



*Security*

**PERSONNEL SECURITY PROGRAM  
MANAGEMENT**

---

**NOTICE:** This publication is available digitally on the PACAF WWW site at: <http://www.hqpacaf.af.mil/publications>. If you lack access, contact your Publishing Distribution Office (PDO).

---

OPR: HQ PACAF/SFI  
(CMSgt Michael A. Caporaletti)

Certified by: HQ PACAF/SFI  
(Mr Berry B. Rigdon)

Pages: 33

Distribution: F

---

This pamphlet will assist commanders, security managers, personnel security specialists, and supervisors to better understand and effectively manage two vital personnel security management programs; security information files (SIF) and the limited access authorization (LAA) program. The pamphlet also contains a self-assessment checklist for the two programs. If a conflict occurs between this pamphlet and program directives, follow DoD 5200.2-R or AFI 31-501 guidance. **Attachment 1** contains a users' feedback worksheet to improve the pamphlet. This pamphlet does not apply to Air National Guard or Air Force Reserve forces.

<b>Chapter 1— SECURITY INFORMATION FILES (SIF)</b>	<b>3</b>
1.1. General SIF Information. ....	3
1.2. Frequently Asked Questions. ....	3
1.3. Functional Responsibilities and the SIF Process. ....	5
1.4. Self-Assessment Checklist. ....	9
Figure 1.1. AFI 31-501 and DoD 5200.2-R Security Clearance Eligibility Criteria. ....	12
Figure 1.2. Sample SIF Establishment Memorandum (Unit Commander to the CSF). ....	13
Figure 1.3. Sample SIF Establishment Checklist. ....	15
Figure 1.4. Sample Evaluation of Continued Security Clearance Eligibility Memorandum. ....	17
Figure 1.5. Sample 497 IG/INS Notification Memorandum (Person Maintains Access). ....	18
Figure 1.6. Sample SIF Memorandum (Commander to SIF Recipient – Access Suspended). ....	19
Figure 1.7. Sample Request for Review and Written Opinion Memorandum. ....	20
Figure 1.8. Sample SIF Establishment Notification Memorandum (CSF to Unit Commander). ....	21
Figure 1.9. Sample SIF Transfer Memorandum (SF PSO to Gaining SF PSO). ....	22

Figure 1.10. Sample SIF Closure Recommendation Memorandum. .... 23

**Chapter 2— LIMITED ACCESS AUTHORIZATION (LAA) PROGRAM 25**

    2.1. General LAA Information. .... 25

    2.2. LAA Program Requirements and the LAA Process. .... 25

    2.3. LAA Self-Assessment Checklist. .... 28

Figure 2.1. Sample Memorandum for Initial LAA Pre-Approval. .... 29

Figure 2.2. Sample Memorandum for LAA Annual Recertification. .... 30

Figure 2.3. Sample Memorandum for LAA Termination. .... 32

**Attachment 1—USERS' FEEDBACK 33**

## Chapter 1

### SECURITY INFORMATION FILES (SIF)

#### 1.1. General SIF Information.

1.1.1. There are three essential elements of personnel security program management; personnel security investigations (PSI), the continuous evaluation process, and SIFs. By far, the continuous evaluation and SIF processes are the most misunderstood and could be the program's weakest link in protecting classified information. Why? Both involve the human factor and often receive the least amount of attention. Commanders and supervisors need to understand the importance of the continuous evaluation and SIF processes to ensure the national security balance stays in our favor. The most secure safes and vaults do little to protect our classified information if one of our people takes classified information home with the intent to sell it or give it away. When is the last time you heard about a security container break-in? We know of only one documented DoD security container break-in case. On the other hand, how often do we hear about a "cleared" person being charged with espionage or unauthorized disclosure of classified information? In most cases, a well developed and managed continuous evaluation program can prevent SIF establishment and associated program problems.

1.1.2. What constitutes an effective continuous evaluation program?

- Active commander and supervisor involvement with their people, both on and off-duty.
- Sincere program emphasis by senior installation leadership, unit commanders, supervisors, and security managers.
- Effective security education, training, and awareness programs.
- Everyone's knowledge of established information and personnel security program management procedures and methods to report unauthorized activities and practices.
- Timely personnel security investigation submissions.
- Decisive and timely actions when program infractions occur.

1.1.3. This chapter provides commanders and supervisors insight into the administrative process required when an incident occurs affecting the trustworthiness, loyalty, reliability, or judgment of one of their people. Reporting the incident to the commander is the first step; the next step is critical in completing the process – whether or not to establish a SIF. This chapter gives commanders and supervisors the necessary management tools to make the appropriate decision. Also, it answers the most frequently asked SIF questions, assigns functional responsibilities for everyone involved in the SIF process, explains the SIF process from inception to final adjudication, and provides commanders and supervisors with a self-assessment checklist to monitor the status of their program.

#### 1.2. Frequently Asked Questions.

**1.2.1. What Is A SIF?** A collection of documents generated as a result of the discovery or development of *unfavorable* information having a bearing on a person's judgment, loyalty, reliability, or trustworthiness with respect to eligibility for access to classified information and/or special compartmented information (SCI) access. (AFI 31-501, para 8.1)

**1.2.2. What Is The Purpose Of A SIF?** It serves as a repository for unfavorable information to determine the need for further investigative, administrative, or adjudicative actions. (AFI 31-501, para 8.1)

**1.2.3. Who Can Establish A SIF?** A commander, chief of staff agency (MAJCOM or Numbered Air Force directorate), supervisor (for civilians not assigned to military units), or by the central adjudication facility (the 497 IG/INS) as a result of a PSI conducted by Defense Investigative Service (DIS), Office of Personnel Management, or other investigative agencies, e.g., AFOSI, DIA. (AFI 31-501, para 8.1)

**1.2.4. Who Do Commanders Have Authority Over For Establishing A SIF?** All people they have jurisdiction over, including tenant or geographically separated units and TDY personnel. (AFI 31-501, para 8.2.1.2)

**1.2.5. How Long Does the Commander Normally Have To Determine If A SIF Should Be Established?** Twenty days; ASAP if it pertains to Sensitive Compartmented Information (SCI) program access. (AFI 31-501, para 8.2.1.3) *Note: If the commander has sufficient reason to doubt the validity of unfavorable information, the decision to establish a SIF and notification to 497 IG/INS may be extended to 45 days.*

**1.2.6. Is There A Time Limit For Submitting SIFs To The 497 IG/INS?** Yes, 120 days from the date the commander determines to establish a SIF. (AFI 31-501, 8.2.2.7)

**1.2.7. Who Can Close A SIF Once It Is Formally Established?** Only the 497 IG/INS.  
(AFI 31-501, para 8.2.1.3)

**1.2.8. Does A Person Automatically Lose Their Security Clearance Eligibility And Access To Classified Information When A SIF Is Established?** Not necessarily, the commander determines whether or not to suspend access (and unescorted restricted area entry) after reviewing all aspects of the case. Also, commanders are responsible for making their recommendation concerning the person's security clearance eligibility when submitting the SIF to the 497 IG/INS (AFI 31-501, para 8.2.1.4)

**1.2.9. Should A SIF Be Established For Incidents Involving Poor Duty Performance, Failure To Comply With Weight Standards, Minor One-Time Alcohol Related Incidents?** Not normally, commanders have other administrative and management tools to address and correct these problems. (AFI 31-501, 8.2.1.3.2)

**1.2.10. When Should A SIF Be Established?** When a person's activity, conduct, or behavior is inconsistent with the security criteria specified in AFI 31-501, Chapter 8, or DoD 5200.2-R, para 2-200 and Appendix I. **Figure 1.1.** provides criteria for circumstances that could warrant SIF establishment.

