

**BY ORDER OF THE COMMANDER,
51ST FIGHTER WING**



AIR FORCE INSTRUCTION 31-401

51ST FIGHTER WING

Supplement 1

9 FEBRUARY 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: 51 SFS/SFAI (TSgt Kerry K. Waldrip)
Supersedes AFI 31-401_51 FW/SUP 1,
7 February 2002

Certified by: 51 MSG/CC (Col. Robert D Kopp)
Pages: 11
Distribution: F

This supplement implements changes detailed in AFI 31-401, Information Security Program Management, and applies to all assigned, attached, geographically separated units (GSUs), tenant units and staff agencies under the 51st Fighter Wing security program.

SUMMARY OF REVISIONS

AFI 31-401, was substantially revised. Therefore, the 51 FW supplement is revised considerably and must be completely reviewed. Revised supplement to conform to the renumbering of AFI 31-401. Added attachments to provide security managers a guide for the following: completing security manager appointment letters, establishing a security manager handbook, sample semiannual self-inspection report format, and classified emergency protection procedural guide. Added the requirement for annual Top Secret inventories to be conducted in January. Clarified DD Form 2501, Courier Authorization, requirements when hand-carrying classified materials.

AFI 31-401, 1 November 2001, is supplemented as follows:

1.3.4. Approval authority for Open Storage and Visitor Group Security Agreements is delegated to the Osan AB senior Security Forces official, 51 SFS/CC.

1.3.4.7. 51 SFS/SFAI will conduct security manager meetings at least quarterly. The primary or alternate security manager must attend. Attendance by geographically separated units (GSUs) while not mandatory is strongly encouraged.

1.3.5.1. Notify 51 SFS/SFAI, within ten days, in writing when a new primary or alternate security manager is appointed ([Attachment 1](#)).

1.3.6.1. Develop a unit security manager handbook. Set up according to the example format ([Attachment 2](#)).

1.3.6.2. Develop security procedures unique to the unit's security operations and include these requirements in a unit operating instruction. Review and update annually.

1.3.6.6. Conduct unit semiannual self-inspections not later than six months following an annual Information Security Program Review. Program reviews as described in paragraph 1.4.2.2. (Added) below may substitute for a semiannual self-inspection. Inspectors should use the Information, Personnel, and Industrial Security Inspection checklist provided by the 51 SFS/SFAI. Follow the proper report format (Attachment 3) to record inspection results and findings. Endorsement by the unit commander is required.

1.4.2. 51 SFS/SFAI will conduct annual information security program reviews on all non-exempt 51 Fighter Wing agencies.

1.4.2.1. (Added) Osan AB agencies exempted from annual information security program reviews are 303rd Intelligence Squadron (7th Air Force Special Security Office) and 18th Intelligence Squadron, Detachment 2.

1.4.2.2. (Added) Program reviews are examinations of a unit's Information, Personnel, and Industrial Security programs. Program reviews are not "compliance inspections" and they are not rated. Instead, they are "assistance" oriented visits to identify noteworthy and problem areas in the security program of the activity visited. The information security program manager may use a random sampling method, but the examination will be extensive enough to determine the overall status of the unit security program.

1.4.2.3. (Added) Unit commanders and staff agency chiefs will review the program review reports and, when necessary, take appropriate corrective action on problem areas identified in these reports. Replies to program review reports are not generally required; however, unsatisfactory reports and corrective actions taken to remedy serious management deficiencies will be documented and reported to the 51 Fighter Wing Commander.

1.4.3. Unit commanders or staff agency chiefs will appoint, in writing, an individual to conduct the unit semiannual self-inspection. Security managers will not inspect their own programs but will monitor and assist as necessary. Cross inspections, which permit one unit security manager to inspect another, are encouraged. The inspection of each element of the security program may be made on the basis of a random sampling, but the inspection must be thorough enough to show compliance with required security directives. The individual conducting the inspection will forward a written report of findings to the unit commander or staff agency chief, which reviews it to determine adequacy of the inspection and specifies the corrective actions to be taken. A copy of the report will be forwarded to 51 SFS/SFAI. A copy of the report will be provided to the appropriate security manager for file in the security manager's handbook.

5.10.1. Units or agencies having a need to store Top Secret material must contact 51 SFS/SFAI prior to, or immediately after, receipt. 51 SFS/SFAI will train all appointed Top Secret Control Officers (TSCOs).

5.10.1.3.1. Annual inventories or audits of Top Secret Control Accounts (TSCAs) will be conducted during the month of January, or whenever the TSCO changes.

