

**BY ORDER OF THE COMMANDER,  
PACIFIC AIR FORCES**



**AIR FORCE INSTRUCTION 31-401**

**PACIFIC AIR FORCES COMMAND**

**Supplement 1**

**28 MAY 2004**

**Security**

**INFORMATION SECURITY PROGRAM  
MANAGEMENT**

**COMPLIANCE WITH THIS PUBLICATION IS MANDATORY**

---

**NOTICE:** This publication is available digitally on the AFDPO WWW site at:  
<http://www.e-publishing.af.mil>

---

OPR: HQ PACAF/SFOP (Bernard V. Mann)

Certified by: HQ PACAF/SFO  
(Maj Joshua D. Fowler)

Supersedes AFI 31-401\_PACAFSUP1,  
5 March 1999

Pages: 9  
Distribution: F

---

**AFI 31-401, 1 November 2001, is supplemented as follows:** This publication applies only to the Air National Guard (ANG) United States Title 10 status. It does not apply to the Air Force Reserves Command (AFRC).

***SUMMARY OF REVISIONS***

**This document is substantially revised and must be completely reviewed.**

1.3.3. The Chief, Security Forces Operations Division, PACAF/SFO, is responsible for policy, resource advocacy, and oversight of the Information Security Program for PACAF. The Chief, Policy Branch, PACAF/SFOP, is the program coordinator for PACAF.

1.3.4. The Director of Security Forces, Pacific Air Forces, is the command Information Security Program Manager (ISPM). The senior security forces official of the host security forces squadron at each PACAF installation serves as the ISPM for that installation. The ISPM manages the information, personnel, and industrial security programs for the activities they serve.

1.3.4.4. (Added) Oversee the appointment of unit and staff security managers.

1.3.4.5. (Added) Develop and implement installation supplements to the information security program.

1.3.4.6. (Added) Train unit and staff security managers within 90 days of their appointment.

1.3.4.7. (Added) Conduct security managers meetings at least semi-annually.

1.3.6.9. Attend security managers training within 90 days of appointment.

1.3.6.10. (Added) Manage the Information, Personnel and Industrial Security Programs for the unit/staff office they are assigned to.

1.4.2. PACAF/SFOP will conduct security reviews at each PACAF installation at least every 24 months. Osan and Kunsan Air Bases in Korea will be visited annually. 13AF will be responsible for conducting security reviews at PACAF sites in Singapore, Diego Garcia and Australia.

1.4.3. Unit semi-annual self-inspections will be conducted no later than six months following an annual security program review. Program reviews may substitute and count as one of the semi-annual self-inspections.

1.5.1.1. Commanders at unit level and higher are authorized to certify and sign Department of Energy Forms 5631.20 granting access to Restricted Data.

1.5.1.1.2. ISPMs must notify PACAF/SFO of any changes to the list. PACAF/SFO will notify USAF/XOFI of any changes.

1.5.2.1. PACAF/SFO is responsible for reporting the status of all NATO information transiting through PACAF. PACAF/SFO is responsible for reporting NATO issues to USAF/XOF.

1.6.1. Request for waivers of this AFI will be sent through PACAF/SFO to USAF/XOF. Waivers will be submitted in Memorandum format. AF Form 116 will not be used for requesting waivers for this program.

1.7.1. SF 311, *Agency Security Classification Management Program Data Report*, must be submitted to PACAF/SFO no later than 25 August of each year.

1.7.2. MIS Reports required by AFPD 31-4 will be submitted to PACAF/SFO by 15 January and 15 July of each year. The format provided in [Attachment 1](#) will be used.

2.1.2.1. PACAF original classification authorities (OCA) are: Top Secret: COMPACAF and NAF Commanders; Secret: PACAF/DO/XP.

2.3.1. Send copies of all challenges to PACAF/SFO.

2.4. PACAF OCAs shall coordinate Security Classification Guides (SCG) with PACAF/SFO.

2.4.1. The review will be documented and a copy of the review will be forwarded to the ISPM for file.

2.4.2. Provide copies of DD Form 2024, *DoD Security Classification Guide Data Elements*, to PACAF/SFO.

2.4.3. Electronic versions of SCGs will be forwarded through PACAF/SFO.

2.4.4. PACAF/SFO will maintain a master list of PACAF SCGs.

5.4. Non-US citizens who are granted Limited Access Authorizations (LAA) will also sign SF 312.

5.5.1.6. (Added) Nondisclosure Agreements for non-US citizens will be filed in the person's case file retained by the ISPM.

