



**MANAGING THE INFORMATION SECURITY  
PROGRAM**

**COMPLIANCE WITH THIS PUBLICATION IS MANDATORY**

---

**NOTICE:** This publication is available digitally on the 3rd Wing WWW site at: <http://infonet/irgs/3wg/3sptg/3cs/scs/scsp/pdl/index.htm>. If you lack access, contact your Publishing Distribution Office (PDO).

---

OPR: 3 SFS/SFAI (SSgt A. Williams)

Certified by: 3 SPTG/CC (Col Timothy W. Van Splunder)

Supersedes AFI 31-401/Wg Sup 1, 7 August 1996

Pages: 10

Distribution: F

---

This publication does not apply to the US Air Force Reserve or Air National Guard units and members.

**SUMMARY OF REVISIONS**

This document is substantially revised and must be completely reviewed.

**AFI 31-401, 1 January 1999, is supplemented as follows:**

**1.1.** The provisions of this supplement are applicable to 3rd Wing staff agencies and associated units for whom a host tenant agreement exists, and applicable 11th Air Force (11 AF) agencies located within the confines of Elmendorf AFB.

**1.3.3.4. (Added)** (3WG). The Information Security Program Manager (ISPM), 3 SPTG/SF has oversight for the wing security program. The ISPM will provide the following services:

**1.3.3.4.1. (Added)** (3WG). Conduct initial interviews within 10 days of appointment. Train all new security managers within 90 days of appointment.

**1.3.3.4.2. (Added)** (3WG). Assist security managers in developing unit security operating instructions.

**1.3.3.4.3. (Added)** (3WG). Conduct annual program reviews. These reviews will incorporate annual industrial security reviews and open storage recertifications.

**1.3.3.4.4. (Added)** (3WG). Process and monitor inquiries and investigations.

**1.3.3.4.5. (Added)** (3WG). Make informal visits to customer unit security managers and work centers to advise, assist, answer questions, resolve problems, and monitor the security atmosphere of the installation.

**1.3.3.4.6. (Added)** (3WG). Monitor the wing semiannual security self-inspection effort.

**1.3.5.4. (Added)** (3WG). Appoint unit security managers in writing (see attachment 1) for a minimum of 12 months; a copy of the appointment letter is to be forwarded to 3 SFS/SFAI. The ISPM will then schedule the initial security manager briefings.

**1.3.6.2.** See attachment 2 for sample Emergency Protective/Relocation Plan of Classified Material.

**1.3.6.9. (Added)** (3WG). Develop a security managers handbook and maintain the following information within:

**1.3.6.9.1. (Added)** (3WG). Security Manager Letter of Appointment.

**1.3.6.9.2. (Added)** (3WG). Internal Security Operating Instructions.

**1.3.6.9.3. (Added)** (3WG). Semiannual Security Inspection Reports (last year only).

**1.3.6.9.4. (Added)** (3WG). Information Security Program Review Report (last year only).

**1.3.6.9.5. (Added)** (3WG). Security Managers Meeting Minuets (last year only).

**1.3.6.9.6. (Added)** (3WG). Information Letters.

**1.3.6.9.7. (Added)** (3WG). Sentinel Key PR Report.

**1.3.6.9.8. (Added)** (3WG). Inspections Checklists.

**1.3.6.9.9. (Added)** (3WG). Miscellaneous Items (AF Forms 2583, *Request for Personnel Security Action*, 2586, *Unescorted Entry Authorization Certificate*, and 2587, *Security Termination Statement*).

**1.3.6.10. (Added)** (3WG). Manage the semiannual security inspections and conduct them twice each year for those units that possess classified material. Units may use the ISPMs program review as one of these inspections. (**EXCEPTION:** Units possessing one drawer or less of classified material may conduct a self-inspection once each year. **NOTE:** This only applies if 3 SFS/SFAI staff deems necessary, based on sound risk management procedures.) Reports are to be reviewed and endorsed by the unit security manager. A copy of the inspectors appointment letter and report will be forwarded to 3 SFS/SFAI. Security managers should not conduct inspections themselves, but have others in the unit perform them. Classified contractors working within units should be included in this inspection.

**2.4.5. (Added)** (3WG). Unit security managers of the preparing agency will review classified operational plans (OPLANS), operational orders (OpOrds), program action directives (PAD) programming plans, and classified supplements/directives for proper portion markings, downgrade/declassification instructions, and classification actions.

