

**21 MARCH 2001**

**Information Security**

**UNIT SECURITY MANAGER**



**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: 940 SFS/SFO (MSgt Donald W. Souron)

Certified by: 940 ARW/CCE  
(Lt Col Randy Lavender)

Supersedes 940 ARWI 31-401, 31 January 1997

Pages: 5  
Distribution: F

---

This instruction implements guidance in AFD 31-4, *Information Security*, DOD 5200.1-R, *Information Security Program* and AFI 31-401AFRCS1, *Information Security Program Management*. Its purpose is to establish guidelines and procedures for the administration of 940 ARW Information Security Program, Access, Accountability, Dissemination, Protection of Classified material information and security education. It is applicable to all 940 ARW Security Managers .

**SUMMARY OF REVISIONS**

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

This revision incorporates the current requirements, information and procedures, including IC 2001 and 2002 to AFI 31-401. It includes the provision of host base oversight and guidance.

**1. Duties and Responsibilities :**

1.1. The Wing Commander:

1.1.1. Ensures proper program management.

1.1.2. Appoints a primary and alternate Wing Security Manager.

1.2. The Host base provides oversight and guidance for Wing Information, Personnel, NATO, Physical Security and Anti-Terrorism Programs.

1.3. The Wing Security Manager:

1.3.1. Acts as the liaison between the Host base and the 940 ARW.

1.3.2. Distributes minutes of the Host base Security Managers Meeting.

- 1.3.3. Ensures requests for personnel security investigations are completed and turned in on a timely basis (30 days) and proper utilization of EPSQ.
- 1.3.4. Develop master safe listing for wing classified safes.
- 1.3.5. Reviews the monthly Automated Security Clearance Approval System (ASCAS) roster and initiates appropriate actions on personnel without valid investigations or security clearances eligibility .
- 1.3.6. Ensures known security violations are reported to the proper agencies.
- 1.3.7. Provide assistance establishing Security Information Files (SIF).
- 1.4. Unit commander is responsible for implementing the Information Security-Training program, developing supplemental training tools, and assessing the health of their programs on a continuous basis. In addition, commanders will:
  - 1.4.1. Ensure primary and alternate unit Security Managers are appointed and the Wing Security Manager is notified of the appointment letter.
  - 1.4.2. Ensure Unit Security Managers have completed training within 90 days of appointment.
  - 1.4.3. Ensure that each Security Manager maintains a Security Manager Handbook for guidance. (See [Attachment 1](#) for Table of Contents)
  - 1.4.4. Review Security Self-Inspection, Program Reviews, and Staff Assistance Visits and ensure proper measures are taken to correct deficiencies.
  - 1.4.5. Provide the security manager with sufficient resources of time, staff and funds to permit the accomplishment of their duties .
  - 1.4.6. Review Security Access Requirements (SAR) Codes annually to ensure they meet mission requirements .
  - 1.4.7. Ensure computer and tempest security officers are assigned to the unit.
  - 1.4.8. Actively support and monitor security education training.
  - 1.4.9. Ensure records are maintained on a calendar year basis of personnel attending initial, refresher and specialized information security training. As a minimum, these records must reflect the date(s) training was conducted and the number of personnel in attendance.
- 1.5. Unit Security Managers will:
  - 1.5.1. Provide the Wing Security Manager with an appointment letter of the primary and alternate Security Managers .
  - 1.5.2. Establish a unit Operating Instruction (OI) for internal operating procedures.
  - 1.5.3. Maintain all applicable directives, instructions, forms, and visual aids.
  - 1.5.4. Ensure Security Self-Inspections are conducted on a semi-annual basis.
  - 1.5.5. Attend Host Base Security Manager's meeting.
  - 1.5.6. Review the unit ASCAS Roster for errors and initiate appropriate actions on personnel without valid investigations or security clearance eligibility.
  - 1.5.7. Maintain a Security Education and Training Program as directed in AFI 31-401.

1.5.7.1. Ensure all personnel receive initial training, refresher training and termination briefings.

1.5.8. Initiate AF Form 2587, **Security Termination Statement**, on any member retiring, separating or who has not performed any military duty for 60 days or more.

1.5.8.1. For individual's who are reassigned for non-participation, an AF Form 2587 will be accomplished and sent to the individual with a self addressed stamped envelope via certified mail, return receipt request. Ensure there is a letter stating the reasons for completing the form.

