BY ORDER OF THE
SECRETARY OF THE AIR FORCE

AIR FORCE INSTRUCTION 10-1102

15 JULY 2002

Operations

SAFEGUARDING THE SINGLE INTEGRATED OPERATIONAL PLAN (SIOP)

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

NOTICE: This publication is available digitally on the AFDPO WWW site at: **http://afpubs.hq.af.mil.**

OPR: AFSPC/SFC (Mr. James E. Moree)

Certified by: HQ USAF/XON (Maj Gen Franklin J. Blaisdell)

Supersedes AFI 10-1102, 5 August 1994

Pages: 5

Distribution: F

This Air Force Instruction (AFI) implements Chairman, Joint Chiefs of Staff Instruction (CJCSI) 3231.01A, S*afeguarding the Single Integrated Operational Plan (SIOP)*, 7 January 2000. It explains Air Force security policies and procedures to make sure authorized personnel have access to SIOP Extremely Sensitive Information (ESI). This instruction is applicable to all USAF activities to include the Air National Guard and the Air Force Reserves. This publication interfaces with AFPD 10-11, *Operations Security.* Use this instruction with CJCSI 3231.01A; DoD 5200.1-R, *Information Security Program Regulation;* AFPD 31-4, *Information Security*; and 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 AFSPC/SFC, 150 Vandenberg Street, Suite #1105, Peterson AFB CO 80914-4560.*

SUMMARY OF REVISIONS

This is the second 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 Air and Space Operations (HQ USAF/XO) is the Office of Primary Responsibility on all policies and procedures for safeguarding the SIOP.

1.2. The Directorate for Nuclear and Counterproliferation, DCS/Air and Space Operations (HQ USAF/XON), through the Operations Division (HQ USAF/XONO), is the Air Staff SIOP Program Manager (SPM) for processing SIOP-ESI matters.

2. Air Force Space Command (AFSPC):

2.1. The Chief, Security Countermeasures Division (HQ AFSPC/SFC) is the Air Force executive agent for AFI 10-1102.

2.2. Send requests for waivers or interpretations, and recommendations to change, add or delete requirements of this instruction, to HQ AFSPC/SFC. Also send an information copy to HQ USAF/XONO.

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 SPM for administering requirements at their level of command. Within a MAJCOM Headquarters, this appointing authority may be delegated to the Director with assigned SIOP Program oversight.

4. Unit, Staff Agency, and Headquarters Directorate SPM.

4.1. Each unit commander, staff agency chief, or headquarters director who has SIOP-ESI documents or access authorizations will appoint a SPM for managing requirements of this instruction.

4.2. SPM responsibilities will include developing and documenting procedures for granting and controlling access for temporary, permanent, and contractor access. This should include a revocation process. Specific positions requiring access will be documented and audited IAW CJCSI 3231.01A. The SPM will be responsible for overseeing training programs relating to managing access and handling of SIOP-ESI documents.

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. They are further designated as SIOP-ESI access granting authorities. These officials may further delegate their access granting authority within the Air Staff to no lower than division chief or equivalent grade of at least O-6.

5.2. The Air Force has approved subordinate commanders and vice commanders tasked to support or 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, FOA, 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 to grant access to those categories.

6. Waivers to basic access criteria: Waiver authority for basic access criteria is authorized under CJCSI 3231.01A to General/Flag Officers and is further delegated to Wing, FOA, DRU, NAF Commanders, Air Staff division chiefs, and MAJCOM directors possessing access granting authority.

7. Documenting Access, Briefings and Debriefings:

7.1. Document access on AF Form 2583, **Request for Personnel Security Action.** In the "Remarks" section of this form, show the briefing date, annual refresher training and signature of the individual briefed. The briefing will cover access requirements, safeguarding of SIOP-ESI information, and personal responsibilities while granted access, and after access is revoked.

7.2. 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.

7.3. Use AF Form 2587, **Security Termination Statement**, when debriefing an individual from SIOP-ESI access and maintain for two years. If indoctrinated personnel depart without a formal debrief, ensure administrative debrief is accomplished and attached to form.

8. Industrial Operations. When classified contract efforts require access to or generation of SIOP-ESI, program and project managers will coordinate DD Forms 254, **Contract Security Classification Specification**, and contractual statements of work, with the servicing SPM. Contractor personnel will not be granted permanent access to SIOP-ESI, but may be granted temporary access through period of government contract not to exceed 3 years (IAW CJCSI 3231.01A). Contractor personnel without a completed special security background investigation may be waived to have access if interim clearance is approved and formal investigation request is on file with DSS.

9. Foreign National SIOP-ESI Access. Send requests for release of SIOP-ESI to a foreign national through SPM channels to HQ USAF/XONO with coordination of MAJCOM Foreign Disclosure office. If a MAJCOM office is not within channels, send direct to SAF/IA..

10. 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 Air Staff, MAJCOM, DRU, or FOA SIOP Program Manager. For Air Staff, MAJCOMs, DRUs, or FOAs without a SIOP Program Manager, or for SPMs needing further resolution, send these requests to the Air Force Executive Agent (HQ AFSPC/SFC) for final appellate review and decision. These appellate determinations are final.

Section C—Control Procedures

11. Marking Standards: The cover page of the document should have "Single Integrated Operational Plan - Extremely Sensitive Information" annotated on the bottom/footer.

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, by secure telephone and followed up in writing, HQ USAF/XONO and HQ AFSPC/SFC 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/XONO and HQ AFSPC/SFC.

Section D—"For Cause" Administrative Discharges, Courts-Marital, 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 determine if a national security risk exists should the individual be discharged or removed. If such a risk is determined to exist, then written permission to proceed must be obtained from SIOP “For Cause” decision authorities responsible for granting the individual SIOP access.

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, a damage assessment by that decision authority must be included in that decision process.

17. Forms Adopted. Air Force Form 144, ***Top Secret Access Record and Cover Sheet***, 2583***, Request for Personnel Security Action***, 2587, ***Security Termination Statement,*** DD Form 254, ***Contract Security Classification Specification***.

CHARLES F. WALD, Lt Gen, USAF
DCS/Air and Space Operations

Attachment 1

GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

References

AFPD 10-11, *Operations Security, May 2001*

AFPD 31-4, *Information Security, Sep 1998*

AFI 31-401, *Information Security Program Management, Nov 2001*

AFI 31-501, *Personnel Security Program Management, Aug 2000*

CJCSI 3231.01A, S*afeguarding the Single Integrated Operational Plan (SIOP), Jan 2000*

DoD 5200.1-R, *Information Security Program Regulation, Jan 1997*

Abbreviations and Acronyms

AF—Air Force

AFI—Air Force Instruction

AFOSI—Air Force Office of Special Investigations

AFPD—Air Force Policy Directive

DCS—Deputy Chief of Staff

DOD—Department of Defense

DRU—Direct Reporting Unit

ESI—Extremely Sensitive Information

FOA—Field Operating Agency

HQ USAF—Headquarters United States Air Force

MAJCOM—Major Command

NAF—Numbered Air Force

PCS—Permanent Change of Station

SAF—Secretary of the Air Force

SIOP—Single Integrated Operational Plan

SIOP-ESI—Single Integrated Operational Plan -Extremely Sensitive Information

SSN—Social Security Number

SPM—SIOP Program Manager