**1.2.11. Can Commanders Revoke A Person's Security Clearance?** No, only the 497 IG/INS can accomplish this. Commanders are responsible for controlling the person's access to classified information and making recommendations about the person's security clearance eligibility, e.g., suspend, reinstate, revoke. (AFH 31-502, para 1.1.1 and 2)

**1.2.12. Can The Commander Recommend A Person's Access to Top Secret Be Suspended, But Allow Continued Access To Lower Levels of Classified Information, e.g., Secret Information?**

No, once the commander makes the determination to suspend the person's access, access to all classified information must be suspended. (AFI 31-501, para 8.2.1.4)

**1.2.13. Is It Necessary To Establish A SIF If The Person Will Soon Be Discharged Or Separated From The Military?** Yes, SIF establishment will “flag” the person's records in the event he/she seeks federal employment after retiring or separating from military service.

**1.2.14. Normally, What Is The Time Period A Person's Security Clearance Eligibility Is Revoked For?** Two years. (AFI 31-501, para 8.12)

### 1.3. Functional Responsibilities and the SIF Process.

**1.3.1. Unit Commander & Staff Agency Chief Responsibilities.** Unit commanders and staff agency chiefs (hereafter referred to as the “commander”) are the key ingredient to SIF program success and protecting classified information vital to our national defense. The unit commander's decision whether or not to establish a SIF has historically been the hardest part of the SIF process. Unit commanders need to take a proactive approach to the continuous evaluation process and not wait for notification of unfavorable actions from the base information security program manager (ISPM) (also known as the Chief of Security Forces – CSF) concerning one of their assigned people. Waiting for security forces' notification delays SIF disposition actions and increases the administrative paperwork load.

1.3.1.1. Although the unit commander must review each incident on a case-by-case basis and at times, make a tough decision, AFI 31-501 and DoD 5200.2-R provide criteria for granting and maintaining security clearance eligibility (**Figure 1.1.**). After reviewing the criteria, commanders should weigh the incident against *four* factors: the seriousness of the incident, the person's motivation, whether it was out of character for the person, and the likelihood of the incident recurring. Commanders are encouraged to consult with the base ISPM and legal office before making a final decision whether or not to establish a SIF. When in doubt, commanders should establish a SIF – it is a lot easier for commanders to go through the administrative process of opening and closing a SIF than the work and embarrassment of going through the process of an investigation into the unauthorized disclosure of classified information. Establishing a SIF is not an adverse or disciplinary action; it's simply an administrative process taken by commanders until they can effectively evaluate all circumstances involving an incident affecting a person's security clearance eligibility.

1.3.1.2. Effectively managing the personnel security program for assigned people is an inherent responsibility of command and has far-reaching effects on protecting information vital to our national security. The rationale of “If I suspend the person's access to classified information and unescorted entry privileges to restricted areas, I can't get the mission done” should not weigh in the factor to establish a SIF or not – national security is the paramount consideration.

1.3.1.3. Commanders should accomplish the following to establish a SIF:

- Render a decision whether or not to establish a SIF within **20** days of receiving unfavorable information – ASAP if Sensitive Compartmented Information (SCI) is involved. *Note: If the commander has sufficient reason to doubt the validity of unfavorable information, the decision to establish a SIF and notification to 497 IG/INS can be extended to 45 days.*

- Consult with the base ISPM (the Chief of Security Forces) and legal office. Consultation with the base ISPM is very important because the SIF could impact or compromise an ongoing security forces or AFOSI investigation.
- Interview the person and inform him/her of your decision whether or not you will establish a SIF. Ensure the person is aware of his/her appeal, due-process, and legal rights (refer to AFI 31-501). Follow up the interview with written notification to the person within *three* duty days; the notification should include all restrictions associated with the SIF establishment, e.g., suspension of access to classified information, removal of unescorted entry privileges.
- Determine if access to classified information and unescorted entry to restricted areas should be suspended. If so, establish positive control measures to prevent unauthorized access to classified information and unescorted restricted area entry. e.g., retrieve the person's restricted area badge, remove the person from access lists. *Note: The decision to suspend access and unescorted restricted area entry should be based on a thorough review of all facts and an assessment of the risk to national security.*
- Ensure the person's supervisor is an integral part of the SIF process.
- Direct and ensure the person receives assistance and counseling, as necessary, from base support agencies, e.g., mental health, legal office, family support center.
- Work and confer with base support agencies to obtain evaluation reports and relevant documentation, e.g., medical, investigative. Follow [Figure 1.7](#). Sample Memorandum for Requests for Review and Written Opinion.
- Notify the installation chief of security forces (CSF) and installation commander, in writing, of your intention to establish a SIF. The memorandum must include a recommendation whether to grant, deny, or revoke the person's security clearance eligibility. Subsequent and follow-up correspondence should be sent to the security forces personnel security office (SF PSO). A sample Initial SIF Establishment Memorandum is at [Figure 1.2](#).
- Immediately notify the installation special security officer (SSO) if the person has SCI access. *Note: The SSO is responsible for managing the SIF program for people having SCI access.*
- Coordinate SIF actions with the applicable installation or MAJCOM special access program (SAP) managers if the person is indoctrinated into a SAP. *Note: Do not initiate SIF actions (suspend access, etc.) until the SAP manager provides guidance. AFI 16-701, "The US Air Force Special Access Programs," provides guidance for SAP due-process procedures.*
- Forward required SIF related correspondence to the SF PSO in a timely manner. A very important factor for correspondence is to ensure decisions are fully justified, e.g., why the person should retain his/her security clearance. Also, ensure your recommendations for SIF disposition actions are consistent with other base support agency inputs, e.g., medical evaluations/recommendations, commander and supervisor recommendations.
- Submit the SIF Establishment Checklist ([Figure 1.3](#)) to the SF PSO. Failure to complete all checklist actions could result in 497 IG/INS adjudication delays.

**NOTE:**

Historically, the failure to submit AFOSI reports with the SIF have delayed the

*497. IG/INS final adjudication process. The 497 IG/INS SIF Program Manager does not send the SIF to the assigned adjudicator until all documentation is received and is ready for processing.*

- Keep the SF PSO informed of SIF related issues, e.g., feedback from base agencies (clinic, social actions, etc.), status of investigations. Ensure SIF suspenses are met or request an extension through the SF PSO. The SF PSO, through the ISPM, can grant extensions when unusual circumstances exist.
- Notify SF PSO when the SIF recipient changes duty stations, receives separation or discharge orders, etc.
- Protect SIFs and associated information in accordance with the Privacy Act of 1974.
- Follow the sample memorandum formats (**Figure 1.4.** through **Figure 1.10.**) for preparing and processing SIF correspondence.

1.3.1.4. SIF Closure Process. Normally, commanders would request favorable SIF closure for one of the following reasons.

- The person successfully completes program rehabilitation or counseling, and in view of the commander and favorable program evaluations/recommendations is capable of meeting security clearance eligibility standards.
- An investigation reveals the person was falsely accused. In this case, forward a coordinated priority message from your office and the ISPM to 497 IG/INS.

1.3.1.4.1. Commanders should accomplish the following to favorably close a SIF.

- Interview the person (and his/her supervisor) and inform them of your decision to close the SIF.
- Obtain a written recommendation from the person's supervisor.
- Review "Request for Review and Written Opinion" from base support agencies involved in the person's SIF evaluation and/or counseling program.
- Forward closure requests to SF PSO with detailed justification and appropriate documentation (evaluation/counseling recommendations) from base support agencies. Ensure all documents that supported SIF inception are included in the case file, e.g., medical evaluation, AFOSI reports, supervisor's recommendation. An important factor to successfully close SIFs in a timely manner is to ensure base support agency evaluation and recommendations are consistent with the commander's recommendation. As a reminder, the primary purpose of evaluations and recommendations is to attest to the person's trustworthiness, loyalty, judgment, and reliability in regards to security clearance eligibility – ensure this is accurately captured! Ask yourself one question before submitting the request, "If I was the 497 IG/INS adjudicator, would I have sufficient information to accurately determine the person's security clearance eligibility status?" If the answer is yes, your request is probably ready for processing and adjudication. *Note: Incomplete and inconsistent (conflicting) documentation are the leading cause for SIF processing delays and final adjudication actions.*

### 1.3.2. Base Information Security Program Manager (ISPM) – CSF Responsibilities.

- Provide installation program oversight and technical expertise. The ISPM should brief unit commanders at least *semi-annually* on the SIF program. As a minimum, the briefing should include; program importance, responsibilities, trends, and any other associated information to enhance the program.
- Maintain current installation SIF information – brief installation and unit commanders when trends reveal a significant increase in SIF establishments and their contributing causes, e.g., trustworthiness, use of illegal substances, sexual misconduct.
- Ensure unit commanders are notified when unfavorable information is received from security forces or AFOSI channels (DD Form 1569, AFOSI reports of investigation, etc.) on one of their assigned people.
- Ensure local and 497 IG/INS program suspenses are met.
- Coordinate SIF establishment with the local or supporting AFOSI detachment to ensure the process will not interfere with an ongoing investigation.
- Sign initial SIF memorandum correspondence (e.g., to the unit commander, 497 IG/INS).
- Review all SIFs before they are forwarded to the 497 IG/INS.
- Forward SIF conflicts that cannot be resolved to the installation commander.