5.13.2. Commanders wishing to remove Secret and/or Confidential material from designated work areas during non-duty hours must request approval to store the material in their residence. Approval authority is MAJCOM through the information security program manager. The residence must be located within the geographic confines of Osan Air Base and have an approved storage container.

5.13.3. Commanders wishing to store classified material at their residence must have written procedures (procedures can be included in the Unit Operating Instruction). As a minimum, procedures will include

arrangements for notifying the responsible activity to pick up the classified container and material in the event something happens to the user. Consider other factors in written procedures, to include measures to prevent access by foreign nationals in the residence.

5.14.1. The following locations are authorized overnight classified repositories on Osan Air Base:

5.14.1.1. (Added) Base Operations, Bldg. 882, 51 OSS/OSM, DSN 784-4288 (for aircrews only).

5.14.1.2. (Added) 7 AF/51 FW Command Center, Bldg 1097, 51 FW/OCO, DSN 784-7000.

5.14.1.3. (Added) 7 AF/SSO, Bldg 940, DSN 784-6445 (SCI only).

5.14.2. The storage of off-loaded pallets containing classified materials during deployments and contingencies will be temporarily stored in the security cage at Bldg. 632. This room is approved for the storage of classified information at the Secret/US level.

5.16.1. The aircraft will be parked in the mass parking restricted area, if parking is available, and demarcated with an elevated barrier. Entry to the aircraft will be controlled by owner/user, and continuous surveillance will be maintained on the aircraft.

5.17.1. The Defense Automated Printing Service (DAPS) on Osan Air Base will be contacted prior to reproducing classified information on copier machines (DSN 784-5518). DAPS will determine if the copier machine retains latent images and specifies how to clear the images when they do. This service can be conducted telephonically for GSUs.

5.19. All security containers under the 51st Fighter Wing Information Security Program, to include GSUs, will be inspected by the 51st Civil Engineer Squadron Locksmith or a qualified locksmith at the GSU prior to use. Ensure the locksmith is NOT a local national prior to the inspection. All security containers will have a label affixed designating a name of the container (e.g. SFAI 1 and SFAI 2 if two safes are owned by that office).

5.20.4. Initial surveys of classified vaults, secure rooms, or open storage locations under the 51 Fighter Wing Information Security Program, to include GSUs, will be inspected by 51 CES and 51 SFS/SFAI and approved for storage by the 51 SFS/CC.

5.20.5. (Added) 51 CES, Project Design Office will notify the 51 SFS facility project representative or 51 SFS/SFAI to review all initial and follow-up facility construction projects that are designed to store classified information.

5.24.1. 51 FW Information Security Program participants, to include GSUs without a locksmith on site, will notify 51 CES Locksmith for security container lockouts and repairs. GSUs requiring onsite service must be prepared to provide fund site for the 51 CES Locksmith TDY (travel and per diem) if a qualified locksmith is not available at the GSU.

5.28.3. All approved routine destruction of classified material not accomplished on an approved shredder must be accomplished at one of the below destruction centers on Osan Air Base. Individuals requiring the use of these facilities must notify the agencies no later than two days prior to the destruction date.

5.28.3.1. (Added) 303rd Intelligence Squadron (7 AF/SSO), Bldg. 301 (SCI only).

5.28.3.2. (Added) 51 Medical Group, Bldg. 777 (will only be used during emergency conditions).

5.29.3. (Added) Regarding emergency protection, removal, and destruction of classified information, each unit is responsible for developing emergency procedures tailored to meet unit needs. Use **Attach-**

ment 4 as a guideline in establishing procedures unique to the unit's classified operations. Maintain a copy of the plan on each security container. Units must practice their emergency plan annually. Record the results and file in section nine of the security manager handbook.

6.3.2.1. (Added) Units or agencies will only allow personnel with security clearances to receipt for registered mail. All registered mail must be protected as classified information until it can be determined otherwise.

6.6.3.1. (Added) Osan Air Base personnel will not enter classified materials into the Base Information Transfer Center (BITC) mobile service. Hand-carry the classified material to BITC, Bldg 995, DSN 784-1189.

6.6.3.2. (Added) When classified material is hand-carried on base (outside the unit or activity), a briefcase may serve as the outer wrapper. The inner envelope will be marked with the classification of the information, to include the unit address.

6.8. Use DD Form 2501 and an authorization letter (to include a sealed package examination exemption notice letter) signed by the unit commander, staff agency chief, or security manager when hand-carrying classified materials off the installation. Refer to AFI 31-401/PACAF Sup 1, **Attachment 1** and **Attachment 2** for courier authorization letter and sealed package examination exemption notice letter templates. Refer to DoD 5200.1-R paragraph C7.3.2.2.3 for DD Form 2501 disposition.