**5.12.1. (Added)** (3 WG). A Standard Form 701, *Activity Security Checklist*, does not need to be completed in offices of 24-hour operations, but must be kept on hand in case 24-hour operation schedule changes. When filled out, indelible ink must be used.

**5.12.2. (Added)** (3WG). A Standard Form 702, *Security Container Check Sheet*, must be affixed to the outside of all locking drawers. When filled out, indelible ink must be used.

**5.14.3. (Added)** (3WG). All removable classified materials and equipment on an aircraft will be removed and stored in a General Services Administration (GSA) approved safe/vault. If mission dictates otherwise, the aircraft commander in the presence of a security force representative must seal the aircraft. A security force patrol will conduct periodic checks not to exceed one every 3 hours on aircraft containing classified materials. If owner/user personnel cannot seal the aircraft, they will be responsible for providing continuous surveillance of the aircraft. Base operations personnel will immediately notify 3 SFS dis-

patcher at 552-3421 when first advised of this type of situation. A blotter entry will reflect the seal number and include the physical location and telephone number for the aircraft commander or designated representative. **NOTE:** Classified material will never be left on an aircraft for the sake of convenience.

**5.14.4. (Added)** (3WG). During deployments, units may place GSA-approved security containers on pallets. These pallets require periodic checks by owner/user or other personnel responsible for the security of the marshaling area. This does not apply if units are deploying from civilian airports. If deploying from civilian airports, owner/user personnel must provide continuous security of the container until it reaches a military installation.

**5.15.1.1. (Added)** (3WG). As a minimum, activities hosting classified meetings or briefings will ensure that they:

**5.15.1.1.1. (Added)** (3WG). Verify attendees clearances by electronic means, that is, Sentinel Key.

**5.15.1.1.2. (Added)** (3WG). Verify attendees need-to-know through the unit security manager.

**5.15.1.1.3. (Added)** (3WG). Post guards (unit hosting) as needed on exit/entry doors to prevent unauthorized monitoring.

**5.15.1.1.4. (Added)** (3WG). Perform positive identification (ID)/picture ID check of all attendees prior to entering.

**5.19.1. (Added)** (3WG). An AFTO Form 36, *Maintenance Record For Security Type Equipment*, must be affixed to the inside of all locking drawers.

**5.20.4. (Added)** (3WG). Storage containers used for storing classified material will be numbered by using functional address symbol and number (that is, SPAI-1). The security manager will maintain a list of storage container designations showing exact location of the safe (functional address symbol, building/room number, classified account custodian). Provide 3 SFS/SFAI with a copy of this list.

**5.20.5. (Added)** (3WG). Open/Secured storage areas that have windows will be covered by a non-transparent material to prevent viewing from the outside. Approval/Recertifications letters will be posted in the area approved for open storage. Approval for storage of classified material in vaults, secure rooms, and cages has been delegated to the ISPM.

**5.20.5.1. (Added)** (3WG). Preliminary survey and final certification requests of open storage areas must be routed through the unit security manager.

**5.20.6. (Added)** (3WG). Bay 8W02 of the 632nd Air Mobility Support Squadron (632 AMSS/TRK), 552-4192, Building 15-380, Air Freight Terminal, is authorized for storage of classified material, up to and including the Top Secret level. The vault must be secured with a built-in GSA-approved combination X-07 lock.

**5.20.7. (Added)** (3WG). If requested, Base Operations (3 OSS/OSAM), Building 11-369, 552-3285, will provide temporary storage of small amounts of classified materials, up to and including Secret (6 cubic feet or less) in the possession of aircrews transiting Elmendorf AFB. In the event transit aircrew classified material exceeds the storage capacity of the 3 OSS/OSAM, the overflow is to be stored with the Elmendorf Command Center (ECC)(3 WG/CP), Building 11-550, Basement, 552-2858. Temporary storage of Top Secret materials will be provided by the ECC. Expanded operations (such as full formation of the Wing Battle Staff) may prohibit storage of large amounts of classified materials within the ECC. If the ECC Senior Controller determines that he/she cannot provide proper protection of the materials, he/she will notify 3 SFS/SFA, 552-6524 (duty hours) 552-3421 (non-duty hours), who will arrange alternate

storage for the materials. The 632nd Air Mobility Control Center (AMCC) 552-4192, is available to provide temporary storage, on a space available basis, of classified material with Air Mobility Command (AMC) transit aircrews.