### 1.3.3. Security Forces Personnel Security Office (SF PSO) Responsibilities.

- The SF PSO is the SIF program manager and liaison between unit commanders and 497 IG/INS.
- Provide initial SIF establishment notification to 497 IG/INS.
- Via message or PT141B (PC-III) if the person's access will be suspended.
- Via memorandum if the person's access will not be suspended.
- Review SIFs to ensure they contain required information, evaluations, and recommendations.
- Forward completed SIFs to 497 IG/INS within **120** days from the date the commander determined to establish the file. Notify 497 IG/INS if circumstances arise requiring an extension. Even though unit commanders forward periodic SIF updates to you (as directed by local policy/instructions), do not submit partial information or fragmented reports to the 497 IG/INS – wait until the SIF is completed.
- Maintain, monitor, and forward (first class mail IAW AF DoD 4525.8-M/AF Supplement) completed SIFs to the 497 IG/INS.
- Ensure the SIF contains a copy of the signed SIF Establishment Checklist (**Figure 1.3**).
- Coordinate SIF establishment with the installation SSO and Special Access Program (SAP) manager.
- Immediately notify unit commanders of 497 IG/INS adjudication decisions. Follow up notification in writing within **three** duty days.
- Safeguard SIFs and related information in locked containers during non-duty hours.
- Protect SIFs and associated information in accordance with the Privacy Act of 1974.
- Monitor ASCAS rosters or SENTINEL KEY to ensure security clearance eligibility decisions are recorded accurately – inform the 497 IG/INS when discrepancies are noted.

- Maintain a SIF record copy until the 497 IG/INS makes a final determination, then destroy the copy.
- Forward SIFs to the gaining SF PSO or security activity when a change of assignment occurs.
- Notify the 497 IG/INS when information results in a discharge, or separation. Forward a copy of the discharge or separation orders or a copy of the SF 50B3PT, *Notification of Personnel Action*, and any additional information used in these actions.
- Notify the 497 IG/INS if a SIF recipient's adverse discharge is overturned and the person returns to active duty.

#### **1.3.4. Security Manager Responsibilities.**

- Manage the unit's personnel security program, placing special emphasis on the continuous evaluation process.
- Keep the SF PSO updated on all SIF disposition actions.
- Ensure unit ASCAS rosters reflect accurate security clearance data; notify the SF PSO when discrepancies are noted.

#### **1.3.5. 497 IG/INS Responsibilities.**

- Adjudicates SIF information and makes a final security clearance eligibility determination.
- Requests Special Investigative Inquiries (SII) from DIS, when required.
- Forwards eligibility notifications to unit commanders (through the SF PSO) and enters the person's eligibility status in the Defense Clearance and Investigations Index (DCII).
- Initiates and manages due-process procedures when security clearance eligibility and/or access is denied, revoked, or suspended.
- Establishes SIFs when unfavorable information is received from other government agencies, court-martial orders, DIS information summary reports, AFOSI reports of investigation, and notification of SAP denial from various access granting authorities. Notifies commanders for further actions, when necessary.
- Maintains SIFs when military and civilians retire or separate from the service.

**1.3.6. DIS Responsibilities.** Conducts PSIs and forwards results to the 497 IG/INS for adjudication.

**1.3.7. AFOSI Responsibilities.** Conducts PSI leads in overseas areas for DIS. A table of offenses the AFOSI and security forces investigate is available in AFI 71-101v1, *Criminal Investigations*.

### **1.4. Self-Assessment Checklist.**

1.4.1. Are unit commanders, security managers, and supervisors knowledgeable of their responsibilities regarding SIFs? (AFI 31-501 and AFH 31-502)

1.4.2. Is a SIF established when a person's activity, conduct, or behavior is inconsistent with the security criteria listed in DoD 5200.2-R, para 2-200 and Appendix I, and AFI 31-501, para 8.2.1.3.1?

1.4.3. Does the unit commander determine whether or not to establish a SIF, on a case by case basis, within **20** days of receiving unfavorable information? (AFI 31-501, para 8.2.1.3)

**NOTE:**

If the commander has sufficient reason to doubt the validity of unfavorable information the decision to establish a SIF and notification to 497 IG/INS may be extended to 45 days.

1.4.4. Does the commander base a SIF establishment decision on the seriousness of the incident, the person's motivation, whether it was out of character for the person, or whether the undesirable conduct of behavior is likely to continue? (AFI 31-501, para 8.2.1.3)

1.4.5. Do unit commanders consult with the installation security program manager (ISPM) and base legal office before establishing a SIF? (AFI 31-501, para 8.2.1.3)

1.4.6. Does the unit commander determine whether or not to suspend access to classified information and unescorted entry to restricted areas when establishing a SIF? The determination should be based on a thorough review of all facts and an assessment of the risk to national security. (AFI 31-501, para 8.2.1.4)

1.4.7. Do unit commanders ensure the SSO and SAP manager are notified when SCI/SAP access is involved in the SIF/access suspension process? (AFI 31-501, para 8.2.1.4)

1.4.8. Are commanders aware of procedures to follow when the person is indoctrinated or working in a special access program? (AFI 31-501, para 14)

1.4.9. Does the unit commander ensure a recommendation whether to grant, deny, or revoke the person's security clearance eligibility and/or SCI access (if applicable) is in the completed SIF? Documented facts must *fully* support the recommendation. (AFI 31-501, para 8.2.1.6)

1.4.10. Are unit commanders knowledgeable of procedures to close a SIF when special circumstances exist (e.g., a person is falsely accused)? AFI 31-501, para 8.2.1.7

1.4.11. Does the SF PSO (SSO when SCI is involved) provide unit commanders with appropriate guidance for establishing SIFs? AFI 31-501, para 8.2.2.1)

1.4.12. Does the personnel security office establish, maintain, monitor, and forward SIFs to the 497 IG/INS? If SCI access is involved, forward the SIF through the MAJCOM or activity SSO. (AFI 31-501, para 8.2.2.2)

1.4.13. Are SIFs forwarded to the gaining SF PSO when a change of assignment occurs? (AFI 31-501, para 8.2.2.2)

1.4.14. Does the SF PSO notify the 497 IG/INS via message or PTI14B upon establishing a SIF? Use a message or memorandum in lieu of the PTI14B when the person will be permitted to have access to classified information. (AFI 321-501, para 8.2.2.4)

1.4.15. Is 497 IG/INS notified when unfavorable information results in a discharge, retirement, or separation? (AFI 31-501, para 8.2.2.24)

1.4.16. Does the SF PSO forward a copy of discharge or separation orders or a copy of the SF 50B3PT, *Notification of Personnel Action*, to the 497 IG/INS when unfavorable information results in a discharge, retirement, or separation? (AFI 31-501, para 8.2.2.24)

1.4.17. Does the initial SIF notification to the 497 IG/INS include the person's full name, SSAN, security clearance eligibility, date SIF established, reason, and if access has/has not been withdrawn. (AFI 31-501, para 8.2.2.4)

