

**BY ORDER OF THE COMMANDER,
SPACE AND MISSILE SYSTEMS CENTER**



**AIR FORCE INSTRUCTION 31-401
SPACE AND MISSILE SYSTEMS CENTER
Supplement 1
24 FEBRUARY 2003**

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: SMC/AXPI (Suzanne Rowland)
Supersedes AFI 31-401, SMC Supplement 1,
dated 20 Jun 01

Certified by: SMC/AXP (Judy Gonce)
Pages: 9
Distribution: F

The OPR for this supplement is SMC/AXPI (Ms Suzanne Rowland). This supplement implements and extends the guidance of Air Force Instruction (AFI) 31-401, dated 1 Nov 01, Information Security Program Management. This supplement describes SMC's procedures for use in conjunction with the basic AFI.

SUMMARY OF REVISIONS

This change updates paragraphs **2.4.1.**, **5.11.3. (Added)**, **5.12.1. (Added)**, **5.29.1.1. (Added)**, **6.1.7. (Added)** and **7.1.1.**; adds paragraphs **1.3.5.1.**, **1.4.2.3. (Added)**, **1.7.1.**, **2.1.2.3.3. (Added)**, **4.8.2.**, **4.12. (Added)**, **5.5.**, **5.6.9.**, **5.7.**, **5.10.1.**, **5.11.4. (Added)**, **5.15.**, **5.15.2.**, **5.15.3.**, **5.25.1. (Added)**, **5.28.3.1. (Added)**, **8.11.1.**, **8.14.4. (Added)**, **8.16.3.**, and **9.7.2.2.**; deletes paragraphs **1.3.5.2.**, **4.11. (Added)**, **5.20.7.**, and 8.9. Removed all references to AFMC.

1.3.4. The Director, Acquisition Systems Protection (SMC/AXP) is SMC's Information Security Program Manager (ISPM) for all SMC organizations and other organizations supported by SMC on Los Angeles AFB or in the Los Angeles area.

1.3.5. For the purpose of this supplement, the term "unit commander" encompasses System Program Directors, Directors, Chiefs of staff agencies, or equivalents.

1.3.5.1. The term Acquisition Systems Protection Managers (ASPMs) will be used for security managers who are in the Security Specialist career field. ASPMs within SMC System Program Offices will perform all duties of a Security Manager for their organization as described in DoD 5200.1-R/AFI 31-401 and this supplement.

1.3.6.1. Use the guidance contained in DoD 5200.1-R/AFI 31-401 and this supplement to implement unit Information Security Programs.

1.3.6.2. Acquisition Systems Protection Managers (ASPMs)/Unit Security Managers (USMs) must establish a Security Manager's Handbook. The book must contain letters of appointment, copies of last SMC/AXP Integrated Protection Review (IPR), Security Operating Instructions, Semi-Annual Security Inspection Reports, Security Manager's Meeting Minutes, Information Letters, Inspection Checklists and other items pertinent to their organizational security programs. Maintain 2 years of Integrated Protection Reviews (IPR) reports. Include other unit security documentation; i.e., Industrial Security, Personnel Security, Operations Security (OPSEC), and Computer Security (COMPUSEC) applicable to the overall unit security program.

1.3.6.2.1. (Added) Prepare a unit Security Operating Instruction (OI) using the SMC/AXP Security OI template.

1.3.6.4.1. (Added) ASPMs/USMs are required to attend SMC/AXP conducted annual Security All Calls/Security Manager Meetings.

1.4.2.1. (Added) SMC/AXP will conduct annual IPRs of each organization that handles, stores, processes or has access to classified information. IPRs serve two primary purposes: (1) identify and benchmark security processes/products within a program for crossfeed to all SMC organizations, and (2) identify security short falls within a program and recommend corrective action. The IPR team uses a random sampling method; but the review will be sufficiently thorough to determine the overall effectiveness of the unit's protection program.

1.4.2.2. (Added) Upon completion of the IPR, the commander/director/staff agency chief will be provided a formalized briefing (as applicable) and a written report indicating the status of their security program. Corrective actions will be implemented as soon as possible. When serious program deficiencies are identified, a letter of response to SMC/AXP is required from the commander/director/staff agency chief indicating the applicable corrective measures taken. A copy of the report must be maintained in the Security Manager's Handbook for two years.

