or change in status of an employee who has been granted access to SIOP-ESI, i.e. marriage, divorce, or remarriage.