1.4.18. Is there a viable process for the SF, SSO, and/or SAP community to coordinate and exchange SIF information? (AFI 31-501, para 8.2.2.4)

1.4.19. Do SIFs contain evaluations and relevant documentation from the following agencies (as applicable)? (AFI 31-501, para .2.2.5)

- **Commander, Military Personnel Flight** (UIF, performance report summary, and other personnel action required as a result of the person's behavior).
- **Security Force** (criminal activity or other pertinent information regarding the subject's police records, to include involvement in previous information security program violations).
- **Judge Advocate** (determines if court proceedings or nonjudicial punishment is legally supportable)
- **Surgeon General** (physical, mental, and emotional state that may affect the person's ability to protect classified information)
- **Social Actions** (involvement, previous or present, with alcohol or illegal/illicit drugs which may indicate a security weakness)

1.4.20. Does the ISPM ensure all supporting documentation is included in the SIF before sending it to the 497 IG/INS? (AFI 31-501, para 8.2.2.6)

1.4.21. Are completed SIFs forwarded to the 497 IG/INS within **120** days? (AFI 31-501, para 8.2.2.7)

1.4.22. Are SIFs forwarded to 497 IG/INS via first class mail? (AFI 31-501, para 8.2.2.7)

1.4.23. Are SIF record copies maintained by the personnel security office until the 497 IG/INS makes a final determination? The SF record copy is destroyed as soon as the 497 IG/INS makes their final disposition decision. (AFI 31-501, para 8.2.2.8)

1.4.24. Does the unit's ASCAS reflect appropriate 497 IG/INS security clearance disposition status once a SIF is established? (AFI 31-501, para 8-10.6)

1.4.25. Are unit commanders knowledgeable of unfavorable administrative action, appeal, and due process procedures when one of their assigned people has their security clearance suspended or revoked? (AFI 31-501, para 8.10.1 through 8.10.12)

1.4.26. Are unit commanders, ISPMs, security managers, and personnel security specialists knowledgeable of the administrative requirements for submitting SIF correspondence to the 497 IG/INS? See AFH 31-502, Chapter 1, for sample memorandum formats.

1.4.27. Do unit commanders notify subjects, in writing, when a decision has been made to suspend or revoke their security clearance eligibility and access to classified information?

(DoD 5200.2-R, para 2-102b)

1.4.28. Are unit commanders knowledgeable of procedures to take before initiating administrative or disciplinary action when SAP information is involved? (AFI 31-501, para 8.14)

1.4.29. Are SIFs maintained in locked containers during non-duty hours?

(AFI 31-501/PS-1, para 8.6)

- 1.4.30. Do unit commanders, security managers, and supervisors implement procedures/controls to ensure access to classified material is denied when a person's security clearance has been suspended or revoked? (PACAF Pamphlet 31-1, para 1.3.1.3)
- 1.4.31. Does the ISPM coordinate establishment of SIFs with the local AFOSI? (PACAF Pamphlet 31-1, para 1.3.2)
- 1.4.32. Does the ISPM brief installation and unit commanders at least semiannually on the SIF program? (PACAF Pamphlet 31-1, para 1.3.2)

**Figure 1.1. AFI 31-501 and DoD 5200.2-R Security Clearance Eligibility Criteria.**

The following circumstances or incidents would warrant SIF establishment.

- 1.1.1. Refusal to sign the Standard Form 312, *Nondisclosure Statement*. (AFI 31-501, para 8.2.1.3.1)
- 1.1.2. Refusal or failure of a person requiring an investigation or periodic investigation (PR) to provide personnel security questionnaire information or release statements for review of medical, financial, or employment records; refusal to be interviewed in connection with a personnel security investigation (PSI). (AFI 31-501, para 8.2.1.3.1)
- 1.1.3. Incidents of theft, embezzlement, child or spouse abuse, unauthorized sale or use of firearms, explosives or dangerous weapons, or misuse or improper disposition of government property or other unlawful activities. (AFI 31-501, para 8.2.1.3.1)
- 1.1.4. Incidents leading to "permanent" decertification from PRP for other than physical reasons. (AFI 31-501, para 8.2.1.3.1)
- 1.1.5. Commission of any act of sabotage, espionage, treason, terrorism, anarchy, sedition, or attempts to threaten or preparation therefore, or conspiring with or aiding or abetting to commit or attempt to commit any such act. (DoD 5200.2-R, para 2-200a)
- 1.1.6. Establishing or continuing a sympathetic association with a saboteur, spy, traitor, seditionist, anarchist, terrorist, revolutionist, or with an espionage or other secret agent or similar representative of a foreign nation whose interests may be inimical to the interests of the U.S., or with any person who advocates the use of force or violence to overthrow the Government of the U.S. or to alter the form of the Government by unconstitutional means. (DoD 5200.2-R, para 2-200b)
- 1.1.7. Advocacy or use of force or violence to overthrow the Government of the U.S. or to alter the Government of the U.S. by unconstitutional means (DoD 5200.2-R, para 2-200c)
- 1.1.8. Knowing membership with the specific intent of furthering the aims of, or adherence to and active participation in any foreign or domestic organization, association, movement, group, or combination of persons which unlawfully advocates or practices the commission of acts of force or violence to prevent others from exercising their rights under the Constitution or laws of the U.S. or of any State or which seeks to overthrow the Government of the U.S. or any State or subdivision thereof by unlawful means. (DoD 5200.2-R, para 2-200d)
- 1.1.9. Unauthorized disclosure to any person of classified information, or of other information, disclosure which is prohibited by Statute, Executive Order, or Regulation. (DoD 5200.2-R, para 2-200e)

- 1.1.10. Performing or attempting to perform one's duties, acceptance and active maintenance of dual citizenship, or other acts conducted in a manner which serve or which could be expected to serve the interests of another government in reference to the interests of the U.S. (DoD 5200.2-R, para 2-200f)
- 1.1.11. Disregard of public law, statutes, executive orders, or regulations including violation of security regulations or practices. (DoD 5200.2-R, para 2-200g)
- 1.1.12. Criminal or dishonest behavior. (DoD 5200.2-R, para 2-200h)
- 1.1.13. Acts of omission or commission that indicate poor judgment, unreliability, or untrustworthiness. (DoD 5200.2-R, para 2-200i)
- 1.1.14. Any behavior or illness, including any mental condition, which, in the opinion of competent medical authority, may cause a defect in judgment or reliability with due regard to the transient or continuing effect of the illness and the medical findings in such case. (DoD 5200.2-R, para 2-200j)
- 1.1.15. Vulnerability to coercion, influence, or pressure that may cause conduct contrary to the national interest. This may be (1) the presence of immediate family members or other persons to whom the applicant is bonded by affection or obligation in a nation whose interests may be inimical to those of the U.S., or (2) any other circumstances that could cause the applicant to be vulnerable. (DoD 5200.2-R, para 2-200k)
- 1.1.16. Excessive indebtedness, recurring financial difficulties, or unexplained affluence. (DoD 5200.2-R, para 2-200l)
- 1.1.17. Habitual/episodic use of intoxicants to excess. (DoD 5200.2-R, para 2-200m)
- 1.1.18. Illegal or improper use, possession, transfer, sale or addiction to any controlled or psychoactive substance, narcotic, cannabis or other dangerous drug. (DoD 5200.2-R, para 2-200n)
- 1.1.19. Any knowing and willing falsification, cover-up, concealment, misrepresentation, or omission of a material fact from any written or oral statement, document, form or other representation or device used by DoD or any Federal Agency. (DoD 5200.2-R, para 2-200o)
- 1.1.20. Failing or refusing to answer questions or to provide information required by a congressional committee, court, or agency in the course of an official inquiry whenever such answers or information concerns relevant and material matters pertinent to an evaluation of the person's trustworthiness, reliability, and judgment. (DoD 5200.2-R, para 2-200p)
- 1.1.21. Acts of sexual misconduct or perversion indicative of moral turpitude, poor judgment, or lack of regard for the laws of society. (DoD 5200.2-R, para 2-200q)
- 1.1.22. Also, refer to DoD 5200.2-R, Appendix I, for adjudicative guidelines for determining eligibility for access to classified information.

