BY ORDER OF THE COMMANDER

AIR FORCE INSTRUCTION 10-1102
OFFUTT AFB SUPPLEMENT 1

9 DECEMBER 2005

Operations

SAFEGUARDING THE SINGLE INTEGRATED OPERATIONAL PLAN

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

Notice: The official version of this publication is available digitally on the Offutt AFB Intranet site at: https://wwwmil.offutt.af.mil/base/publications/sup/10series/index.htm. If you lack access, contact the Base Publishing Office or 55 SFS/SFAI for an electronic copy.

OPR: 55 SFS/SFAI (Mr. Mercier)
Approved by: Mr. Selph
Editor: MSgt Springer
Supersedes: AFI10-1102_OFFUTTAFBSUP1, 31 Mar 2001

Certified by: (55 SFS/CC)
(Lt Col Bradley A. Wayland)
Pages: 22
Distribution: F

AFI 10-1102, 15 Jul 02, *Safeguarding The Single Integrated Operational Plan (SIOP)* is supplemented as follows. The purpose of this supplement is to establish procedures for processing and safeguarding of the Single Integrated Operational Plan (SIOP) within the 55th Wing. This supplement provides several key local policies and procedures for Safeguarding the SIOP and should be completely reviewed. It provides specific guidance on matters of particular concern applicable to the 55th Wing and supporting tenant units. Ensure that all records created as a result of processes prescribed in this publication are maintained in accordance with AFMAN 37-123, *Management of Records* (to be replaced by AFMAN 33-363), and are disposed of in accordance with the Air Force Records Disposition Schedule (RDS) located at: https://afrims.amc.af.mil/. Contact supporting records managers as required.

SUMMARY OF REVISIONS: This document has been administratively revised and should be completely reviewed.

Section A – Responsibilities Assigned

3.1. (Added) SIOP-Extremely Sensitive Information (ESI) Program Manager. 55 SFS/SFAI is designated by the 55 WG/CC as the servicing SIOP Program Manager for the 55th Wing. 55 SFS/SFAI, is the Office of Primary Responsibility for preparing and keeping this supplement current and ensuring the SIOP-ESI information is processed and safeguarded.

4.3. (Added) Unit SIOP-ESI Monitor. Unit with personnel briefed on SIOP-ESI will forward a copy of appointment letters designating a primary/alternate SIOP-ESI monitor to 55 SFS/SFAI.

Section B – Access Requirements

5.2.2.1. (Added) SIOP-ESI Access Granting Authorities. The 55 WG/CC is the sole granting authority for access to SIOP-ESI for individuals subject to military, OPM, or DoD personnel policies. The wing commander delegates this authority to 55 WG/CV, 55 CG/CC, 55 MXG/CC, 55 OG/CC, 55 MDG/CC and 55 MSG/CC. Personnel requiring access to SIOP-ESI who are not assigned to the 55th Wing or tenant units, will not be granted access through 55th Wing channels. These personnel must properly coordinate through their local channels prior to visiting the 55th Wing or tenant unit and accessing SIOP-ESI.

5.2.2.2. (Added) The unit commander or staff agency chief determines SIOP-ESI access requirements within their unit. The position code is 5 for a SSBI which allows access to SIOP-ESI. As prescribed by reference (g), (para 7.1.2 - 7.1.2.4). Each unit with personnel who are briefed on SIOP-ESI will be required to procure and maintain a copy of CJCSI 3231.01A, Chairman, Joint Chiefs of Staff Instruction.

5.2.2.2.1. (Added) Commanders or designated unit SIOP-ESI monitors will review all SIOP-ESI positions within their unit for recertification annually as prescribed by reference (g), (para 7.1.2.2)

5.2.2.3. (Added) Foreign travel. All SIOP-ESI cleared personnel must be aware of the risks associated with foreign countries and foreign intelligence services. A foreign travel briefing will be administered during the initial SIOP-ESI briefing. The foreign travel briefing is included in *Attachment 2*.

5.2.2.4. (Added) Access Eligibility. There are three types of access to SIOP-ESI, permanent, temporary, and contractor. Personnel must have a current SSBI within five years. If the date of their last investigation is over 5 years old, they must submit a periodic reinvestigation prior to being granted access. (Reference g, (A3.4 and A3.5) Those personnel granted temporary access will not need to submit a new SSBI.

