



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: 39 SFS/SFAP (TSgt Aretha Barnes)

Certified by: 39 SFS/CC
(Lt Col Timothy D. Ferguson)

Supersedes AFI31-401_USAFESUP1,
INCIRLIK SUP1, 1 May 2000

Pages: 10
Distribution: F

AFI 31-401, 1 November 2001, AFI31-401_USAFE SUP 1, 15 June 2002, is supplemented as follows: This supplement identifies the Installation Security Program Manager (ISPM) for Incirlik AB, establishes and significantly clarifies policies, procedures, and responsibilities for conducting semi-annual self-inspections, and the establishment of a Security Manager of the Year program. This supplement applies to all of Incirlik and its GSUs. This supplement also applies to the Air National Guard and the Air Force Reserve upon mobilization. . In general, it also establishes requirements for Top Secret Control Officers and alternates to be trained; for a security container inventory to include COMSEC containers; to have an accountability system for all classified material; for the development of emergency action procedures for each unit, for downgrading and declassification, for accountability procedures when reproducing classified; identifies temporary storage facilities for classified material on Incirlik AB; delegates the approval authority for classified meetings to the ISPM; for each unit to establish an operating instruction on Information Security Program Management regardless if they store classified; additional training requirements, as identified in DoD 5200.1-R, AFI 31-401 USAFE SUP1, and T.O. 00-20F-2; additional guidance for conducting security incident inquiries, investigations, and adds an attachment providing specific Security Manager program guidance. These specific procedures addressed are required actions for the Incirlik Air Base and its Geographical Separated Units (GSU) functions in general. Ensure that all records created as a result of processes in this supplement are maintained in accordance with AFMAN 37-123, *Management of Records* and dispose of in accordance with the Air Force Records Disposition Schedule (RDS). This supplement requires collection and or maintenance of information protected by the Privacy Act (PA) of 1974. The authorities to collect and or maintain the records prescribed in this supplement are Title 10 United States Code, Section 8013, 37 U.S.C. 301a, Public Law 92-204, P. L. 93-5704, and P. L. 93-294. Forms affected by the PA have an appropriate PA statement. System of records notice F060 AF A applies.

SUMMARY OF REVISIONS

This document is substantially revised and must be completely reviewed.

1.3.3. **Commander.** The Commander, 39th Air Base Wing (39 ABW/CC), has the overall responsibility for implementing and ensuring compliance with this supplement.

1.3.4. **Information Security Program Manager (ISPM).** The ISPM for Incirlik Air Base and its GSUs is the Chief, 39th Security Forces (CSF), who will manage the information security program through the auspices of the 39th Security Forces Squadron, Security Forces Administration office (39 SFS/SFA).

1.3.5.1. Individual commanders for each unit within the 39 ABW will appoint a primary and alternate security manager for their squadrons in writing. These letters of appointment will be forwarded to 39 SFS/SFA.

1.3.6. Security managers will comply with the additional program guidance outlined in **Attachment 17 (Added)**.

1.4.3. Unit commanders and equivalents of all activities within Turkey involved with processing or holding classified information will ensure personnel conduct semiannual security self-inspections to evaluate information security program effectiveness.

1.4.3.1. A knowledgeable person must be assigned to conduct self-inspections.

Security Managers will not conduct self-inspections within their own unit; however, they are normally the most qualified individuals to inspect programs outside their unit and commanders/staff agency chiefs are encouraged to utilize them in that role.

1.4.3.2. (Added) All semiannual self-inspections will be conducted during the second calendar quarter of each year (April-June). 39 SFS/SFA will conduct an information security program review of each unit during the last calendar quarter of each year (October-December). This review will satisfy the requirement for the second semiannual self-inspection.

1.4.3.2.1. (Added) Security Manager of The Year Program. In January of each year the ISPM and 39 SFS/SFA will evaluate all Information Security Program Reviews, attendance to security manager meetings, suspense's, etc for the selection process. The individual selected will be presented the award by the 39 ABW/CC.

2.3.1. Coordinate all challenges to classifications of Air Force material through 39 SFS/SFA, for review, prior to sending to the OCA.

2.3.2. Challenges to material not originated by Air Force personnel will be routed through 39 SFS/SFA to the OCA with an information copy to HQ USAF/XOFI.