**Figure 1.2. Sample SIF Establishment Memorandum (Unit Commander to the CSF).**

MEMORANDUM FOR (Installation Chief of Security Forces)

FROM: Unit Commander's Address Element

SUBJECT: Request Security Information File (SIF) Establishment, (full name, rank, SSAN)

1. Request your organization initiate actions to establish a SIF on (rank and name).
  
2. I have become aware of (rank and name) involvement in (brief synopsis of situation). After reviewing AFI 31-501, Chapter 8, and DoD 5200.2-R, para 2-200 and Appendix I, I determined that further evaluation is required to determine (rank and name) continuing eligibility for access to classified information and unescorted restricted area entry.
  
3. (Rank and name) has been placed in a non-sensitive position, and access to classified information and restricted area unescorted entry privileges are suspended in accordance with AFI 31-501, **or**

(Rank and name) will continue to have access to classified information and restricted area unescorted entry, pending required program evaluation and professional recommendation. My decision is based on (specific facts with justification)

***Note: Ensure the access to classified information and restricted areas unescorted entry privilege decision is sufficiently justified.***

4. The following SIF associated information and documentation is provided (list as applicable).
  - a. Report of Investigation (ROI) Information: List agency conducting ROI and date of ROI.
  - b. Mental health (will/will not) be conducting an evaluation; (date of referral).
  - c. Subject (was/was not) referred to Social Actions; (date of referral).
  - d. Subject was administered disciplinary action (list type, e.g., reprimand, Article 15).
  - e. A court-martial is projected for (date).
  - f. Subject was placed in appellate leave status on (date)
  - g. Subject's current retirement or separation eligibility date is:
    - h. We (do/do not) intend to discharge subject IAW AFI 36-3206, *Administrative Discharge Procedures for Commissioned Officers*, or AFI 36-3208, *Administrative Separation of Airman*.
  
5. My POC (name and phone number) will keep you advised on the progress of all SIF actions.

Unit Commander's Signature Element

Attachments:

(as applicable, e.g., AF Forms 2583/2586/2587)

cc:

SPTG/CC and Wing/CC

**Figure 1.3. Sample SIF Establishment Checklist.**

MEMORANDUM FOR (Installation Chief of Security Forces)

FROM: Unit Commander's Address Element

SUBJECT: Security Information File (SIF) Establishment Checklist

1. We provide the following SIF information.
  - a. Identification Data.
    - (1) Full Name: Karol A. Cruze
    - (2) Rank: AB
    - (3) SSAN: 123-12-1234
    - (4) Organization and Office Symbol: 15 CEF/CEEF
    - (5) Installation/Country: Hickam AFB HI (USA)
  - b. SIF Establishment Information:
    - (1) Date: 1 Jan 97
    - (2) By: Commander
    - (3) Reason (brief synopsis): Narcotic Possession Charge on 25 Dec 96
    - (4) Source (if appropriate): Local Police Report and AFOSI Report of Investigation
  - c. ASCAS/SENTINEL KEY Data:
    - (1) Clearance: SECRET
    - (2) Security Access Code: 2
    - (3) Investigation Type: ENTNAC
    - (4) Investigation Date: 1 Dec 96
    - (5) Special Access Program: (Yes or No): No
  - d. Check the following questions/requirements with yes, no, or non-applicable (NA). Provide a brief but descriptive explanation for any of the blocks that are marked "no." Use a separate sheet to address the issue – identify the issue with the corresponding paragraph number.

Yes No NA

\_\_\_ \_\_\_ (1) Was the Chief of Security Forces (CSF) consulted before establishing the SIF? *Note: The CSF will coordinate the SIF with the local AFOSI.*

\_\_\_ \_\_\_ (2) Was the base legal office consulted before establishing the SIF?

\_\_\_ \_\_\_ (3) Was the SIF recipient interviewed and briefed on his/her appeal, due-process, and legal rights?

\_\_\_ \_\_\_ (4) Was the interview followed up in **three** work days with written notification?

\_\_\_ \_\_\_ (5) Does the completed SIF contain a copy of the commander's recommendation to grant, deny, or revoke the person's security clearance? eligibility? **Documented facts must support the recommendation.**

\_\_\_ \_\_\_ (6) Was the person's access to classified information suspended?

\_\_\_ \_\_\_ (a) If so, have positive control measures been implemented to preclude access to classified information, e.g., supervisor and peers notified, person's name removed from access letters?

\_\_\_ \_\_\_ \_\_\_ (b) If so, was the AF Form 2587, *Security Termination Statement*, completed? **Ensure you place a copy of the form in the SIF.**

\_\_\_ \_\_\_ (7) Was the person's unescorted entry to restricted areas suspended?

\_\_\_ \_\_\_ (a) If so, was the person's restricted area badge retrieved and secured?

\_\_\_ \_\_\_ (b) If so, was the AF Form 2586, *Unescorted Entry Authorization Certificate*, annotated? **Ensure you place a copy of the form in the SIF.**

\_\_\_ \_\_\_  (8) Was the installation Special Access Program (SAP) Monitor notified if the person has access to SAP information?

\_\_\_ \_\_\_  (a) If so, was the AF Form 2583, *Request for Personnel Security Action*, annotated and withdrawn? **Ensure you place a copy of the form in the SIF.**

\_\_\_ \_\_\_ (9) Was the person directed to seek treatment, counseling, etc.?

\_\_\_ \_\_\_ (10) Was the installation commander notified of the SIF establishment?

\_\_\_ \_\_\_ (11) Are the following support documents/information, if applicable, submitted with the SIF?

Commander's and supervisor's recommendation.

Most recent PSI conducted by the investigating agency.

AFOSI reports of investigation.

Security forces or child advocacy reports, e.g., DD Form 1569, AF Form 3545, ISPM memorandum of unfavorable information received through SF channels.

Summary of facts to substantiate any unfavorable information not covered by one of the reports listed above.

A summary of UIF entries.

Medical (to include mental health) evaluations which indicate significant impairment of the person's judgment or reliability. The report must contain a diagnosis; its effect on the person's judgment or reliability and prognosis along with any additional instructions or restrictions on the use of the information by appropriate medical authority.

Summary of actions by Social Actions (SA), e.g., why the person was involved; how program personnel categorized the person's situation, a diagnosis and SA's recommendations regarding clearance eligibility. The date of successful completion of a rehabilitation program, progress in a rehabilitation program, or the date termed a rehabilitative failure was declared.

A summary or actual report of administrative/disciplinary actions to include, letters of counseling, letters of reprimand, Article 15 or court-martial orders, bankruptcy petitions, discharge orders, or copies of letters of indebtedness.

Orders or written notification advising the status and location of persons placed in retraining, or appellate leave, or rehabilitation or confinement status.

Correspondence or forms relating to the withdrawal of access, to include SAP, SCI, unescorted entry, or decertification from the Personnel Reliability Program (PRP).

Any other pertinent information that could assist the adjudication process.

(12) Are commander/supervisor recommendations consistent with base support evaluations and recommendations?

(13) Does the SIF and supporting documentation "clearly" support the commander's decisions to establish the SIF and other recommended actions?

2. My POC is (rank and name), (telephone number).

Unit Commander's Signature Element

Attachment:  
(as required)

**Figure 1.4. Sample Evaluation of Continued Security Clearance Eligibility Memorandum.**

MEMORANDUM FOR (Designated Unit Commander)

FROM: CSF Address Element

SUBJECT: Evaluation of Continued Security Clearance Eligibility – (Subject's rank, name, SSAN)

1. My unit received the attached (unfavorable/derogatory) information concerning a member of your organization, (rank and name). Please review the information and decide on the basis of available facts if it is in the best interest of national security to establish a security information file (SIF). Also, a determination must be made whether the person should have continued access to classified information and maintain restricted area unescorted entry privileges. Your review of security clearance eligibility criteria in AFI 31-501, Chapter 8, and DoD 5200.2-R, para 2-200, and Appendix I should provide sufficient criteria upon which to base your decision. Please use PACAF Pamphlet 31-1 for preparing and processing SIF correspondence.
2. Please forward your decision, with sufficient rationale, whether or not a SIF will be established by (NLT **20** days from this memo).
3. My personnel security office stands ready and willing to assist.

