BY ORDER OF THE
SECRETARY OF THE AIR FORCE

AIR FORCE INSTRUCTION 10-1102

5 August 1994

Operations

SAFEGUARDING THE SINGLE INTEGRATED OPERATIONAL PLAN (SIOP)

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

NOTICE: This publication is available digitally on the SAF/AAD WWW site at: http://afpubs.hq.af.mil. If you lack access, contact your Publishing Distribution Office (PDO).

OPR: HQ ACC/SPIP (Mr. Gerald J. Dvorak)

Certified by: HQ USAF/XOF
(Col Norton A. Schwartz)

Supersedes AFR 205-25, 27 December 1984.

Pages: 4
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.

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.

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.

5.2.2. 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.

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

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.

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.

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