1.5.8.2. If there is no response within 90 days, another AF Form 2587 will be initiated and included in unit files. File all copies of AF Form 2587 to include certified mail receipts in unit files.

1.5.9. Initiate AF Form 2586, **Unescorted Entry Authorization Certification** on personnel receiving a valid security clearance that require frequent unescorted entry into restricted areas.

1.5.9.1. Ensure personnel receive physical awareness training IAW AFH 31-104, formerly AFI 31-103.

1.5.9.2. Conduct an annual 100% inventory of all restricted area badges and provide the host base with all discrepancies.

1.5.10. Initiates SF 312, **Classified Information Nondisclosure Agreement** for all new personnel and place into person's official record.

1.5.11. Review challenges to classification of improperly marked documents.

1.5.12. Ensure Foreign Travel Briefings are conducted by authorized personnel.

1.5.13. Recommend to the commander to establish a SIF on personnel in the unit.

1.5.14. Ensure AFVA 31-4, formerly AFVA 205-11, is posted in conspicuous area.

## 2. Access Briefings.

2.1. Supervisors, security managers or designated officials conduct and document the following access briefings, as appropriate:

2.1.1. Brief and execute the SF 312, **Classified Information Nondisclosure Agreement**, prior to granting an individual access to classified information. The SF 312 may also be used to document attestations .

2.1.2. Brief and execute the DD Form 2501, **Courier Authorization**, when an individual is authorized to escort or hand carry classified information.

2.1.3. Brief and execute the AF Form 2583, **Request for Personnel Security Action**, prior to granting an individual access to NATO classified information.

2.1.4. Brief and execute the AF Form 2583, **Request for Personnel Security Action**, prior to granting an individual access to SIOP-ESI.

## 3. Termination Debriefings .

- 3.1. Debrief individuals having access to classified information or security clearance eligibility when they terminate civilian employment, separate from the military service, have their access suspended, terminated, or have their clearance revoked or denied .
- 3.2. Use AF Form 2587, **Security Termination Statement**, to document debriefing.
- 3.3. Maintain the AF Form 2587's for two years. Dispose of AF Form 2587 according to AFMAN 37-139.
- 3.4. Refusal to sign a termination statement.
  - 3.4.1. When an individual willfully refuses to execute AF Form 2587, the supervisor, in the presence of a witness will:
    - 3.4.1.1. Debrief the individual orally.
    - 3.4.1.2. Record the fact that the individual refused to execute the termination statement and was orally debriefed.
    - 3.4.1.3. Ensure the individual no longer has access to classified information.
    - 3.4.1.4. Forward the AF Form 2587 to the servicing Information Security Program Manager for Security Information File (SIF) processing according to AFI 31-501.

VIK C. MALLING, Colonel, USAFR  
Commander

**Attachment 1****SECURITY MANAGER CONTINUITY BOOK**

## TABLE OF CONTENTS

1. Appointment Letters. (Keep the most current letters)
  - Primary and Alternate Security Manager/Monitors.
  - Primary and Alternate Top Secret Control Officer's (TSCO). (If applicable)
  - Primary and Alternate Safe Custodians and Safe Listing.
  - Personnel authorized to Reproduce Classified.
  - Personnel authorized to Pick-up/Receipt for Classified.
2. 940 ARW Instruction 31-401 and Unit/Directive Operating Instructions. (Keep until superseded or rescinded.)
3. Semiannual Self-Inspection Program. (Keep a copy of last two inspections.)
  - Self-Inspection Appointment Letters.
  - SI Checklist.
  - SI Reports and Replies.
4. Information Security Program Oversight Visit (ISPOV) Reports. (Keep the most current ISPOV.)
5. Information and Personnel Security Program Miscellaneous Information. (Keep for one year.)
  - Security Manager Minutes.
  - HQ AFRC/SFI Letters/Instructions/email, etc.
6. Unit /Directorate Automated Security Clearance Approval System (ASCAS) Roster (military). (Keep the most current ASCAS ordered every 30 – 45 days.)
  - Security Clearance Eligibility Verification Letters.
  - Correspondence Relating to the ASCAS Roster. (AF Forms 2583, 2587, 9 SFS Supervisory Sheet, etc.)
7. Unit/Directorate Restricted Area Badge Listing. (Keep the most current listing.)
  - AF Form 2586, **Unescorted Entry Authorization Certification.**
8. Miscellaneous Security Information. (Keep for one year.)