5.2.2.4.1. (Added) Permanent Access. Prior to granting access to SIOP-ESI, the following criteria must be met:

5.2.2.4.1.1. (Added) The individual is a United States citizen;

5.2.2.4.1.2. (Added) The individual has been granted a final Top Secret clearance by the appropriate adjudication facility per policy and criteria prescribed in reference (c);

5.2.2.4.1.3. (Added) The individual has been the subject of a complete Single Scope Background Investigation (SSBI) or other type of background equivalent to an SSBI that meet the criteria set forth in reference (c);

5.2.2.4.1.4. (Added) Access must be essential to the performance of duties, need-to-know and the individual is directly involved in the review, development, maintenance, or implementation of SIOP-ESI.

5.2.2.4.2. (Added) Temporary Access. The 55 WG/CC may approve temporary access to SIOP-ESI information for briefings, working meetings, etc., for military and DoD personnel whose duties require short-term or limited access, if all of the following criteria are met:

5.2.2.4.2.1. (Added) Access is essential to the performance of duty;

5.2.2.4.2.2. (Added) The individual meets the basic criteria as specified for permanent access to SIOP-ESI;

5.2.2.4.2.3. (Added) The individual is subject to military, OPM, or DoD personnel policies.

5.2.2.4.3. (Added) Temporary access may be granted for up to one year. Document the access as prescribed in paragraph 6.1 of this supplement. Place an expiration date in block 30, remarks section of the AF Form 2583, **Request for Personnel Security Action**, not to exceed 1 year from date of approval. The expiration date must correspond to a termination date of requirement for temporary access.

5.2.2.4.4. (Added) Personnel granted temporary access to SIOP-ESI need not complete a briefing or debriefing certificate provided the briefing contains appropriate oral and visual warnings regarding the sensitivity of the data of the briefing, working meeting, etc. However, documentation of access levels and granting authority shall be recorded on the AF Form 2583, **Request for Personnel Security Action**.

5.2.2.4.5. (Added) The 55WG/CC is the approval authority for temporary access to personnel who do not have a completed SSBI. It is not necessary to initiate an SSBI for personnel who will only have temporary SIOP-ESI access.

5.2.2.5. (Added) Waiver Authority for Access Eligibility (Interim). The 55 WG/CC is the waiver approval authority for SIOP-ESI, *Attachment 5*. Waivers will only be approved if the individual concerned meets the following criteria:

5.2.2.5.1. (Added) Assigned to a position for which access to SIOP-ESI is required;

5.2.2.5.2. (Added) Possesses an interim Top Secret clearance granted per the policy and criteria prescribed in reference (g);

5.2.2.5.3. (Added) Has an SSBI initiated.

6.1. (Added) Annotate SIOP-ESI categories authorized access to in section VI, AF Form 2583 **Request for Personnel Security Action.**

6.1.1. (Added) Unit SIOP-ESI monitors list the briefing date of the individual briefed in the remarks section, block 30, of the AF Form 2583, **Request for Personnel Security Action**. Attach the SIOP-ESI Briefing certificate to the AF Form 2583, **Request for Personnel Security Action,** *Attachment 1*, or print on reverse side of AF Form 2583, **Request for Personnel Security Action**.

6.1.2. (Added) Unit SIOP-ESI monitors will list the clearance and investigation dates in the remarks section, block 30, of the AF Form 2583**, Request for Personnel Security Action**, . Unit SIOP-ESI monitors will attach the signed waiver of access criteria to the AF Form 2583, **Request for Personnel Security Action,** and update the clearance and investigation dates in the remarks section, block 30 when the Top Secret clearance is finalized. The date of the final Top Secret clearance will establish the start of permanent access and eliminate the waiver.

6.2. (Added) The unit SIOP-ESI monitor will complete and file the AF Form 2587, **Security Termination Statement**, as proof of debriefing and maintain it for two years. If a member converts from one SIOP-ESI category to another do not complete the statement.

6.3. (Added) Unit SIOP-ESI monitors do not require access to SIOP-ESI in order to brief individuals into the program.