CSF's Signature Element

Attachment:  
(related reports)

cc:  
SPTG/CC and Wing/CC

**Figure 1.5. Sample 497 IG/INS Notification Memorandum (Person Maintains Access).**

MEMORANDUM FOR 497 IG/INS

FROM: CSF Address Element

SUBJECT: Security Information File (SIF) Establishment – (Subject's full name, rank, SSAN)

1. The commander of (identify unit and base) requests SIF establishment on (name, rank, SSAN) due to (specify reason and issue). Based on available information, the commander determined not to suspend the person's access to classified information at this time.

2. The SIF was established on (date).

CSF's Signature Element

Attachment:  
(related SIF information)

cc:  
Subject's Unit Commander

**Figure 1.6. Sample SIF Memorandum (Commander to SIF Recipient – Access Suspended).**

MEMORANDUM FOR (SIF Recipient)

FROM: Unit Commander's Address

SUBJECT: Security Information File (SIF) Establishment and Suspension of Access to Classified Information

1. I hereby notify you that I am suspending your access to classified information and removing your restricted area unescorted entry privileges. My decision is based on your alleged (be specific as protection of sources allows and national security permits).
2. A SIF will be established. When all final actions, and base support activity evaluations and recommendations have been completed, I will evaluate the case and make a security determination and recommendation concerning your security clearance eligibility. The 497 IG/INS will make the final determination concerning your security clearance eligibility.
3. If you wish to provide a formal rebuttal reply to my decision, it must be provided to me no later than (list date – no more than *five* working days from the memo).
4. I encourage you to review AFI 31-501, Chapter 8, and DoD 5200.2-R, para 2-200 and Appendix I.

Unit Commander's Signature Element

cc:

SF PSO

**Figure 1.7. Sample Request for Review and Written Opinion Memorandum.**

MEMORANDUM FOR (Installation Support Activity, e.g., JA, DP, SG)

FROM: Unit Commander's Address

SUBJECT: Request for Review and Written Opinion – Security Information File (SIF) Establishment

1. Request your assistance concerning SIF establishment on one of my assigned people, (full name and rank). AFI 31-501 requires your professional opinion and recommendation concerning (rank and name) security clearance eligibility. Your inputs and recommendation will assist me and the 497 IG/INS adjudicators to determine if (rank and name) continued security clearance eligibility would be in the best interest of national security. Please ensure your recommendation clearly and undisputedly states whether the person should maintain his/her security clearance eligibility.
2. Also, please review any pertinent records available in your office (e.g., unfavorable information folder, medical records) and advise me if there is any additional information that would warrant the continued denial of this person's access to classified information and/or restricted area unescorted entry privileges.
3. Please return the entire package with a record of your review comments and recommendation by (list a date within **10** working days).
4. My POC is (rank and name), (telephone number).

## Unit Commander's Signature Element

Attachment:  
(SIF and related documents)

**Figure 1.8. Sample SIF Establishment Notification Memorandum (CSF to Unit Commander).**

MEMORANDUM FOR (Unit Commander)

FROM: CSF Address element

SUBJECT: Security Information File (SIF) Establishment – (SIF recipient's rank and full name)

1. A SIF has been established for (rank and full name) of your organization in accordance with AFI 31-501.
2. The following documents have been placed in the file:
  - a. A copy of your SIF Establishment memo, (date).
  - b. A copy of the SIF Establishment notification to 497 IG/INS.
3. The SIF will be maintained by my personnel security office until all local actions necessary to make a security clearance eligibility determination are completed. The file will be forwarded to the 497 IG/INS for a final security clearance eligibility determination. Please provide us with the following documents and information for SIF incorporation:
  - a. Copies of all investigative reports (e.g., AFOSI, DIS, Security Forces, local police agencies) that have a bearing on the case.
  - b. Summary of the person's unfavorable information file (UIF), if any, that may have a bearing on the adjudication process.
  - c. Reports or summaries of medical evaluations having a bearing on the medical aspects affecting the person's ability to be granted or retain access to classified information, and/or restricted area unescorted entry privileges. The medical evaluation must contain a recommendation concerning the person's continued security clearance eligibility.
  - d. Correspondence and information related to the withdrawal, revocation, or suspension of the person's access to classified information and security clearance eligibility.
  - e. Review and written opinions from base support agencies.

- f. Any other information that will assist the adjudication process.
4. I recommend you to review AFI 31-501, Chapter 8; DoD 5200.2-R, and PACAF Pamphlet 31-1.
5. My POC is (rank and name), (telephone number).

CSF's Signature Element

**Figure 1.9. Sample SIF Transfer Memorandum (SF PSO to Gaining SF PSO).**

MEMORANDUM FOR (Gaining SF PSO)

FROM: SF Address Element

SUBJECT: Transfer of Security Information File (SIF) – (full name, rank, SSAN)

1. The attached SIF is forwarded in accordance with AFI 31-501 for your review and action.
2. The person has permanent change of station orders to your unit; RNLTD is (date).
3. Please inform us by message, memo, or E-mail that you received this correspondence.
4. My POC is (rank and name), (DSN).

CSF's Signature Element

Attachment:

SIF – Full Name and Rank

cc:  
497 IG/INS

**Figure 1.10. Sample SIF Closure Recommendation Memorandum.**

MEMORANDUM FOR XX SFS/CC

497 IG/INS

In Turn

FROM: Unit Commander

SUBJECT: Recommendation to Close Security Information File (SIF) – (name and rank)

1. Request SIF on (name and rank) be forwarded to 497 IG/INS for final adjudication. The following information is provided:
  - a. Mental health evaluation (as required).
  - b. Successfully completed Alcohol Rehabilitation Program on (date), (as required).
  - c. Successfully completed financial counseling on (date), if required.
  - d. Completed administrative action(s).
  - e. Judicial action (an opinion from the SJA regarding factors used in the determination of withdrawal or dismissal of charges when there is evidence the person engaged in the misconduct, e.g., positive urinalysis, but found not guilty through court-martial).
  - f. Commander's and supervisor's recommendations.
  - g. Any other pertinent information.
2. The person will be (returned to duty/cross-trained/separated/placed in appellate leave status) on (date). Based on the information provided in this case, recommend (rank and name's) security clearance eligibility be (reinstated/revoked) – (ensure you provide supporting rationale).
3. If additional information is required, please contact me at (number).

Unit Commander's Signature Element

Attachments:  
(as required)

cc:  
SPTG/CC and Wing/CC

## Chapter 2

### LIMITED ACCESS AUTHORIZATION (LAA) PROGRAM

#### 2.1. General LAA Information.

2.1.1. Only U.S. citizens are eligible for and can possess a U.S. security clearance. There are times however, especially at overseas locations, when foreign nationals having a special or unique skill or program expertise require access to classified information in order for the U.S. to successfully accomplish its mission. In these rare circumstances, the LAA program is used to satisfy the requirement. Commanders and supervisors need to understand the LAA program does not equate to a security clearance and does not give full freedom and access to classified information; access must be *limited* to a specific scope of classified information in order for the U.S. to accomplish its mission. The ISPM must ensure all people assigned to the installation are aware of the LAA program and its associated limitations. LAA program success requires everyone's involvement and understanding.

#### 2.2. LAA Program Requirements and the LAA Process.

##### 2.2.1. LAA Limitations.

2.2.1.1. LAAs must be limited to people having a special skill or technical expertise essential to fulfilling a DoD requirement that can not be filled by a U.S. citizen.

2.2.1.2. LAAs must not be granted to people who perform routine administrative or other support duties, such as secretaries, clerks, drivers, unless it has been *clearly* established that the duties can not be performed by a U.S. citizen.