**5.29.2.6. (Added)** (3WG). Building 9-468 is designated as the base central destruction facility. The Chief, Base Records Management, 552-4382, is the office of primary responsibility for access use, training, and management of this facility. Arrangements must be made through the Chief, Base Records Management. Also available is a Security Engineered Machine Model 1200 for destruction of classified CD ROMs.

**6.3.2.1. (Added)** (3WG). Recipients of express mail containers are required to protect these parcels as classified until the classification of the contents is determined.

**6.4.1.** Personnel authorized to receipt for first class mail bearing the “**RETURN SERVICE REQUESTED**” notice, certified and registered mail, are responsible for giving the package to the unit security manager or the person in the office of the addressee for storage in an approved storage container by the end of the duty day.

**6.4.1.1.** There must be 1/2-inch clear space both above and below the endorsement.

**6.6.3.1. (Added)** (3WG). Personnel will use an outer container or envelope when entering Secret material into the Official Mail Center (OMC). The only exception will be when material is shipped by pouch, in which case the pouch can be used as the outer container.

**6.6.4.1.3. (Added)** (3WG). For purposes of tracer actions, Alaska is considered to be in the Continental United States (CONUS).

**6.7.4. (Added)** (3WG). Procedures for disseminating classified material within the unit/staff agency, sign out logs, AF Form 614, *Charge Out Record*, on-loan suspense file, and so forth will be incorporated into a unit directive or established as an operating instruction in accordance with AFI 33-360, Vol I, *Air Force Publication Management Program*.

**6.9.** See attachment 3 for sample courier authorization letter.

**8.3.1.1. (Added)** (3WG). Personnel will be indoctrinated based upon the degree of involvement with classified materials.

**9.3.2.1.1. (Added)** (3WG). The official appointed as investigating official will contact 3 SFS/ SFAI the first day of appointment for a briefing on duties and responsibilities. Attachment 4 contains the format of a preliminary inquiry appointment letter.

**9.3.2.3.1. (Added)** (3WG). Prior to forwarding the completed inquiry report to the appointing authority, the inquiry officer will forward the report for a technical review by 3 SFS/SFAI. The technical reviews will be attached to the inquiry report.

**9.6.2.1. (Added)** (3WG). Forward inquiry reports to 3 SFS/SFAI within 10 duty days of the discovery of incidents. (Reasonable extensions may be granted by appointing authorities.)

**Attachment 1**  
**SECURITY MANAGERS APPOINTMENT LETTER**  
**(UNIT LETTERHEAD)**

MEMORANDUM FOR 3 SFS/SFAI

FROM:

SUBJECT: Security Managers Appointment

1. In accordance with AFI 31-401, as supplemented, the following personnel are designated as the primary and alternate security managers for this unit/agency.

<b>NAME</b>	<b>CLEARANCE</b>	<b>DUTY PHONE</b>
MSgt John DOE	Top Secret	2-5528
TSgt Jane DOE	Secret	2-6524

2. This letter supersedes this unit's previous letter, same subject.

COMMANDER, STAFF AGENCY, or  
DET CHIEF'S SIGNATURE

## Attachment 2

### EMERGENCY PROTECTIVE/RELOCATION PLAN OF CLASSIFIED MATERIAL

**A2.1. Purpose/Threat.** This plan supplements AFI 31-401, paragraph 1.3.6.2. It establishes procedures for the protection and removal of classified materials in case of fires and natural disasters. Since Alaska is one of the 50 United States, no emergency destruction plan is required. However, the threats against Alaska are those of natural disasters, such as fires, floods, volcanic eruptions, or earthquakes.

**A2.2. Scope/Responsibilities/Limited Factors.** This plan is applicable to all military activities located on Elmendorf AFB. All personnel with appropriate security clearances are responsible for the proper care and disposition of classified materials in their charge, with the classified account custodians bearing primary responsibility for the security containers during the execution of this plan. Limiting factors will vary depending on the specific emergency and situation.

**A2.3. Task Organization/Coordination Instructions.** For all military activities on Elmendorf AFB. All units need to establish an operating instruction for the information security program, detailing what actions will be accomplished by assigned personnel for securing or relocating classified material during emergency situations described above. (**NOTE:** This plan must extend to include those authorized to keep classified at home in any case of incapacitation.) The base Security Forces and Fire Department would respond as part of their normal duties. As such, coordination will be handled on a case by case basis.

**A2.4. Protection/Relocation Procedures.** In the event of fires, floods, volcanic eruptions, or earthquakes the following actions will be taken.