6.3.1. (Added) A Security Force local records check is required prior to interim access to SIOP-ESI.

8.1. (Added) Contractor Access. All access to SIOP-ESI will be directly coordinated with 55 SFS/SFAI.

8.1.1. (Added) Access may be granted on a by-name basis and only after determining the task(s) must be accomplished by contractor rather than government personnel. Access by contractor personnel will be on a temporary basis, not to exceed one year. All personnel must have a final Top Secret clearance based on an SSBI. Strict need-to-know criteria applies.

8.1.2. (Added) Program and project managers will coordinate DD Forms 254, **Contract Security Classification Specification, Department Of Defense**, and contractual statements of work, with the unit SIOP-ESI monitor and/or security manager.

8.1.3. (Added) The unit SIOP-ESI monitor will submit requests for access to 55 SFS/SFAI with a SIOP-ESI Security Clearance Request prepared by the contractor, *Attachment 4*. HQ USSTRATCOM must clear all contractors requiring access to SIOP-ESI. The package will be coordinated through 55 SFS/SFAI through HQ ACC/SPOP to HQ Air Force for authorization.

After HQ USSTRATCOM approval is received, the unit SIOP-ESI monitor will conduct briefing procedures for access outlined in paragraph 6.1 through 6.1.2 of this supplement. The unit SIOP-ESI monitor will attach the SIOP-ESI Security Clearance Request and SIOP-ESI briefing certificate to the AF Form 2583, **Request for Personnel Security Action**. These documents will be maintained by the unit SIOP-ESI monitor on all contractors with access to any level of SIOP-ESI material.

8.1.4. (Added) The need for contractor access must be recertified no later than 31 August of each year of expiration using the procedures outlined in paragraph 8.1 – 8.1.3. 55 SFS/SFAI will provide guidance as required.

8.1.5. (Added) Contractor debriefings shall be conducted and recorded on the AF Form 2587, and maintained according to the Air Force Records Disposition Schedule. Notify 55 SFS/SFAI when contractors are debriefed and no longer require access.

10. The SIOP-ESI monitor will notify 55 SFS/SFAI of any personnel subject to debriefing or removal under adverse circumstances.

10.1. (Added) Follow guidelines in reference (e) for administrative due process procedures.

Section C – Control Procedures.

13. Contact 55 SFS/SFAI when any loss or compromise of SIOP-ESI is suspected. A security inquiry will be conducted as prescribed in reference (f). If SIOP-ESI is compromised or lost, the results of the inquiry will be forwarded to HQ USAF/XOFS.

Section D – "For Cause" Administrative Discharges, Courts-Martial, and Civilian Removal Actions

15.1. (Added) For military and civilian personnel, the SIOP-ESI access granting authority has been designated as the decision authority to approve or deny requests to proceed with "for cause" actions. The appropriate commander will forward a memorandum, including the elements shown in *Attachment 3*, to the SIOP-ESI granting authority who granted the SIOP-ESI access to the individual.

15.2. (Added) The unit SIOP-ESI monitor will be responsible to provide the results of "for cause" requests to 55 SFS/SFAI within 30 calendar days of action.

JONATHAN D. GEORGE, Colonel, USAF
Commander, 55th Wing

7 Attachments:
1. SIOP-ESI Briefing Certificate
2. Foreign Travel Security Briefing
3. "For Cause" Request to Proceed Sample Letter
4. Format for SIOP-ESI Security Clearance Request
5. Request for Waiver of Access Criteria Sample
6. Briefing for Access to the Single Integrated Operational Plan-Extremely Sensitive Information
7. Glossary of References and Supporting Information

Attachment 1
SIOP-ESI BRIEFING CERTIFICATE

1. I, _____, acknowledge that by virtue of my position as _____, it is necessary that I have access to Single Integrated Operational Plan-Extremely Sensitive Information (SIOP-ESI) category/categories _____ for the duration of these duties.

2. Because of the extreme sensitivity of SIOP-ESI, I certify that I will not communicate, transmit, or disclose in any manner such information that I have gained as a result of SIOP-ESI access except in the performance of my official duties.