6.8.1. (Added) The DD Form 2501 is not required when hand-carrying classified information to and from activities within the installation during normal day-to-day operations, except when transporting the material through an entry control facility (e.g., restricted area, controlled area, etc.).

6.8.2. (Added) 7 AF/SSO is exempt from issuing DD Form 2501 to classified couriers during contingencies and exercises. 7 AF/SSO will supplement the DD Form 2501 by using local courier authorization designation and exemption from examination letters.

6.8.3. (Added) The entry controller will stop individuals not in possession of a valid DD Form 2501 or courier authorization/exemption from examination letter when entering an entry control facility. The entry controller will contact the unit being visited, and that unit will escort the classified material in and out of the facility or area. The entry controller will verify the escort has a DD Form 2501 or courier authorization/exemption from examination notice in their possession prior to the exchange of classified materials. DD Form 2501 exempts the materials from examination.

6.8.4. (Added) DD Form 2501 will be carried by individuals hand carrying classified information during increased Force Protection Conditions Bravo, Charlie, and Delta. The DD Form 2501 exempts classified packages from examination at facility entry and inspection points.

6.8.5. (Added) When emergency situations occur during increased Force Protection Conditions Bravo, Charlie, and Delta (e.g., relocation of wing, group, or unit control centers, etc.), individuals do not need to be in possession of DD Form 2501 when transporting or relocating classified information.

8.3.5.6. Training efforts of unit security managers will be announced at Security Manager meetings. Criteria for selection will be based on attention to detail in the following categories:

AF Forms 2586, Unescorted Entry Authorization Certificate, (attention to detail)

AF Form 2586 Approving Official Memorandums

Annual Program Reviews and Self-Inspections

Clearance Data Survey Submissions

EPSQ Package Submissions

ISPM Requests with Suspense

Security Inquiries / Investigations

8.3.5.7. Security managers will establish an annual information security program training plan as outlined in AFI 31-401 para 8.3.6. Provide each cleared and uncleared individual initial information security orientation and quarterly security refresher training. Security managers must maintain documented initial and refresher training.

8.6. 51 SFS/SFAI will provide training to Original Classification Authorities (OCA) within 30 days of appointment. Training must be conducted prior to OCA authority being exercised.

9.2.1. Report security violations no later than the end of the duty day on which the incident occurred to 51 SFS/SFAI, 784-6866. 51 SFS/SFAI will assign a case number for each security violation.

9.3.1. (Added) 51 SFS/SFAI will brief the preliminary investigating official on his/her responsibilities and provide assistance as needed. The preliminary inquiry official will complete an investigation report using the format as prescribed in PACAF PAM 31-2, Attachment 2. All investigations will be completed no later than 10 duty days after the incident was reported to 51 SFS/SFAI.

Attachment 1

SECURITY MANAGER APPOINTMENT LETTER TEMPLATE

(APPROPRIATE LETTERHEAD)

(Date)

MEMORANDUM FOR 51 SFS/SFAI

FROM: (YOUR UNIT)/CC

SUBJECT: Security Manager Appointment Letter

1. The following individuals are appointed Unit Security Managers for the (Your UNIT):

<u>POSITION</u>	<u>NAME/RANK</u>	<u>RANK</u>	<u>OFF SYM</u>	<u>PHONE</u>	<u>DEROS</u>
-----------------	------------------	-------------	----------------	--------------	--------------

PRIMARY

ALTERNATE

2. The security managers e-mail addresses are XXXX.XXXXXX@osan.af.mil and xxxx.xxxxxx@osan.af.mil. Their fax number is 784-XXXX.

3. This letter supersedes letter dated 04 Oct 00, same subject.

COMMANDER'S SIGNATURE BLOCK

Commander

NOTES:

1. Do not include any other information on this letter (e.g., SSAN, dates trained, etc.).
2. Separate letters are completed for authorizing signatures on AF Form 2586 and DD Form 2501.

Attachment 2

SECURITY MANAGER HANDBOOK FORMAT

A2.1. Section 1, Designation Letters (i.e., security manager appointment letter, Top Secret Control Officer appointment letters, other security related appointment letters, and copies of security manager training certificates).

A2.2. Section 2, Internal Information Security Operating Instruction. Tailor the unit's information security operating instruction (OI) according to how you plan to protect your classified information and implement your security program. Review annually.