2.2.1.3. LAA recipients can not be permitted uncontrolled access to areas where classified information is stored or discussed.

2.2.1.4. Classified information must be maintained in locations under the continuous control and supervision of a cleared U.S. person. *Note: LAA recipients can never be given security container combinations.*

2.2.1.5. The scope of access must be specifically described in the LAA nomination request and must be strictly adhered to. Access to classified information not specifically addressed in the nomination request constitutes a compromise of classified information and must be investigated.

2.2.1.6. LAA recipients can not be designated as a courier or escort classified information outside the location in which access is permitted unless they are accompanied by a cleared U.S. person.

2.2.1.7. Commanders must plan LAA requirements accordingly. The average time from the decision to initiate a LAA request through final adjudication is 9 to 15 months.

##### 2.2.2. LAA Access Levels.

2.2.2.1. LAAs are only authorized at the SECRET or CONFIDENTIAL level.

2.2.2.2. Commanders may never grant interim access.

2.2.2.3. The information released to the LAA recipient must be releasable to the person's country or countries of citizenship.

2.2.2.4. Access must be limited or related to a specific program or project . The LAA must be terminated or rejustified upon completion of the project or program.

### 2.2.3. LAA Requirements.

2.2.3.1. The installation ISPM – CSF approves unit LAA requests. When approved, the ISPM sends the request to HQ PACAF/SF.

2.2.3.2. The MAJCOM/SF pre-approves all LAA requests. *Note: SF pre-approval does not authorize or constitute access to classified information; it's intended to give units permission to initiate an investigation request – single-scope background investigation (SSBI).*

2.2.3.3. A favorably completed and adjudicated SSBI is required before access can be granted.

2.2.3.4. A periodic reinvestigation (PR) must be conducted every *five* years; the date is based on the AF Form 2584 Investigation Date, Block 9.

2.2.3.5. LAAs must be recertified annually by HQ PACAF/SF. Recertification requests are due to HQ PACAF/SFI by 1 Oct each year. In concert with para 2.2.3.4, the MAJCOM/SF will not recertify LAAs if the required PR has not been submitted. Non-recertification results in LAA suspension.

2.2.3.6. All requests for LAAs must contain a detailed justification and plan describing the following:

- Location of classified information (security container, vault, etc.) in relationship to the location of the foreign national.
- Nature of access – must be *specifically* spelled out. Statements such as “the person is needed to translate host nation communications and correspondence or needed to execute mission requirements” is too broad and generic and will cause LAA requests to be disapproved.
- The compelling reason for not employing a cleared or eligible U.S. citizen.
- A synopsis of an annual continuing evaluation program to evaluate the person’s continued trustworthiness and eligibility for access.
- A plan to control access to secure areas, and to classified and controlled unclassified information.

2.2.3.7. LAA recipients must sign a SF Form 312, *Nondisclosure Agreement*, before they can have access to classified information.

2.2.3.8. Unless prohibited by host nation laws, LAA recipients must agree (in writing) to undergo a polygraph if directed by competent authority before they can have access to classified information.

2.2.3.9. LAA recipients must sign an AF Form 2587, *Security Termination Statement*, when they no longer require access to classified information or terminate their service.

2.2.3.10. Unit commanders must immediately notify the ISPM when LAA is terminated or suspended; in-turn the ISPM notifies HQ PACAF/SFI.

2.2.3.11. Changes to LAA (nature of access or level of access) information must be forwarded to HQ PACAF/SF for approval. Recommend units attach a separate memo to the initial LAA

request and rejustify changes to the initial LAA requirement. *Note: LAA to the new information can not be granted until approved by HQ PACAF/SF.*

2.2.3.12. HQ PACAF/SF must submit an annual LAA report to 497 IG/INS NLT 1 Nov each year.

#### **2.2.4. LAA Case File/Records Maintenance.**

2.2.4.1. LAA files/records must be maintained for *five* years from the date of LAA termination.

2.2.4.2. As a minimum, the LAA file/record must contain the following:

- The identity of the LAA recipient: full name, date and place of birth, current citizenship, SSAN (if applicable), and national identification number.
- The person's status as an immigrant alien or foreign national. *Note: If the person is an immigrant alien, annotate the date and place status was granted.*
- The LAA classification level, e.g., SECRET or CONFIDENTIAL.
- Date and type of most recent background investigation/PR and the investigating agency.
- Whether a polygraph examination was conducted; if so, the date and administering agency.
- The nature and identity of the classified program materials to which access is authorized and the precise duties performed.
- The compelling reason for granting access to classified information.
- A copy of the most recent Personnel Security Investigation, or computer disk containing the information.
- The SF Form 312, *Nondisclosure Agreement*.
- A copy of the most recent AF Form 2583, *Request for Personnel Security Action*
- A copy of the most recent AF Form 2584, *Record of Personnel Security Investigation and Clearance*.
- The most recent annual HQ PACAF/SF Recertification memo.
- Written acknowledgment to take a polygraph test when directed by competent authority, e.g. unit commander, AFOSI, DIS.
- An AF Form 2587, *Security Termination Statement*, when access to classified information is no longer required, e.g., retirement, program completion.
- Any other unit or official correspondence pertaining to LAA status, e.g. rejustification of access, suspensions.

#### **2.2.5. The LAA Process.** (See [Figure 2.1.](#) through [Figure 2.3.](#) for required memorandum format)

2.2.5.1. After determining mission requirements can not be successfully accomplished without employing a foreign national, the unit commander submits an initial LAA pre-approval request to the installation ISPM for review and concurrence.

2.2.5.2. If the installation ISPM concurs with the request, he/she endorses it and forwards it to HQ PACAF/SF for pre-approval. The ISPM must ensure unit commanders accurately depict their LAA requirements and provide detailed justification, especially in the area of the nature of access (specific nature of work regarding classified information).

2.2.5.3. If HQ PACAF/SF pre-approves the LAA request, the memorandum is endorsed and sent to 497 IG/INS, with a courtesy copy to the requesting ISPM.

2.2.5.4. Once HQ PACAF/SF pre-approves the LAA request, the requesting unit can initiate personnel security clearance requirements, e.g., EPSQ or SF 86, AF Form 2583. Follow locally established procedures for distributing paper work to the security forces and AFOSI detachment.

2.2.5.5. The AFOSI will conduct their portion of the LAA recipient's SSBI and forward the results to the Defense Investigative Service (DIS). After DIS completes their portion of the investigation, they will forward the case file to 497 IG/INS for adjudication.

2.2.5.6. If the 497 IG/INS favorably adjudicates the LAA, they will forward an AF Form 2584 to HQ PACAF/SF. HQ PACAF/SF will endorse the adjudication and forward it to the installation ISPM, who in turn forwards it to the requesting unit.

2.2.5.7. After completion of all the above actions (para 2.2.5.1 to 2.2.5.6), the unit commander can grant access to classified information as soon as the LAA recipient signs the SF 312, *Nondisclosure Agreement*, and consents (in writing) to take a polygraph when directed by competent authority.

### 2.3. LAA Self-Assessment Checklist.

2.3.1. Are commanders, supervisors, security managers, and co-workers aware of LAA requirements, restrictions, and associated limitations? (DoD 5200.2-R, para 3-402a)

2.3.2. Has the unit commander established controls to ensure the LAA program is effectively managed and controlled? (DoD 5200.2-R, para 3-402 b, c, and d.)