3. I have read and understand the SIOP-ESI briefing material.

4. I acknowledge that I have read and understand my obligations relative to foreign travel.

Signature: _____
Date: _____

Signature of Briefing Official: _____

Attachment 2
FOREIGN TRAVEL SECURITY BRIEFING

Personnel cleared for access to classified information must always be alert to the threat of approaches from foreign intelligence services. This threat is particularly acute for those traveling abroad, beyond the jurisdiction of U.S. law enforcement agencies.

This briefing provides vital information for anyone with access to classified or unclassified sensitive information who is planning visits outside the United States. Because you may have access to classified or unclassified sensitive information, you are a potential target for foreign intelligence agents. When you travel outside the United States, whether on vacation or for the USAF, you will meet people from various foreign countries. It is under these conditions the stage is often set for foreign intelligence gathering activities.

Although the "Designated Country List" has been rescinded, U.S. technology and national defense information is still targeted by foreign nations.

As a traveler, you are more vulnerable because you may be unfamiliar with the customs, people, language, topography, laws, and the judicial system of that country. You become more dependent upon strangers. This is an attractive situation for the foreign agent. The same opportunities exist in both "friendly" and "unfriendly" countries.

Be especially aware that the following circumstances provide perfect opportunities for foreign intelligence agents to contact you. Be alert to overly friendly or helpful strangers. Do not fall into a compromising situation where outside help may be needed or threats of blackmail could surface. Examples of behavior which have led to problems for other U.S. travelers are:

Involvement in illicit currency trade.

Poor judgment in alcohol consumption.

Minor traffic violations.

Gambling.

Any immoral conduct.

Viewing political demonstrations or parades.

Be a smart traveler. Carry personal identification and any special medical information with you at all times. Store essential medication in original containers. Do not leave your wallet or purse unattended. Leave your itinerary at home with a point of contact, and advise him or her of any changes to your itinerary during your trip. Keep a low profile and avoid giving an impression of

wealth. Carry international traveler's checks and always exchange currency at reputable currency exchanges (it is illegal to do otherwise in some countries).

Drive carefully (you may want to apply for an international driver's license if you plan on traveling extensively by car). Observe local laws and customs. For example, in Turkey, Taiwan, and Spain, individuals are prohibited from making derogatory comments about the government or its leaders. In other countries it is unlawful to use insulting language or abusive gestures toward another person while driving. Remember that you are representing the United States while abroad. Avoid political discussions, and remember you may encounter anti-American sentiments. Be patient rather than critical of local customs.

If you follow the basic precautions listed in this briefing, you will reduce your risk of encountering problems while in a foreign country. Enjoy your trip and remember these guidelines are offered to assist you while abroad. In general, keep foremost in your thoughts the reality you have specific knowledge that is valuable to agents of foreign countries. To protect yourself and the information, maintain a low profile and be aware of what is happening around you.

If you have something to report, please contact your security manager or your servicing security office to discuss even the most minor incidents. Remember...

Report any attempt by a foreign national or stranger to establish a continuing association, or arrange future meetings or correspondence.

Report any contact with anyone whom you suspect may be attempting to gather classified information from you.

Maintain a high level of personal standards and conduct. Keep in mind that you are a foreign guest and a representative of the United States.

Do not become involved with local political matters of any kind.

Do not include military or other restricted areas in your visits or picture-taking tours.

Avoid unknown candid or commercial photographers.

Do not promise favors, such as mailing letters for strangers or hand-carrying letters or any other items back to the United States for them.

A foreign travel telephone tip: Even up-to-date publications can be overtaken by political events. Immediate information concerning travel advisories for specific areas of the world are available from the Department of State's Citizen's Emergency Center at (202) 647-5225.

HAVE A GOOD TRIP AND COME HOME SAFELY!!!