A2.3. Section 3, Semiannual Security Self-Inspection Reports. Inspectors should use the Information/Personnel/Industrial Security Inspection checklist provided by 51 SFS/SFAI. The last two semiannual self-inspection reports must be maintained in the handbook. These will be reviewed during the annual Information Security Program Review.

A2.4. Section 4, Annual Information Security Program Reviews. These reviews are conducted by 51 SFS/SFAI and consist of reviewing a representative sampling of the Information, Personnel, and Industrial (if applicable) Security Programs but they are extensive enough to gauge their effectiveness. The last two annual program reviews must be maintained in the handbook.

A2.5. Section 5, Quarterly Security Manager Meeting Minutes. Security managers are required to attend these meetings. These meetings are designed to keep security managers abreast of all policy and procedural changes taking place in the program. A copy of the last four quarterly meeting minutes will be maintained in the security manager's handbook.

A2.6. Section 6, Information Letters. You will receive numerous information letters on the security program throughout the year. These letters are provided to help you administer your security program. Maintain information letters for as long as they apply and are useful to your program. Periodically purge this section of obsolete, rescinded, or superseded information.

A2.7. Section 7, JPAS. Maintain a current unit JCAVS roster. The security manager must be a registered member of JPAS to obtain access to the program. If the security manager can not access JPAS, or can not generate reports through JPAS, the security manager will maintain a roster with applicable security information for all members of the unit. Notify 51 SFS/SFAS, DSN 784-2287/6766, for access information.

A2.8. Section 8, Inspection Checklists. Maintain the checklist as prescribed in PACAFDIR 90-215/12 November 1999 (Information/Personnel/Industrial Security).

A2.9. Section 9, Miscellaneous Items. Any items not covered in other sections of the handbook can be filed here. Periodically purge this section to remove outdated information. Items that may be included are a consolidated listing of all safes, vaults, and secure storage areas assigned to the unit; lost restricted area badge letters; security education training plan; AF Form 2586; AF Form 2583, Request for Personnel Security Action; classified emergency protection procedures and results, etc.

Attachment 3**SAMPLE SEMIANNUAL SELF-INSPECTION REPORT FORMAT**

(Date)

MEMORANDUM FOR (Inspected Unit Commander/Staff Agency Chief)

FROM: (Inspecting Official's Rank/Name/Unit/Office Symbol)

SUBJECT: Semiannual Security Inspection

1. Authority And Date Of Inspection: This inspection was conducted on (date(s)) under the authority of DoD 5200.1-R, Information Security Program and AFI 31-401, Information Security Program Management.
2. Personnel Contacted: Identify Key Personnel.
3. Inspecting Personnel: Self-explanatory.
4. Summary: The inspection should inquire into procedures for handling and safeguarding classified material. Further, check the security education, Personnel Security, and Industrial Security Programs, if applicable. Inspect each element of the security program on the basis of a representative sampling but extensive enough to evaluate practices in effect for compliance with regulatory guidance. Note any changes (improvements or otherwise) in the overall security program since the last inspection. Identify any repeat discrepancies or other conditions that could result in the loss or compromise of classified material. Ensure you utilize the self-inspection checklist provided by 51 SFS/SFAI. Results of the unit's efforts during the annual classified reduction day in January must be recorded in this report.
5. Findings: Make a comment on each element examined. List the good as well as deficient areas. Include a specific "Recommended Corrective Action" on noted discrepancies. Using checklists provided and following this suggested format will assure you address key program areas.
 - a. Security Education: Is there a program, and how effective is it? Does it include, as minimum, initial and quarterly refresher training? Is training documented?
 - b. Classified Document Handling and Storage:
 - (1) Classification, Declassification, and Downgrading.
 - (2) Marking.

- (3) Retention.
- (4) Safekeeping and Storage.
- (5) Access, Dissemination, Transmission, and Accountability.
- (6) Reproduction Controls.
- (7) Disposal and Destruction.
- (8) Emergency protection, removal, and destruction plan.

c. Security Incidents: Have any security incidents occurred since the last inspection? If so, was appropriate action taken to prevent incidents from reoccurring?

d. Personnel Security Program: Do persons have the proper security clearance to perform the duty of the position they occupy? Have all personnel with a security clearance executed the SF Form 312, Classified Non-Disclosure Agreement? Are there any personnel requiring periodic reinvestigations?

e. Industrial Security Program: (If applicable)

6. Other Comments: Enter any other information not listed above but relating to overall management of the security program. This is a good place to recognize individual exceptional performance in following established security practices.