5.10.1.1. **Top Secret Control Officer (TSCO) Appointment.** Units with a Top Secret Control Account will forward appointment letters identifying the Top Secret Control Officer and at least one alternate to 39 SFS/SFA.

5.10.1.1.3. (Added) **Top Secret Control Officer (TSCO) Training.** TSCO's and alternates must be trained within 30 days of appointment. 39SFS/SFA is responsible for conducting this training.

5.10.1.3.1. During the inventory, the commander and the users of the information will make a determination whether to keep or destroy the information.

- 5.10.1.3.4. (Added) The commander certifies the review of information by endorsing the inventory report. The report is then kept on file for two years.
- 5.10.2. Implement a documented accountability system (such as an inventory sheet) for all Secret material retained over 7 days, regardless of where the information is stored. Use an unclassified description of the material and file separately from the classified material. This will facilitate an assessment of a compromise.
- 5.11. Use AF Form 614, **Charge Out Record**, or similar form, when a document is removed from a security container.
- 5.11.3. (Added) Develop plans for the protection, removal, or destruction of classified material in case of natural disaster, fire, civil disturbance, terrorist activities, or enemy action. (Reference, DoD 5200.1-R, para 6-303). Include in your unit operating instruction.
- 5.13.2. Forward requests through 39 SFS/SFA to HQ USAFE/SFXI.
- 5.14.3. (Added) The primary 24-hour, temporary storage facility for classified material (transient air crew personnel) is Airfield Management, Bldg. 500 at ext 6-6837/6811/3286. The secondary facility is the 39 ABW/CP, Bldg 364 at extension 6-9920/9921/9922/3100. Couriers will ensure the material is properly packaged prior to storage. (Reference, AMCI 10-202, V2.9.5.)
- 5.15.1. The sponsoring unit who arranges the meeting will designate individuals to control entry to the conference room to guard against inadvertent access and to make sure all personnel attending the conference/meeting are authorized. Security Forces personnel will not be tasked for this function unless approved by the CSF.
- 5.15.2. The installation commander has delegated the approval authority for classified meetings to the ISPM (CSF).
- 5.15.6. (Added) Cellular phones, two-way radios, two-way beepers, and other electronic equipment that can receive and transmit a signal are prohibited in all offices and areas when classified and sensitive information is discussed. Owners of designated areas should make every effort to inform personnel of the prohibited use of electronic equipment, to include but not limited to posting signs and visual aids, and including the information in briefings and training, etc.
- 5.15.6.1. (Added) Due to the increasing advances in technology, if there is any question concerning the capabilities of an electronic device, the device will be left outside the area where classified information is being processed and/or discussed. The 39 CS/SCBIA (Information Assurance Office) will then be contacted immediately and AFI 33-202, *Network and Computer Security*, USAFE SUP 1 will be reviewed for further guidance.
- 5.17.1. Post visual aids at all machines (to include fax machines) approved for classified reproduction. At a minimum, post visual aids at all copy machines not authorized for classified reproduction.
- 5.20. Include COMSEC security containers in the memorandum that lists all security containers in the unit for accountability purposes only in case of emergency actions.
- 5.20.3.1. (Added) Post the storage facility approval notices, letters inside the approved area.
- 5.20.5. Contact 39 SFS/SFA and 39 SFS/SFOPR before ordering or installing alarms or designating any area as a controlled area for the purpose of storing classified material.

5.20.6. Upon completion of emergency destruction plans, all material must be clearly marked to facilitate its priority of destruction in an emergency situation.

5.20.7. (Added) Unit commanders and staff agency chiefs will ensure approved emergency destruction plans are tested to ensure designated actions will accomplish the desired task semi-annually to ensure all personnel are familiar with required actions.

5.23.2. All personnel having the combination will be recorded on SF Form 700, **Security Container Information**. An additional SF Form 700 may be necessary for containers with more than five users.

5.24.4. (Added) The Base Civil Engineer Service Desk(BCE) at ext 6-7008 will provide this service. Ensure that personnel annotate the AFTO Form 36, **Maintenance Record for Security Type Equipment**.