1.4.2.3. (Added) The interval between IPR may be extended to two years when an organization has relatively small classified holdings and results of other visits reflects the organization has a strong Information Security Program.

1.4.3.2. (Added) Ensure that contractors performing work at LAAFB on Visitor Group Agreements or classified contracts for your organization are covered under the organization's self-inspection program.

1.7.1. Security Managers will submit SF Form 311, Agency Information Security Program Data (available at <http://www.gsa.gov/forms>), to SMC/AXP by 15 August of each year.

2.1.2.3.3. (Added) Only the individual occupying the position of SMC/CC, as well as AFPEO Space, has been delegated by SAF as an Original Classification Authority (OCA) for Top Secret and further delegation is not authorized. Any SMC organization requesting delegation as an OCA must submit a request with full justification to SMC/AXP for processing through ISPM channels in accordance with para 2.1.2.4.

2.3.1.3. (Added) Keep a suspense copy of the classification challenge letter with the classified information/material in question until final determination is provided by the OPR.

2.4. SMC's Program Protection Plans (PPPs) and existing System Protect Guides must contain required collateral security classification determinations for the program in accordance with SMC/CC's approved

Space Program Protection Planning Guide (SP³G). Formal coordination with SMC/AXP, as the designated ISPM for SMC, is required and will be documented in the PPP.

2.4.1. SMC/AXP maintains copies of PPPs, SPGs and associated security classification guides (SCGs) for all SMC programs. SMC Program Directors/Program Managers will conduct biennial reviews of their PPPs to ensure security classification, threat, and vulnerability currency and provide SMC/AXP with a record.

4.7.1. (Added) Classified diskettes/CDs must be marked externally with the Office of Primary Responsibility, overall classification level, and date. Internal files must be marked with the date of creation, classification & declassification instructions, additional warning notices, as applicable, and page and paragraph markings.

4.7.2. (Added) Unclassified diskettes must be marked externally with the Office of Primary Responsibility and dated.

4.7.3. (Added) Apply overall classification marking to the front, back, and spine of all classified media, to include the container of the media (CD, VCR and cassette tape jackets). Apply all applicable associated markings to the media as prescribed in DoD 5200.1-R/AFI 31-401.

4.7.4. (Added) Mark and control digital cameras used for classified filming with the highest classification of the information contained within, and other applicable associated markings as appropriate.

4.8.2. SMC/IN performs SSO functions for all SMC organizations.

4.9. (Added) Amendment to E.O. 12958 extended the deadline to 17 April 2003 for non-exempt records and 17 Oct 2001 (see para 3.2.1.1) for permanent records to ensure that all classification markings required by the Executive Order 12958, Classified National Security Information, are applied to original and derivative classified information.

4.10. (Added) All classified material must reflect a date of creation either on the classified material itself or within an applicable Technical Order/Security Classification Guide/System Protection Guide/Program Protection Plan.

4.11. (Added) Mark file dividers on the top, bottom and tab with the highest classification.

4.12. (Added) The absence of "NOFORN", or equivalent markings on documentation of any kind is not authority for release to a foreign government, representative, or international organization. This applies to classified national security information and unclassified controlled information requested by a foreign citizen. Contact your ASPM/USM, or SMC/AXP Foreign Disclosure Office for guidance on obtaining authorization for disclosure of information, unless it has already been cleared for public release by SMC/PA.

4.13. (Added) The last page of a document will be considered its back cover unless there is a clearly discernible separate page serving as the cover. Mark the back cover as required in the DoD 5200.1R.

4.14. (Added) For Official Use Only (FOUO) markings refer to DoD 5400.7R, Freedom of Information Act program, Chapter 4, as supplemented by AF and AFSPC.

5.4.1.5. (Added) As a additional option, SMC personnel may verify security clearance eligibility and completion of the SF 312, Nondisclosure Agreement, with SMC/AXP. Need-to-know must be determined by the possessor of the classified material/information. SMC organizations will not require formal visit request documents of other SMC organizations.

5.5. **NOTE:** Submit signed/resigned SF Forms 312, Nondisclosure Agreements, to SMC/AXP for entry into Sentinel Key. AXP will send the SF 312s to either Civilian Personnel or Military Personnel as applicable.