Attachment 3
"FOR CAUSE" REQUEST TO PROCEED SAMPLE LETTER

DD/MM/YY

MEMORANDUM FOR 55 WG/CC (Access Granting Authority)

FROM: Unit Commander

SUBJECT: Request for Permission to Proceed With SIOP-ESI "For Cause" Action (FOUO)

1. The following information is provided pursuant to AFI 10-1102, paragraph 15, in obtaining permission to proceed with the SIOP-ESI "for cause" action as indicated below.

a. Personal Data:

(1) Name:
(2) Grade:
(3) SSN:
(4) Date of Birth:
(5) Place of Birth:
(6) Marital Status: Single, Married, Divorced
(7) Number of Dependents:
(8) TAFMSD:
(9) Date of Separation:
(10) Organizational Commander: Rank First MI Last
(11) Unit of Assignment: Squadron/Office Symbol
(12) Duty Title:..
(13) AFSC:

b. Access Data:

(1) Date SIOP-ESI Access Granted:
(2) Access Granting Authority: Rank First MI Last Squadron/Office Symbol
(3) Access Category:
(4) Frequency of Access: Daily, Weekly, Monthly Annually
(5) Date Access Terminated:
(6) Date Member Debriefed:
(7) Other Accesses Held: If none, so specify

c. Access History:

(1) Depth of Access: Be as specific as possible. Describe frequency of access and to which level(s). Give a general description of duties accomplished with granted access.

(2) Member's Technical Knowledge: The member's familiarity with the information to which access was authorized.

(NOTE: IF THE SIOP-ESI ACCESS CATEGORY IS ASSOCIATED WITH ITS ASSIGNED CJCSI 3231.01 DEFINITION, THEN THE REQUEST FOR PERMISSION TO PROCEED CONSTITUTES CONFIDENTIAL CLASSIFIED INFORMATION. PLEASE AVOID THIS ASSOCIATION SO AS TO KEEP THESE REQUESTS UNCLASSIFIED. CLASSIFIED REQUESTS SHOULD BE A LAST RESORT AND SHOULD BE COORDINATED WITH HQ ACC/SPIP BEFORE FURTHER PROCESSING.)

d. Incident and Background:

(1) Details of Incident: Give brief description of incident(s) location, time(s) occurred, law enforcement agencies involved.

(2) Local Publicity: (is) (is not) expected. (If publicity is expected, specify to what extent.)

(3) Security Information File (SIF): An SIF (has) (has not) been established. The individual's access to classified information (has) (has not) been suspended. In addition, the individual's unescorted entry into restricted areas (has) (has not) been withdrawn.

(4) Security Forces Records Check: A check of local security police records revealed the member (was) (was not) the subject of previous offenses. (If prior offenses exist, then provide the details, such as:)

DATE	OFFENSE	ACTION TAKEN
DD/MM/YY	Crime Committed	LOC/LOR/Article 15/etc

(5) Unit Personnel Information File (PIF): A review of the individual's PIF revealed the member (was) (was not) the subject of previous disciplinary or administrative actions. (If such information exists, then provide the details, such as:)

DATE	MATTER/ISSUE	ACTION TAKEN
DD/MM/YY	Reason for action	LOC/LOR/Article 15/

e. Proposed Disciplinary/Administrative Action:

(1) For court-martials, include the highest courts-martial possible; the type of courts-martial contemplated; the UCMJ article(s) violated; the charges and specifications; the maximum sentence possible; any data as to the individual's physical restraint; and any other circumstances that could affect the outcome of the trial, such as a pretrial agreement to limit the sentence, a request for immunity, or a resignation in lieu of trial.

(2) For administrative discharges, include the worst possible characterization of service; the type of discharge contemplated; the specific regulatory provision being cited as the basis for discharge; the reason for discharge; and any civil court action pending as a result of the misconduct.

(3) In either above situation, coordinate the requested data with the servicing Staff Judge Advocate's office.

f. Commander's Evaluation of Information: The type of information for which the member was authorized access (is) (is not) perishable. (If not perishable, provide a statement as to the impact of such information on national security or any other factors warranting special consideration.)

g. Commander's Assessment of Member:

(1) The member has a (low) (average) (high) ability to comprehend and remember details.

(2) The member (is) (is not) subject to potential blackmail, defection, or exploitation. (If answered in the affirmative, then provide specific details.)

(3) The member (does) (does not) harbor any bitterness or resentment as a result of the proposed adverse action. (If answered in the affirmative, then provide specific details.)

(4) The member (will) (will not) continue to protect classified information. (If answered in the negative, then provide specific details.)