5.24.5. (Added) A visual and operational inspection of the safe for cleanliness and serviceability should be done on a frequent basis, upon change of custodians, and/or when the combination is changed. As a minimum, an inspection will be conducted upon initial procurement (by BCE) and prior to being placed into service and every 5 years thereafter by a locksmith certified to inspect GSA security containers approved for the storage of classified material (BCE) and annotated on the AFTO Form 36. (Reference, TO 0-20F-2)

5.24.5.1. (Added) Changing of safe combinations is the owners responsibility. Organizations can request safe combinations changed can call BCE for scheduling at ext. 6-7008. Users are requested to give BCE eight working hours notice prior to any combination change; however, emergency safe repairs will be given top priority. Safe users who are experiencing problems opening or closing their safes should call BCE at the onset of their safe problems to preclude a possible lockout.

5.26.3.4. (Added) Secondary distribution lists will be attached to the documents reproduced or an annotation will be made on the file copy of the document to be reproduced showing the number of copies reproduced and the distribution of each copy. Distribution information will include the name and organization of receipt, date, and copy number, which will be affixed to the first page of the reproduced document.

5.28.3. Establish an annual clean-out day and include in your unit operating instruction.

5.29.1.2. (Added) Shredders approved for the destruction of classified material are those approved through GSA. All other shredders, i.e. purchased on the local economy can be used if they meet the GSA standards set forth in DoD 5220.22-M, *National Industrial Security Program Operating Manual* (NIS-POM) and approved by the unit security manager in writing.

5.29.1.2.1. (Added) IAW HQ USAF/SXFI, Memo dated 29 Jan 03, New Shredder Policy Update, units and organizations may continue using existing cross cut shredders approved for destruction of collateral classified information "ONLY IF" the shredded material is further destroyed by burning, dispersing the waste (e.g., emptying the contents of the shredder bag into a dumpster or similar large sized waste container versus placing the sealed bag in a dumpster), wet pulping the shredded material, or converting it to paper mache by mixing the shredded material with water and a small quantity of liquid soap. If the purchase of a new shredder for the destruction of collateral classified information is required, the new shredder may only be purchased from the GSA evaluated products list, previously provided by USAFE/SFXI to all USAFE SFAs via e-mail on 19 Dec 02.

5.29.1.3. (Added) Post visual aids at shredders approved and not approved for destruction of classified.

5.29.2.6. (Added) The 39 ABW/CC or a designated representative will make the final determination when emergency destruction is to begin. The order will be received and disseminated by the Command Post Emergency Action Controllers.

5.29.2.7. (Added) The 39 ABW/CC will determine if classified information will be destroyed or packaged for evacuation as transportation becomes available. Upon notification by appropriate authorities of evacuation, you will also be notified of what material will be collected and compiled. You will be notified when to destroy all other classified material at a later time by appropriate authorities (i.e. Command Post) as directed.

5.29.2.8. (Added) Base communications centers will destroy residue by-products as they would classified waste.

5.29.2.9. (Added) If while in transit an emergency occurs, and it appears the material cannot be adequately protected, it may be burned or destroyed by other means to render recognition impossible. The 39 ABW/CC and 39 SFS/SFA will be immediately notified and a complete report of the circumstances surrounding the destruction will be accomplished.

5.30.1.1.1. (Added) An Operating Instruction (OI) will be developed prior to the use of alternate or compensatory security controls and be approved by the 39 ABW/CC through 39 SFS/SFA. The use of alternate or compensatory security controls will not be considered prior to the development of the OI.

6.3.2. Incorporate into the internal operating instruction to ensure only properly cleared individuals sign for incoming registered mail. An AF Form 12, **Accountable Container Receipt**, or AF Form 310, **Document Receipt and Destruction Certificate**, must be completed anytime the material is transferred to a recipient not shown on the material's distribution. In addition, when using registered mail, personnel must verbally indicate whether the mail piece contains classified material to allow the Base Information Transfer Center (BITC) to verify delivery. (Reference, AFI 24-201, 7.8.1.)

8.3.3.1.1. (Added) Security Managers assigned as Temporary Duty (TDY) for approximately 180 days or more, are required to be formally trained by the ISPM. Security Managers are responsible to and will report all Security Manager related issues to the ISPM.

8.3.3.1.2. (Added) Security Managers are highly encouraged to complete the Information Security interactive courseware, L6AGU3P071-000. This is highly recommended since they are selected by their commander/staff agency chief to administer the activity information security program and to provide advice and assistance to the unit commander, staff agency chief and assigned personnel.

8.5.1. Supervisors and security managers provide training to uncleared personnel. Supervisors are responsible for ensuring that all uncleared personnel receive an initial security education orientation within 30 days of assignment to the unit.