5.5.3.4. (Added) Immediately notify SMC/AXP when an individual refuses to sign a SF 312, Nondisclosure Agreement.

5.6.9. SMC/AXP is the AFSPC designated Foreign Disclosure Office for all foreign visits and disclosure for all SMC organizations and The Aerospace Corporation. SMC/AXP must be notified immediately when a foreign visit to any SMC organization is to occur or any SMC personnel are going to visit a foreign national/country.

5.7. SMC organizations will send a visit request letter with the following information to the visit location.

Name, Grade, and Position Title

Nationality, Date, and Place of Birth

Duty Address

Level of Security Clearance

Date/Duration of Visit

POC to be Visited

Purpose

Signature (Security Managers), Grade, Title, Phone #, & Date

5.10.1. SMC/AXP must be consulted before any SMC organization establishes a Top Secret account.

5.10.4.1. (Added) Record NATO briefing completed for access to NATO classified information on the AF Form 2583, Request for Personnel Security Action. Maintain the forms in the Security Manager Handbook

5.11.3. (Added) Annotate the SF 702, Security Container Check Sheet, each time the container is opened and closed and again at the end of each duty day. If the container was not opened, annotate the SF 702 with "NOT OPENED" or line through the applicable row. Ensure that the "check by" block is initialed and the time is recorded. Include weekends and holidays when personnel are working.

5.11.4. (Added) Safeguard Federal Express packages and United States Postal Service First Class Mail bearing the notice "Postmaster: Do Not Forward" as classified information at the Secret level until you confirm the contents. If the above material has not been verified at the close of business (COB), secure the material in a GSA security container or an approved vault/secure storage room. For organizations that do not have secure storage capability, contact 61 ABG/DO (Command Post) to store overnight.

5.12.1. (Added) Each SMC organization that possesses classified, FOUO, unclassified controlled information (UCI) information, or Automated Information System (AIS) equipment will conduct an end-of-day security check to ensure the material is stored/secured appropriately. Individuals must be designated in writing to conduct end-of-day security checks and post SF 701, Activity Security Checklist.

5.15. A DepSecDef Memo, dated 26 Oct 01, rescinds subparagraph 6-307b of DoD Regulation 5200.1-R, dated January 1997. Portions or sessions of classified meetings, conferences, etc., shall be limited to appropriately cleared U.S. government or U.S. government contractor locations".

5.15.2. SMC/AXP performs this approval authority on behalf of SMC/CC. Organizations requiring recurring secure conference facilities under their control must contact SMC/AXP prior to use for an information and physical security assessment.

5.15.3. SMC/AXP is the designated Foreign Disclosure Office and must be coordinated with prior to any SMC organization hosting a conference, symposium, or other security meeting involving foreign nations.

5.17.1.1. (Added) Reproduction equipment, to include microfiche readers/printers, must be approved prior to classified use by 61 CS. SMC/AXP can conduct an on-site survey of the proposed location and review the unit operating instruction outlining procedures for protecting classified information during the reproduction process. If possible, locate reproduction equipment in areas under constant surveillance of personnel responsible for enforcing rules against unauthorized use or in lockable areas/rooms. Once approval is obtained, post Classified Reproduction Rules near the reprographic equipment.

5.20.1.4. (Added) SMC/AXP is the approval authority for construction/modification of unattended collateral classified storage areas, secure storage rooms and vault-type rooms. All such plans will be coordinated with SMC/AXP prior to use. Initial requests for certification will be accomplished via a letter from the requesting organization. Unattended classified storage areas will meet, as a minimum, the physical security standards identified in DoD 5200.1-R, Appendix G. Upon approval, a Secure Storage Room Certificate will be issued to the requesting organization, to be posted within the certified area. Certification will be re-accomplished at a minimum, every three years.

5.20.4.1. (Added) Security containers with a built in Sergeant & Green leaf or Mosler locking devices may continue to be used to store SECRET and CONFIDENTIAL information until the locking device becomes inoperative; i.e., due to wear & tear or a lockout. Organizations must install the MAS-Hamilton X-08 or other certified mechanical locking mechanism IAW Federal Specification FF-L-2740 in order to store classified information. Classified security containers storing TOP SECRET and/or Special Access Program (SAP) information must install the MAS-Hamilton X-08 locking mechanism or equivalent locking device IAW Federal Specification FF-L-2740.