5.6.1. The following officials may authorize access to individuals outside the executive branch: COM-PACAF, PACAF/CV/DO/XP/LG, and NAF commanders.

5.6.9. Request for authorization to disclose information to non-US organizations or individuals will be forwarded through PACAF/INX.

5.13.2. The Director of Security Forces, PACAF/SF, approves requests for removing Secret and Confidential material from designated work areas during non-duty hours.

5.15.2. At HQ PACAF, directors of staff agencies approve secure conference rooms.

5.20.1. Regardless of its physical characteristics and/or form, i.e., classified munitions, classified information and/or material are protected based on their "classification" level. Classified information and/or material should be secured in accordance with DoD 5200.1R and AFI 31-401. Other appropriate security measures must be utilized to provide the required protection level, i.e., IDS, armed guard, and periodic patrol checks when the size and form of classified information and/or material can not be secured in a secure container.

5.20.1.4. (Added) The room must be locked.

5.20.4. Wing commanders, in coordination with the Installation ISPM and the Base Civil Engineer, approve storage of classified material in vaults, secure rooms, cargo security cages, and munitions storage facilities. The Civil Engineer Squadron will conduct an initial survey for the open storage areas with the ISPM for coordination of construction requirements. Airfreight terminals cargo security cages may be approved up to Secret classification level. All classified storage facilities must meet the minimum standards IAW Appendix G of DoD 5200.1-R.

5.20.5. (Added) ISPMs will inspect secure storage facilities annually to ensure they continue to meet standards IAW D0D 5200.1-R.

5.24.1. When qualified US-citizen locksmiths are not available, foreign national locksmiths may be used to neutralize lockouts and repair security containers. The security container custodian will continuously escort foreign national locksmiths during repair of security containers.

5.28.3. PACAF activities will conduct the annual clean-out day in January of each year. Unit and Staff Security Managers will file the results of the annual clean-out day in their Unit Security Manager Handbook and send a file copy to the ISPM.

5.29.1. Classified material may be destroyed by burning, shredding, pulping, melting, mutilation, chemical decomposition, or pulverizing. Residue shall be inspected during each destruction to ensure that classified information cannot be reconstructed. Crosscut shredders shall be designed to produce residue particle size not exceeding ½ inch by 1/32 inch (1/64-inch variance).

5.29.1.1. (Added) Dispose of classified magnetic media according to AFSSI 5020, *Remanence Security*.

5.29.1.2. (Added) The approved method for routine destruction of CD-ROMs is incineration or National Security Agency (NSA) approved CD-ROM declassifier. SONY CDs are toxic and must not be burned. Security Engineered Machinery (SEM) Model 1200, CD-ROM declassifier approved for declassifying CD ROMs. However, it is not approved for CDs that are CD-R (recordable) or CD-RW (rewritable). The SEM 1200 may be ordered through your normal supply channel. If you cannot burn at your location, do not have a declassifier, or have CD-R or CD-RW disks, mail your classified CDs to NSA for destruction:

NSA L322

9800 Savage Road

Fort George G. Meade, MD 20755-6000

5.30.1. Each risk management factor as outlined in paragraph 6-800a of DoD 5200.1-R will be addressed in the ISPMs documentation. A statement of security-in-depth will be included in the justification.

5.30.1.1. Do not use AF Form 116 in PACAF for this purpose. Use Air Force Memorandum format to document alternative or compensatory control measures.

6.3.2. Recipients of packages sent via the GSA contract courier (i.e. FedEx Corp) must protect packages as Secret until determined otherwise.

6.9. See **Attachment 1** for sample courier authorization letter, and **Attachment 2** for sealed package exemption notice.

8.4.1.2.6. (Added) NATO briefing will be conducted concerning the following topics: Handling, Safeguarding, Marking, Transmission and Destruction. PACAF/SFO will be notified of any NATO information and or materials transient within the Pacific Command.