**A2.4.1.** The senior ranking individual assigned to the activity or the installation commander will implement the appropriate emergency procedures.

**A2.4.2.** Time permitting, secure all classified materials in an approved security container for the storage of classified materials.

**A2.4.3.** If time or conditions preclude proper storage, the individual in possession of the material at the time is responsible for its safekeeping until conditions permit proper storage.

**A2.4.4.** If relocating the classified materials is required, each unit needs to have designated an alternate storage location. When material is to be relocated, all classified materials will be placed in an appropriate container, that is, bag, box. The container will then be sealed and marked with the highest classification and transported to the alternate location until the situation is terminated.

**A2.4.5.** If material cannot be accounted for after the incident, the unit security manager and commander will be notified immediately. The unit commander will then initiate a preliminary inquiry in accordance with AFI 31-401, Chapter 6. If communications security (COMSEC) material is involved, the Base COMSEC office must be notified immediately.

**A2.5.** Questions concerning this plan should be directed to 3 SFS/SFAI.

**Attachment 3**

**IDENTIFICATION OF OFFICIAL COURIER**

MEMORANDUM FOR WHOM IT MAY CONCERN

FROM: 3 CS/CC

8517 20th Street, Suite 4

Elmendorf AFB AK 99506-2210

SUBJECT: Identification of An Official Courier

1. SSgt John A. Daggett (SSN \*\*\*-\*\*-\*\*\*\*), 3rd Communications Squadron Elmendorf AFB, Alaska, is designated an official courier for the United States Government. He will be traveling aboard (Name of Airlines), departing from (Location) on (Date) and will arrive in (Destination) on (Date). Upon request, he will present his official identification card DD Form 2AF, number G00000001.
2. SSgt Daggett is hand-carrying a sealed package, size 18 x 13, addressed from 3 CS/SBR, Elmendorf AFB, Alaska 99506-2210, and addressed to 18th Communications Squadron (Base location and zip). This sealed package is further identified by the inscription "OFFICIAL UNITED STATES AIR FORCE COMMUNICATION, EXEMPT FROM EXAMINATION" bearing the signature of the undersigned (Commander's Name), Commander of the 3rd Communications Squadron, Elmendorf AFB, Alaska.
3. SSgt Daggett will depart Anchorage International Airport and transit through (Location of Expected Airport Stops) on (Date of Departure). This courier authorization expires on (Date of completed TDY).
4. If additional assistance or courier verification is required, my point of contact is (Security Manager's Name) at commercial 907-552-1110, DSN 317-552-1110 (during normal duty hours). After normal duty hours, please call commercial 907-552-2666, DSN 317-552-2666.

COMMANDER, STAFF AGENCY, or  
DET CHIEF'S SIGNATURE

**For Official Use Only**  
**(When Filled In)**

## Attachment 4

### PRELIMINARY INQUIRY APPOINTMENT LETTER

MEMORANDUM FOR (PERSON APPOINTED)

FROM: (Unit Appointing Authority)

SUBJECT: Appointment of Inquiry Official

1. Under the provisions of DOD 5200.1-R, AFI 31-401, and PACAF Sup 1, you are appointed to conduct a preliminary inquiry into the security incident (give a summary of the incident as to what classification level is involved, where the incident occurred, agency, building, room number, and the date and time discovered).
2. The purpose of this inquiry is to determine whether a compromise occurred and to categorize this security incident. These categories are: compromise, or security deviation. You are authorized to interview those persons necessary to complete your findings. You are further authorized access to all records and files, to include classified up to and including (level) classified material involved in the security incident which are pertinent to this inquiry.
3. Conducting this inquiry will be your primary duty until it's completed. You must immediately contact the Base Information Security Program Manager 552-5528/6524 for a briefing on your responsibilities, conduct, and limitations of this inquiry. Your written report will be forwarded to the 3 SFS/SFAI within 10 duty days from the date the security incident was discovered. As a minimum, your report must contain the following:
  - a. A statement that a compromise or possible compromise did or did not occur.
  - b. Category of the security incident.
  - c. Cause factors and responsible persons.
  - d. Recommended corrective actions.

4. Notify me immediately if you determine that a compromise has occurred. You are encouraged to obtain technical assistance from the Staff Judge Advocate or Base Information Security Program Manager during the course of this inquiry, whenever necessary.

SIGNATURE OF APPOINTING OFFICIAL

cc:3 SFS/SFAI

DOUGLAS M. FRASER, Colonel, USAF  
Commander