(5) Other Pertinent Matters: (If none, so state. Evaluate the following when answering this item:)

(a) Any attempts by member to expand access to classified information by repeatedly volunteering for special assignments which would require additional access, or inquiring about classified information about which the individual has no need-to-know.

(b) Unauthorized removal of classified material from the work place.

(c) Any documents charged or signed out to the individual that could not be accounted for during annual inspections.

(d) Repeated or unusual overtime.

(e) Falsifying destruction records.

(f) Sudden unexplained affluence.

(g) A pattern of recurring travel, either in the US or abroad, without apparent recreation or business purposes.

(h) Falsifications of locations visited on either leave statements or travel vouchers.

(i) Repeated associated with non-US citizens, regardless of nationality.

(j) Any known financial problems.

(k) Any known medical problems.

2. If you should have any further questions, please contact Rank Last Name, Squadron/Office Symbol, DSN 000-0000.

3. This communication contains "FOR OFFICIAL USE ONLY (FOUO)" information that must be protected under the Privacy Act of 1974 (see AFI 33-332, *Privacy Act Program*). Do not release outside of DoD channels without consent of the originator's office. If you received this communication in error, please notify the sender immediately.

Commander's Signature Block

Attachment 4
SIOP-ESI SECURITY CLEARANCE REQUEST

COMPANY NAME (If Subcontractor, identify to who)
Bldg #, Room #
Offutt AFB NE 68113

POC: Last, First Phone Number:

"FOR OFFICIAL USE ONLY"

In compliance with the Government's directive in the National Industrial Security Program dated January 1995, we are required to have a system for limiting personnel security clearances. Your signature indicates that this clearance is necessary.

Type of Action: _____New Request _____Revalidation _____Upgrade _____Transfer

Frequency of Access: _____Daily _____Weekly _____Monthly

1. Location where SIOP-ESI Information will be accessed:
2. Company Name:
3. Name: LAST, First, Middle
4. SSAN:
5. Date of Birth: YYYYMMMDD
6. Place of Birth: City, State
7. Citizenship of Applicant:
8. Citizenship of Spouse:
9. SIOP-ESI Category:
10. Top Secret/SSBI: Investigation Date: YYYYMMMDD Clearance Date: YYYYMMMDD
11. Contract Number/Name:
12. Employee's job title/specific description of duties: for which employee will require access. Responsible for...
13. Justification: Provide appropriate justification for access to SIOP-ESI
14. Impact if SIOP-ESI denied: If SIOP-ESI access is not granted…
15. Inclusive dates: Present date through not to exceed three years OR past their five-year mark of current investigation date not exceeding three years.
16. Remarks: Include if the individual has submitted a SSBI-PR and the date of submission; other extenuating circumstances pertaining to the individual.
17. This communication contains "FOR OFFICIAL USE ONLY (FOUO)" information that must be protected under the Privacy Act of 1974 (see AFI 33-332, *Privacy Act Program*). Do not release outside of DoD channels without consent of the originator's office. If you received this communication in error, please notify the sender immediately.

Supervisor _____ Date
Signature/Printed Name, Organization, Phone No.

Project Manager _____ Date
Signature/Printed Name, Organization, Phone No.

Requesting Official _____ Date
Signature/Printed Name, Organization, Phone No.

J0502 _____ Date
Signature/Printed Name, Organization, Phone No.

J050 _____ Date
Signature/Printed Name, Organization, Phone No.