9.8.6. (Added) All Security Incidents Inquiries, Investigations will be conducted IAW USAFE Pamphlet 31-402, *Conducting Security Incident/Inquiries and Investigations*.

9.11.2.1. Appointing official will close the investigation; however, the ISPM has the authority to elevate the decision should he/she disagree with the appointing official.

9.11.4. Inquiry, Investigative officials must complete inquiry/investigations within 30 duty days from appointment.

9.11.5. (Added) Retain a copy of the investigation. Maintain and dispose of records according to AFMAN 37-139, *Records Disposition Schedule*.

9.13. (Added) Forms Adopted. AF Form 12, **Accountable Container Receipt**, AF Form 310, **Document Receipt and Destruction Certificate**, AF Form 2519, **All Purpose Checklist**, AF Form 332, **Base Civil Engineer Work Request**, AF Form 614, **Charge Out Record**, SF Form 700, **Security Container Information**, and AFTO Form 36, **Maintenance Record for Security Type Equipment**

Attachment 1

GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

References

AFI 31-401, *Information Security Program Management*

AFI 33-202, *Network and Computer Security*

AFMAN 37-139, *Records Disposition Schedule*

DoD 5220.22-M, *National Industrial Security Program Operating Manual*

T.O. 00-20F-2, *Inspection and Preventive Maintenance Procedures for Classified Storage Containers*

Abbreviations and Acronyms

ABW—Air Base Wing

AFMAN—Air Force Manual

BITC—Base Information Transfer Center

CSF—Chief of Security Forces Squadron

GSU—Geographically Separated Unit

IAW—In Accordance With

ISPM—Installation Security Program Manager

OI—Operating Instruction

TDY—Temporary Duty

TSCO—Top Secret Control Officer

Attachment 17 (Added)

39 SFS/SFA PROGRAM GUIDANCE

A17.1. Applicability. This attachment outlines general procedures and requirements to govern the Information Security Program for the 39 ABW and all attached organizations, units, and agencies within Turkey. More specific procedures are contained in the Incirlik AB Supplement.

A17.2. Installation Security Program Manager (ISPM) Channels. The statement “through ISPM channels” is defined as from the 39 ABW and all attached organizations, units, and agencies within Turkey to the 39 SFS/SFA.

A17.3. ISPM. The 39 ABW/CC, has the overall responsibility for implementing and ensuring compliance with this supplement. The CSF is designated as the ISPM. 39 SFS/SFA serves as the OPR to manage the program on behalf of the ISPM.

A17.4. Security Manager Meetings. 39 SFS/SFA will conduct, as a minimum, semi-annual security manager meetings.

A17.5. Security Manager Appointment Letters. Forward a copy of the primary and alternate security manager appointment letters to 39 SFS/SFA.

A17.6. Unit Security Operating Instruction.

A17.6.1. Each organization as specified in **A17.1.** will develop a unit specific operating instruction.

A17.6.2. Forward a copy of the unit security operating instruction to 39 SFS/SFA.

A17.6.3. Security managers will conduct an annual review of the unit’s operating instruction in June of each year. Document results of the review in a memorandum, forward to the commander for approval, send a copy to 39 SFS/SFA, and maintain a copy of the memorandum in the security manager’s handbook.

A17.7. Security Manager Meeting Minutes. Maintain the minutes of the last two security manager meetings in the security manager’s handbook.

A17.8. Semiannual Security Self-Inspections. Semiannual security self-inspections will be conducted in the second quarter of each calendar year (April through June). Utilize the 39 SFS/SFA provided checklists (AF Form 2519, **All Purpose Checklist**) to conduct the semiannual security self-inspections. Maintain the last semiannual security self-inspection inspection report and completed checklists in the security manager’s handbook. Forward a copy of the semiannual security self-inspection report to 39 SFS/SFA.

A17.9. Security Managers Handbook. Maintain a security manager’s handbook with the following:

A17.9.1. Primary and alternate security manager memorandum of appointment.

A17.9.2. Primary and alternate security manager training certificates or other documented proof of training completion.

A17.9.3. Applicable operating instructions and annual review memorandum.

A17.9.4. List of unit security containers, vault and secure rooms.

A17.9.5. Vault and secure room survey reports and approval memorandums.

A17.9.6. List of unit shredders approved for the destruction of classified material.

A17.9.7. Unit protection, removal, or destruction of classified material plan (if not included in the unit's operating instruction).