5.25.1. (Added) Any Civil Service Job Series 0080 security specialist or military AFSC equivalent can perform preventive maintenance inspections on approved GSA security containers as required by AFTO 00-20F-2, Inspection and Preventive Maintenance Procedures for Classified Storage Containers. The inspection is conducted following instructions in paragraph 7 of the AFTO. Record the inspection on AFTO Form 36, Maintenance Record for Security Type Equipment.

5.28.3.1. (Added) The second Thursday of March is the annual clean-out day for SMC organizations.

5.29.1.1. (Added) Before procuring any destruction equipment, contact SMC/AXP for the NSA Approved Destruction Devices list used for classified information. Mark it with "Unauthorized Shredder for Classified Destruction" or "Authorized Shredder for Classified Destruction" on the destruction equipment.

5.29.1.2. (Added) SMC/AXP established procedures for use of the Los Angeles Air Force Base destruction equipment located in Building 100. The equipment is capable of destroying paper products, communication tapes, carbon paper, ribbons, film, microfilm, microfiche, floppy disks and magnetic cards. Contact AXP to schedule an appointment to use the base destruction equipment.

6.1.7. (Added) Commanders will designate in their unit security operating instruction internal Official Mail Distribution Points within their organizations.

6.4.1.2. (Added) Use an opaque pouch, brief case or similar outer container when handcarrying classified information on Los Angeles AFB. This procedure includes message pickup and delivery from/to the Communications Center. Protect classified material with an appropriate cover sheet while in transit on Los Angeles AFB. Do not mark the exterior pouch/container with classified markings.

6.5.3. (Added) Coordinate with SMC/AXP prior to transmitting any classified material or unclassified controlled information to a foreign government.

6.6.1.1. (Added) When transmitting classified material ensure the inner container is marked with any additional warning notices that appear on the document. This avoids the possibility that unauthorized individuals will access the material.

6.8.1. (Added) Personnel handcarrying classified information within the confines (Areas A, B, & Aerospace complex) of Los Angeles AFB remain subject to exit/entry inspections when passing through controlled area entry points. To expedite an individual's movement during these checks, provide written authorization to personnel who regularly handcarry information/material. Use DD Form 2501, Courier Authorization Card, or a courier letter signed by the program director, chief of staff agency or security manager. The DD Form 2501 will be stored within the organization when not utilized by authorized personnel.

6.8.2. (Added) An official courier letter to handcarry classified information/material and an exemption notice affixed to the package is required when an individual will be departing the confines of Los Angeles AFB. Courier letters must include the individual's full name, social security number, organization, description of packages (i.e., how many, size, addresses, etc.), the point of contact and phone number for verifying the information and an expiration date. The exemption notice must include the organizations full address, official business, the notation that this information is exempt from examination, and the program director, chief of staff agency, or security manager's signature. (see **FIGURE 6.1 (Added)** for an example of a courier letter and **FIGURE 6.2 (Added)** for an example of an exemption notice).

6.10. (Added) **Transmitting NATO Classified Information** . (Reference AFI 31-406, Chap 6, 1 April 00)

6.10.1. (Added) Requests to handcarry NATO classified information outside the continental United States aboard commercial aircraft must be forwarded through SMC/AXP for approval.

6.10.2. (Added) All incoming and outgoing NATO Classified information must go through NATO Control Point. Space Command will send the NATO documents directly to the action offices as applicable.

6.10.3. (Added) When NATO classified information is permanently transmitted outside your activity; use an AF Form 310, Document Receipt and Destruction Certificate. For documents loaned out on a temporary basis record the location, date signed out, and the name and address of the individual (on loan basis should be no longer than 72 hours). Maintain records of accountability for two (2) years.