2.3.3. Are LAA recipients granted interim access, pending final adjudication? – **NOT AUTHORIZED**. (DoD 5200.2-R, para 3-402c(1))

2.3.4. Has the unit commander established a continuous evaluation process to ensure LAAs are effectively managed and controlled? (DoD 5200.2-R, para 3-402d(7)(c))

2.3.5. Are LAA periodic reinvestigations (PR) accomplished every *five* years? (DoD 5200.2-R, para 3-402d(6))

2.3.6. Are LAA annual recertifications submitted to HQ PACAF/SF by 1 Oct 97 of each year?

2.3.7. Is LAA correspondence prepared in accordance with PACAF Pamphlet 31-1? (PACAF Pamphlet 31-1, **Figure 2.1.** through **Figure 2.3.**)

2.3.8. Are LAA files/records maintained for *five* years after the LAA is terminated? (DoD 5200.2-R, para 3-402f(1))

2.3.9. Are LAA records/files maintained in accordance with PACAF Pamphlet 31-1? (PACAF Pamphlet 31-1, para 2.2.4.2)

2.3.10. Did the LAA recipient sign the SF Form 312 before he/she was granted access to classified information? (PACAF Pamphlet 31-1, para 2.2.3.7)

2.3.11. Do LAA recipients consent, in writing, to undergo a polygraph test before they are granted access to classified information? (DoD 5200.2-R, para 3-402, f(4))

2.3.12. Did the LAA recipient sign an AF Form 2587 after the LAA was terminated? (PACAF Pamphlet 31-1, para 2.2.3.9)

2.3.13. Are LAAs terminated or rejustified upon program/project completion? (PACAF Pamphlet 31-1, para 2.2.3.11)

2.3.14. Are LAA changes and/or rejustifications sent to HQ PACAF/SF for review and approval before the LAA recipient is granted access to classified information? (PACAF Pamphlet 31-1, para 2.2.3.11)

2.3.15. Is LAA strictly limited to the specific scope of access requested in the initial LAA memorandum? (PACAF Pamphlet 31-1, para 2.2.15)

**Figure 2.1. Sample Memorandum for Initial LAA Pre-Approval.**

MEMORANDUM FOR (INSTALLATION ISPM -- CSF) or (HQ PACAF/SF)

FROM: (Unit Commander)

SUBJECT: Initial Limited Access Authorization (LAA) Pre-Approval Request

1. Request initial LAA pre-approval for (name). The LAA is required in support of DoD mission requirements. We provide the following information:

- a. Full Name:
- b. Date and Place of Birth:
- c. Current Citizenship: (if the person maintains dual-citizenship, list both)
- d. Status of Individual (immigrant alien, foreign national, etc.):
 

**Note:** If an immigrant alien, provide date and place where status was granted.
- e. Personal Identification #: (SSAN or foreign country identification number)
- f. LAA Access Level: (SECRET or CONFIDENTIAL)
- g. Nature of Access (list specific duties and program responsibilities):
- h. Compelling Reason for Granting Access:
- i. Describe the Location of Classified Material in Relationship to the Location of the Foreign National:

j. The Compelling Reason for Not Employing a Cleared U.S. Citizen in the Position:

k. Synopsis of the Unit's Annual Continuing Assessment Program to Evaluate the Individual's Trustworthiness and Eligibility for Access:

l. Unit's Plan to Control Access to Secure Areas and Classified and Controlled Unclassified Information:

m. Will the Person Consent (in Writing) to a Counterintelligence-Scope Polygraph if Directed by Competent Authority? (Yes or No) LAA Recipient's Initials: \_\_\_\_\_

n. Does the Recipient Agree to Sign an AF 312, Nondisclosure Agreement? (Yes or No) LAA Recipient's Initials: \_\_\_\_\_

2. I understand LAA can not be granted until the recipient's investigation is completed and favorably adjudicated by 497 IG/INS, and the recipient signs a SF 312, *Nondisclosure Agreement*, and agrees in writing to undergo a polygraph examination if directed by competent authority.

3. LAA will be immediately terminated when no longer operationally required or suspended if circumstances warrant such a decision.

4. My POC is \_\_\_\_\_, DSN \_\_\_\_\_.

Unit Commander's Signature Element

1st Ind (if applicable), ISPM's Address Element

MEMORANDUM FOR HQ PACAF/SF

I concur/do not concur with initial LAA request.

ISPM'S Signature Element

**Figure 2.2. Sample Memorandum for LAA Annual Recertification.**

MEMORANDUM FOR (INSTALLATION ISPM – CSF) or (HQ PACAF/SF)

FROM: (Unit Commander)

SUBJECT: Annual Limited Access Authorization (LAA) Recertification Request

1. Request annual LAA recertification for (name). We provide the following information:
  - a. Full Name:
  - b. Date and Place of Birth:
  - c. Current Citizenship: (if recipient maintains dual-citizenship, list both)
  - d. Status of Individual (immigrant alien, foreign national, etc): Note: If an immigrant alien, provide date/place where status was granted.
  - e. Personal Identification #: (SSAN or foreign country identification number)
  - f. Date and Type of Investigation (include investigative agency):
  - g. LAA Access Level: (SECRET or CONFIDENTIAL)
  - h. Are Access Requirements and Duties the Same as the Initial LAA Pre-Approval Request? (Yes or No) If no, specifically describe and rejustify access requirements.
  - i. Does the LAA Recipient Consents (In Writing) to Take a Counterintelligence-Scope Polygraph, if Directed by Competent Authority: (Yes or No) If applicable, date of last polygraph examination:  
\_\_\_\_\_
  - j. Individual Has Signed a Nondisclosure Statement? (Yes or No), Date:\_\_\_\_\_
  - k. Has a Periodic Reinvestigation (PR) Been Accomplished Within *Five* Years? (Yes or No) Date of last PR: \_\_\_\_\_
2. The LAA is required in support of DoD mission requirements.
3. LAA will be immediately terminated when no longer operationally required or suspended, if circumstances warrant such a decision.
4. My POC is \_\_\_\_\_, DSN \_\_\_\_\_.

Unit Commander's Signature Element

1st Ind (if applicable), ISPM's Address Element

MEMORANDUM FOR HQ PACAF/SF

I concur/do not concur with the LAA recertification request.

ISPM's Signature Element

**Figure 2.3. Sample Memorandum for LAA Termination.**

MEMORANDUM FOR (Installation ISPM – CSF) or (HQ PACAF/SF)

FROM: (Unit Commander)

SUBJECT: Limited Access Authorization (LAA) Termination

1. Request LAA termination for (name). We provide the following information:
  - a. Full Name:
  - b. Date and Place of Birth:
  - c. Current Citizenship: (if the person maintains dual-citizenship, list both)
  - d. Status of Individual (immigrant alien, foreign national, etc.):
 

**Note:** If an immigrant alien, provide date/place where status was granted.
  - e. Personal Identification #:
  - f. LAA Classification Level:
  - g. Nature of Access (list specific duties and program responsibilities):
  - h. Reason for LAA Termination:
  - i. Individual Has Signed a Security Termination Statement? (Yes or No), Date: \_\_\_\_\_
  
2. As required by DoD 5200.2-R, the LAA file/record will be maintained for **five** years from the date of LAA termination.
  
3. My POC is \_\_\_\_\_, DSN \_\_\_\_\_.

Unit Commander's Signature Element

1st Ind (if applicable), ISPM's Address Element

MEMORANDUM FOR HQ PACAF/SF

Concur.

ISPM's Signature Element

DOSS C. VON BRANDENSTEIN, Col, USAF  
Director of Security Forces

**Attachment 1**

**USERS' FEEDBACK**

**A1.1.** We encourage users of this pamphlet to input their comments and recommendations. Send your comments to HQ PACAF/SPI, 25E St Ste M307, Hickam AFB HI 96853-5439. Please provide the following:

A1.1.1. User's rank and name:

A1.1.2. Unit:

A1.1.3. Mailing address:

A1.1.4. DSN:

**A1.2. Pamphlet Content.**

A1.2.1. Does the pamphlet provide a conceptual framework for the topics?

A1.2.2. Is the information accurate and factual? What needs to be updated?

A1.2.3. Is the pamphlet consistent with other AF documents?

A1.2.4. Can the pamphlet be better organized for the best understanding of the material presented?

A1.2.5. Is the pamphlet useful? If not, how can it be improved?

**A1.3. Writing and Appearance.**

A1.3.1. Where does the pamphlet need revision to make the writing clear and concise? How would you word it to make it more clear and precise?

**A1.4.** Recommended urgent changes(s) (if any).

**A1.5.** Other Comments.