A17.9.8. Unit classified material reproduction authority appointment letters.

A17.9.9. Last semiannual security self-inspection report and completed checklist.

A17.9.10. Last Information Security program review report, to include written replies to findings (as required).

A17.9.11. Minutes of the last two-security manager's meetings.

A17.9.12. Current unit JCAVS roster.

A17.10. Program Reviews. 39 SFS/SFA will conduct annual program reviews on all programs identified in **A17.1**. Program review reports will identify discrepancies as either an observation or a finding. Observations and most findings do not require a reply; however, repeat findings and those deemed critical and have a significant impact on the program require a written reply and/or update every 30 days to 39 SFS/SFA. Written replies will include action taken to correct the finding and status of the finding (if open, provide estimated completion date; if closed, provide the date the finding was corrected).

A17.11. Top Secret Control Account (TSCA). Units with a TSCA will forward appointment letters identifying the Top Secret Control Officer (TSCO) and at least one alternate to 39 SFS/SFA.

A17.11.1. **Top Secret Control Officer (TSCO) Training.** TSCO's and alternates must be trained within 30 days of appointment. 39SFS/SFA is responsible for conducting this training.

A17.12. Secure Conference Facilities. Forward written requests for Secure Conference Facilities to 39 SFS/SFA.

A17.13. Security Container, Vault, and Secure Room List. Forward a copy of the security container, vault, and secure room list to 39 SFS/SFA.

A17.14. Vault or Secure Room Surveys and Intrusion Detection System.

A17.14.1. **Vault or Secure Room Surveys.** Utilize AF Form 332, **Base Civil Engineer Work Request**, for vault or secure room surveys. The request must be coordinated through the unit security manager, signed by the commander or designated representative, coordinated first through 39 SFS/SFA, and then submitted to the 39 CES. Once the survey is scheduled, it is the requesting organization's responsibility to notify 39 SFS/SFA since the survey must be conducted jointly between 39 SFS/SFA and the 39 CES. If subsequent work requests are required for structural improvements or modifications to the vault or room, complete and submit another AF Form 332 following the procedures outlined above. Vaults or rooms that are structurally modified or altered after initial certification require re-certification to ensure they still comply with DoD 5200.1-R, Appendix G.

A17.14.2. **Intrusion Detection Systems.** Installation of Intrusion Detection System (IDS) requires a separate AF Form 332. The request must be coordinated through the unit security manager, signed by the commander or designated representative, coordinated first through 39 SFS/SFA and then submitted to the 39 Civil Engineer Squadron. The requesting organization must also submit an AF Form 3215, **Communication Work Request**, to the 39 Communications Squadron for the installation of or to secure one free and serviceable twisted cable pair to connect the alarm to the appropriate control panel.

A17.14.3. **Survey Reports and Approval Memorandums.** The unit security manager will maintain a copy of the vault and secure room survey report and approval memorandums in the unit security manager's handbook, and forward a copy of the approval memorandum to 39 SFS/SFA.

A17.15. Approved Classified Material Shredders. Security managers will develop a memorandum that lists shredders approved for the destruction of classified material located in their organization. This memorandum will include make, ID number, and location.

A17.16. Security Manager Training. 39 SFS/SFA is responsible for conducting security manager training for all units identified in [A17.1](#). Forward training requests to 39 SFS/SFA.

A17.17. Security Incidents:

A17.17.1. All Security Incidents Inquiries/Investigations will be conducted IAW USAFE Pamphlet 31-402, *Conducting Security Incident/Inquiries and Investigations*.

A17.18. Completed Security Incident Report Coordination. Forward completed reports to 39 SFS/SFA through the unit security manager. 39 SFS/SFA will review the report and forward it to 39 SFS/SFA for coordination via an AF FM 1768, **Staff Summary Sheet**. Upon completion of the coordination process, 39 SFS/SFA will complete a memorandum recommending concurrence or non-concurrence and forward the report to the 39 SFS/CC for approval. Once the CSF approves the report, 39 SFS/SFA will forward a hard copy of the approval memorandum and the report to the unit commander or equivalent through the unit security manager.

A17.19. Security Incident Report Disposition. Security managers and 39 SFS/SFA will maintain a copy in accordance with AFMAN 37-139, *Records Disposition Schedule*.

MICHAEL C. GARDINER, Colonel, USAF
Commander