(Signature Block of Inspection Official)

1st Ind, (Commander/Staff Agency Chief)

MEMORANDUM FOR: (Unit Security Manager)

I have reviewed the inspection report and concur with the recommended corrective actions (unless otherwise noted). Please ensure discrepancies are corrected as soon as possible. Inform me of the status of any items which cannot be immediately corrected.

(Signature Block of Commander/Staff Agency Chief)

Attachment 4**EMERGENCY PROTECTION, REMOVAL AND DESTRUCTION OF CLASSIFIED MATERIAL****A4.1. Threat:**

A4.1.1. Natural Disasters. Osan Air Base has experienced severe rainstorms and flooding.

A4.1.2. Civil disturbance, terrorism, and enemy action. Osan Air Base is susceptible to civil disturbances from outlying communities. Terrorism is a threat that could be experienced at any military installation at any time. The threat of terrorist action increases with the level of the local Force Protection Condition (FPCON). The Defense Condition (DEFCON) increases with the increased threat of enemy action.

A4.2. Limiting Factors. There is no central destruction facility on the installation capable of destroying classified material within the time criteria specified by this plan. As a result, units must effectively plan and acquire enough routine and emergency destruction equipment to execute this plan.

A4.3. Execution:

A4.3.1. Phase I, Emergency Protection. Phase I will be implemented in the event of fire, natural disaster, bomb threat, civil disturbance, or in the case of an increased terrorist threat.

A4.3.1.1. Fire, Natural Disaster, or Bomb Threat.

A4.3.1.2. Secure material in approved security containers if time and safety permit. When personal safety is in jeopardy, evacuate the area and post individuals to control entry and emergency access (owner/user is responsible for the protection of his/her classified and facilities, Security Forces will not be used for this function).

A4.3.1.3. Allow only responding emergency crews to enter the facility (Fire Department, Medical Services, Security Forces, etc.). Classified custodians may enter the facility to account for the unsecured classified materials after the area is declared safe.

A4.3.1.4. No entry to the facility will be allowed until all classified material is accounted for.

A4.3.1.4.1. Civil Disturbance or Increased Terrorist Threat.

A4.3.1.4.2. Post personnel in classified storage areas, if the situation warrants. Posted personnel must be knowledgeable of procedures to request emergency assistance. Armed guards are not required.

A4.3.1.4.3. Prepare for the initiation of Phase II. Phase II is implemented when the possibility of conflict increases.

A4.3.2. Phase II, Precautionary Destruction:

A4.3.2.1. Segregate all classified into "mission essential" and "non-mission essential" categories.

A4.3.2.2. Retain mission essential classified material. Destroy non-mission essential classified material using routine classified destruction methods.

A4.3.2.3. Prepare for PHASE III.

A4.3.3. Phase III, Emergency Destruction:

A4.3.3.1. Phase III actions will be initiated upon the determination that an imminent threat exists of the installation being overrun. The effect of premature destruction is considered inconsequential when measured against the compromise of classified information.

A4.3.3.2. Each unit will predesignate a location for the emergency destruction of classified material and procure or manufacture sufficient equipment to accomplish the destruction process (i.e., modified trash cans, BBQ grill, etc.). If time does not permit you to use predesignated material, immediate destruction will be accomplished in any available container.

A4.3.3.3. Top Secret material holders must have the capability to destroy all holdings within one hour.

A4.3.3.4. Secret and Confidential material holders must destroy the materials within two hours.

A4.3.3.5. No destruction records are required under emergency destruction procedures.

A4.4. Notification:

A4.4.1. The Osan Command Center (per PACAFI 10-207, para. 1.1 and 1.2) will implement this plan by order of the installation commander or higher authority.

A4.4.2. The 51 FW Contingency Support Staff (CSS) will be formed upon implementation to track progress and ensure all units are notified.

A4.4.3. Any senior individual present in an area containing classified material, who determines there is a sufficient threat, may implement any portion of this plan.

A4.5. Preparation Instructions:

A4.5.1. Assign classified material one of the following priorities.

A4.5.1.1. Priority One: Top Secret, Controlled Nuclear Weapons Design Information.

A4.5.1.2. Priority Two: Secret.

A4.5.1.3. Priority Three: Confidential.

A4.5.2. Develop in-depth checklists to implement this plan. Post the checklists on the security container or on the primary entrance to vaults, secure storage rooms, and bulk storage rooms.

A4.6. Taskings:

A4.6.1. 51 SFS/SFAI. Maintain this plan IAW applicable directives.

A4.6.2. Osan Command Center. Ensure notification is made upon implementation of this plan.

MAURICE H. FORSYTH, Brigadier General, USAF
Commander