FIGURE 6.1 (Added) SAMPLE COURIER LETTER

MEMORANDUM FOR (ORGANIZATION)

FROM: (ORGANIZATION)

SUBJECT: Designation of Official Courier Letter

1. Mr. Albert Johnson, SSAN: 122-69-9932, 412 TW/FG, Edwards AFB, California 93524-0001, is designated an official courier for the United States Government. Upon request, he will present official identification.
2. Mr. Johnson is handcarrying four sealed packages, size 9" X 8" X 24" addressed from 2420 Vela Way, Suite 1467, Los Angeles AFB, El Segundo, California 90245-4659, and addressed to HQ AFSPC, 18 Mellow Drive, Peterson AFB, CO 45433-0002. Each package is identified on the outside of the package with the marking "OFFICIAL BUSINESS – MATERIAL EXEMPTED FROM EXAMINATION" bearing the signature of the undersigned.
3. Mr. Johnson is departing Los Angeles International Airport with a final destination to Dayton International Airport. He has a transfer point of Dallas-Fort Worth International Airport.
4. This courier designation can be confirmed by contacting the undersigned at 412 TW/FG, area code (805) 277-1111. This letter expires on (date of return to Los Angeles AFB).

(signature of program director, chief of staff
agency, or security manager)

FIGURE 6.2 (Added) EXEMPTION NOTICE

<p>Department of the Air Force</p> <p>Space Missile Command</p> <p>Los Angeles AFB, California</p> <p>Official Business</p> <p>MATERIAL EXEMPT FROM EXAMINATION</p> <p>(Program Director, Director/Chief of Staff Agency or Security Manager)</p>
--

7.1.1. With the exception of SMC/IN, who controls all SCI Programs for Los Angeles AFB, to include tenant organizations, any SMC organization contemplating establishing a Special Access Program must coordinate with SMC/AXP prior to contacting external SMC organizations.

8.3.6.5. (Added) Use the SMC Security Education & Training Guide, January 2001 to help conduct and satisfy quarterly security education training requirements.

8.10.4.6. (Added) Foreign Travel. Security Managers must provide a foreign travel briefing to individuals who perform personal foreign travel. The Foreign Travel Program should consist of reporting procedures, applicable threat information and briefing/debriefing requirements. The Det 110, AF Office of Special Investigations can assist organizations by furnishing applicable threat information.

8.11.1. Because of the volume of information to be covered, recurring and refresher training should, as a minimum, be presented in semiannual sessions. Quarterly sessions are recommended for maximum motivational and retentive effect.

8.14.4. (Added) Provide AF Form 2587 to SMC/AXP with signature of individuals.

8.16.3. SMC/AXP is the focal point for all host/sponsored on site security training for SMC organizations and will be coordinated with prior to conducting such training.

9.4. Immediately report security incidents/violations involving Sensitive Compartmented Information (SCI) to SMC/INS.

9.7.2.2. SMC/AXP will accomplish these notifications for all SMC organizations.

9.8.1.2. Security incidents involving collateral issues of high visibility or involving multiple organizations will be conducted by personnel assigned to the Director, Acquisition Systems Protection, SMC/AXP. This allows for a complete look at the incident and avoids potential conflicts of interest. If in doubt, contact SMC/AXP.

9.8.1.3. (Added) Preliminary inquiry officials should have no other assigned duties while conducting required inquiries.

9.8.1.4. (Added) At Los Angeles AFB, take the following actions.

9.8.1.4.1. (Added) Security Managers must contact SMC/AXP and briefly describe/discuss preliminary facts surrounding the violation, obtain a control number and guidance/assistance. The appointing authority will forward a copy of the appointment letter to SMC/AXPI. Inquiry officials will contact the organization's Security Manager to obtain an initial briefing on the security incident and administrative inquiry/investigation guidance.

9.8.3.1. (Added) The appointing official will review the report for adequacy and initiate appropriate corrective action/disciplinary action. Based on the findings in the preliminary report, the appointing official decides whether to open a formal investigation or close the inquiry. The report will indicate administrative corrective action(s) and/or disciplinary action(s) and coordinate with staff judge advocate, civilian and military personnel offices, as appropriate. Forward completed reports to SMC/AXP.

9.11.3.2. SMC/AXP is the reviewing authority for all preliminary inquiries. Upon review of the final preliminary inquiry report, facts may indicate further investigation. SMC/AXP will notify the appointing official to initiate a formal investigation, as appropriate.

A3.1. For protection of For Official Use Only (FOUO) information, see DoD Regulation 5400.7/AF and AFSPC Supplement, Freedom of Information Act Program, 22 Jul 99, which superseded AFI 37-131.

BRIAN A. ARNOLD, Lieutenant General, USAF
Commander