SIOP-ESI Screening Interview

Last, First, MI _____ SSAN _____ Date _____

1. Are you now or have you ever been a member of any organization associated with or contributed to any movement or group that advocates the overthrow of the U.S. Government?	Yes	No
2. Are you or have you ever been a dual citizen of the U.S. and another country?	Yes	No
3. Are any of your immediate family members not a U.S. citizen? (Immediate family members are spouse, cohabitant, parents, siblings, and children)	Yes	No
4. Do you or any immediate family members have foreign property or foreign financial interests?	Yes	No
5. Have you ever experienced financial difficulties that resulted in bankruptcy, repossession, tax lien, wage garnishment, judgment, or collection accounts?	Yes	No
6. Have you ever had any alcohol-related arrests, treatment, or counseling?	Yes	No
7. Have you ever illegally used, possessed, bought, sold, or transferred any narcotic, depressant, stimulant, hallucinogen, cannabis, or any other illegal drug or controlled substance?	Yes	No
8. In the last seven years, have you consulted with a mental health professional (psychiatrist, psychologist, counselor, etc.) or have you consulted with another health care provider about a mental health related condition? (For yes answers, request interviewees provide dates of treatment, name and address of mental health professional. Do not report on marital, family, or grief counseling, not related to violence by interviewee.)	Yes	No
9. Have you ever been charged with or convicted of any felony offense?	Yes	No
10. Are there currently any charges pending against you for criminal offense(s)?	Yes	No
11. Have you ever been the subject of an inquiry involving the loss or mishandling of classified information or material?	Yes	No
12. Have you ever been denied a security clearance?	Yes	No
Interviewee will be asked to provide a narrative explanation (attach a memo to this questionnaire) for all "yes" answers. If interviewee declines to provide such information, the interviewer must make it clear this may slow the adjudicative process and delay access. Individual may need to provide a signed copy of their PR submission paperwork upon request.		
I have answered all questions to the best of my knowledge. I have not intentionally provided any incorrect or misleading information. _____ _____ Signature Date		

Authority: 10 U.S.C. 8013, Secretary of the Air Force and E.O. 9396 (SSN)
Purpose: SSN is required to validate personnel identity in order to conduct the required investigation commensurate with clearance and access requirements.
Routine Uses: Those disclosures permitted under 5 U.S.C. 552 a(b) pf the Privacy Act
Disclosure: Disclosure is voluntary. Failure to provide the SSN data or other personal data could result in individual being determined ineligible for security clearance and access.

Attachment 5
SAMPLE REQUEST FOR WAIVER LETTER

DEPARTMENT OF THE AIR FORCE
HEADQUARTERS, 55TH WING (ACC)
OFFUTT AIR FORCE BASE, NEBRASKA

MEMORANDUM FOR 55 WG/CC

FROM: (Unit of Assignment)

SUBJECT: Request for Waiver of Access Criteria

1. In accordance with Chairman, Joint Chiefs of Staff Instruction 3231.01A, *Safeguarding the Single Integrated Operational Plan*, this request for waiver is submitted to permit the below individual access to Single Integrated Operational Plan-Extremely Sensitive Information (SIOP-ESI) pending completion of the required personnel security investigation.

2. Name: (Name of personnel requiring interim access to SIOP-ESI)

3. Impact: Impact statement (Reason that individual must have interim access to SIOP-ESI)

4. The following additional information is provided: (any pertinent additional information that the granting authority should be aware of)

a. The member is assigned to a position that requires permanent access to SIOP-ESI.

b. The member possesses an interim Top Secret security clearance, granted on (date interim granted).

c. The Defense Security Service has opened a request for Single Scope Background Investigation on (date investigation was posted to DSS as received)

5. If you have any further questions, please contact (unit of assignment) at (Phone #) or e-mail at (e-mail address).

Commander's Signature Block
(Unit of Assignment)

Attachment 6
BRIEFING FOR ACCESS TO THE SINGLE INTEGRATED OPERATIONAL PLAN (SIOP)- EXTREMELY SENSITIVE INFORMATION (ESI)

1. GENERAL: This information is presented for the purpose of briefing personnel who will have access to SIOP. The term SIOP-ESI stands for Single Integrated Operational Plan-Extremely Sensitive Information and refers to material of such a nature that its disclosure to unauthorized persons could seriously degrade the effective execution of the SIOP.

2. CLASSIFICATION OF SIOP DOCUMENTS: All SIOP-ESI documents must be classified Top Secret.

3. SIOP MATERIAL: SIOP material is any recorded information that is part of the Joint Chiefs of Staff (JCS) SIOP or is derived from, or published in support of the SIOP. This includes:

a. Written material, whether printed, typed or handwritten.

b. Painted or drawn material.

c. Electronic, optical, or magnetic recordings, punch cards, or paper tape.

d. Sound recordings.

e. Data processed by photogenic media.

f. Reproductions of the above items.

g. Materials used in the reproduction of the above items.