8.5. At HQ PACAF, staff agency security managers are responsible for training OCAs. Unit/staff agency security managers are responsible for training action officers on the security classification process. The proper use of derivative classification will also be included in the training.

8.7.1. (Added) Newly appointed security managers will be provided training on their duties within 90 days of appointment. Within 10 duty days of appointment, an appointment letter will be forwarded to the ISPM.

8.7.2. (Added) Security managers will include an evaluation of the effectiveness of security training during semi-annual self-inspections.

9.3.1. (Added) All classified message incidents (CMI) should be reported to the local ISPM to begin an evaluation on the impact of the incident to national security and the organization's operations IAW PACAFI 33-201, *Classified Message Incident Program*, 13 Feb 04.

**Attachment 1**

**SAMPLE LETTER, AUTHORIZING HAND CARRY OF CLASSIFIED MATERIAL  
ABOARD COMMERCIAL AIRCRAFT**

MEMORANDUM FOR WHOM IT MAY CONCERN

FROM: (Unit and address)

SUBJECT: Authorization to Hand-carry Sealed Package

1. MSgt Joe Doe, Directorate of Security Forces, Headquarters Pacific Air Forces Command (HQ PACAF/SFO) is designated an official courier for the United States Government. He will be traveling aboard Northwest Airlines depart Honolulu on October 1, 1998 and will arrive Naha, Japan, on October 3, 1998. Upon request he will present his official identification card DD Form 2AF, number G00005522.
2. MSgt Doe is hand carrying a sealed package, size 9" X 8" X 12", addressed from HQ PACAF/SFO, Hickam AFB, Hawaii 96853-5439, and addressed to 18th Security Forces Squadron, Unit 5212 APO AP 96368-5212. The package is identified on the outside by the marking 'OFFICIAL BUSINESS – MATERIAL EXEMPTED FROM EXAMINATION' bearing the signature of the undersigned.
3. MSgt Doe will depart Honolulu International Airport transit through Kansai International Airport, Osaka, Japan to Naha International Airport Japan.
4. This courier authorization may be confirmed by contacting the undersigned at HQ PACAF/SF, (808) 449-8153. This authorization expires 18 Oct 98.

**Attachment 2**

**SAMPLE, SEALED PACKAGE EXEMPTION NOTICE**

Department of the Air Force

HQ PACAF/SF

Hickam AFB, Hawaii 96853-5439

Official Business

MATERIAL EXEMPTED FROM EXAMINATION

**Attachment 3****SAMPLE, SECURITY MANAGER INITIAL BRIEFING**

Name/Rank: \_\_\_\_\_XXXXXXXXXXXXX\_\_\_\_\_ Date: \_\_\_XXXXXXXXXXXXX\_\_\_

Unit/Staff Agency: \_\_\_\_\_XXXXXXXXXXXXX\_\_\_\_\_ Primary / Alternate (Circle One)

I was provided an initial Information Security orientation briefing concerning the basic policies and procedures involved in the Information, Industrial, and Personnel Security Programs, as applicable to my unit/staff agency. This orientation briefing consisted of, but was not limited to, the following:

## 1. Security Managers Responsibilities:

- a. Providing advice and assistance to the unit commander/staff agency chief and unit personnel
- b. Establishing internal operating instructions and program management
- c. Ensure applicable security education training is conducted
- d. Attending formal security managers training within 90 days of appointment
- e. Attending quarterly security managers meetings
- f. Other responsibilities, as applicable

## 2. Information Security Program:

- a. Applicable regulations and instructions
- b. Basic Classification Management
- c. Derivative Classification

d. Accountability and Control of Classified information

e. Safekeeping and Storage

f. Transmission and Transportation

g. Foreign Travel Briefing

h. Disposal and Destruction

i. (Semi) Annual Security Self-Inspections

j. Security Incidents

k. Security Managers Handbook

l. Types of Information Security Surveys

3. Personnel Security Program:

a. Personnel security investigations and forms

b. Security clearances and the ASCAS roster

c. Security Information Files

d. Assignment of non-US nationals to sensitive positions

e. Unescorted entry into restricted areas

4. Industrial Security Program directives/procedures, as applicable.

**Signature of Briefer/Date**

**Signature of Security Manager/Date**

ALBERT F. RIGGLE, Colonel, USAF  
Director of Security Forces