4. SECURITY CLEARANCE REQUIREMENTS:

a. Military, DOD Civilian, and contractor personnel who require access to SIOP-ESI material must be US citizens, and possess a final Top Secret Clearance based on a favorable Single Scope Background Investigation (SSBI).

b. Military and DOD civilian may obtain a waiver to the investigative requirements if they possess a Top Secret clearance based on a favorable Background Investigation (BI). The 55 WG/Commander grants this waiver. Contact 55 SFS/SFA for other waiver considerations.

5. ACCESS TO SIOP-ESI INFORMATION:

a. The 55 WG/CC is the granting authority for access to SIOP-ESI for individuals subject to military, OPM, or DOD personnel policies, and delegates this authority to 55 WG/CV,

/CG/LG/OG/MDG/MSG Commanders. Each authorized access granting authority must have the required categories of SIOP-ESI prior to exercising their authority.

b. Each person who is granted access to SIOP-ESI must be briefed as required by MJCS 75-87.

6. SIOP-ESI MARKINGS:

a. SIOP-ESI documents must be marked according to DOD 5200.1-R. The indicator "SIOP-ESI" is not a form of security classification, but is a device to identify extremely sensitive Top Secret SIOP information.

b. SIOP-ESI cover or title pages must carry a conspicuous marking (hand stamped, hand printed, or printed, but not typed). The AF Form 144, Top Secret Access Record and Cover Sheet, must also bear this marking. The marking must be annotated on the bottom of the front cover and on the first or title page of each major component (basic letter, attachment, annex, appendix, etc.) that contains SIOP-ESI information.

7. SECURITY HAZARDS: If you see or hear someone compromising SIOP information or any classified information, ensure that you notify your immediate supervisor or security manager. If compromise of SIOP-ESI material occurs or is suspected immediately notify the 55 SFS/SFAI (extension 294-5252).

8. REPRODUCTION: Reproduction of SIOP-ESI material is severely restricted and is only authorized by special permission of the JCS.

9. EXTRACTION AND DISSEMINATION: Extraction of a SIOP-ESI document is permitted only on a highly selective basis. When an extract of a SIOP-ESI document is made, or any portion of it reproduced, it must be determined whether the extract or reproduction is still classified as SIOP-ESI.

10. PACKAGING: The inner wrapping of any package that contains SIOP-ESI documents must be stamped "SIOP-ESI". The outer wrapping of any package that contains SIOP-ESI material must carry the notation, "Restricted Handling Required."

11. TRANSMISSION: SIOP-ESI information is transmitted only by secure electrical transmission, by armed forces courier service, by two couriers with a final Top Secret clearance based on a SSBI, airlifted by US Military Aircraft or by U.S. commercial non-passenger cargo aircraft, or by SIOP-ESI cleared individuals when transmitted between offices on the same installation.

12. INVENTORY REQUIREMENT: All SIOP-ESI material must be inventoried semi-annually and on change of custodian.

13. SIOP-ESI CUSTODIAN: Each unit commander or staff agency chief who has SIOP-ESI documents or access authorizations will appoint a unit or staff agency SIOP-ESI Program Manager for managing requirements of this instruction.

14. DESTRUCTION: When a SIOP-ESI document is superseded or no longer required, it must be destroyed by officials authorized access to the specific categories being destroyed.

15. CONCLUSION: This concludes the briefing, do you have any questions?

Attachment 7
GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

References

(a) EO 12958, *National Security Information*, 14 Oct 95
(b) DoD 5200.1-R, *DoD Information Security Program*, Jan 97
(c) DoD 5200.2-R, DoD Personnel Security Program, Jan 87
(d) CJCSI 3231.01, Safeguarding the Single Integrated Operational Plan, 30 Nov 93
(e) AFI 10-1102, Safeguarding the Single Integrated Operational Plan, 15 Jul 02
(f) AFI 31-401, Information Security Program Management, 1 Nov 05
(g) AFI 31-501, Personnel Security Program Management, 27 Jan 05
(h) AFI 31-601, Industrial Security Program Management, 29 Jun 05

Abbreviations and Acronyms

OPM--Office of Personnel Management
OPR--Office of Primary Responsibility
SIOP--Single Integrated Operational Plan
ESI--Extremely Sensitive Information
SSBI--Single Scope Background Investigation