

**BY ORDER OF THE COMMANDER  
934TH AIRLIFT WING**

**934TH AIRLIFT WING INSTRUCTION 31-401**

**19 NOVEMBER 2009**

Certified Current 9 May 2012  
*Security*



**MANAGING THE INFORMATION  
SECURITY PROGRAM**

**COMPLIANCE WITH THIS PUBLICATION IS MANDATORY**

---

**ACCESSIBILITY:** Publications and forms are available on the e-Publishing website at [www.e-Publishing.af.mil](http://www.e-Publishing.af.mil) for downloading or ordering.

**RELEASABILITY:** There are no releasability restrictions on this publication.

---

OPR: 934 AW/IP

Supersedes: AFI31-401\_934AWSUP1,  
29 March 2000

Certified by: 934 AW/CCE  
(Capt Julie Hamiel)

Pages: 14

---

This instruction implements Air Force Instruction 31-401, *Information Security Program Management*, the requirements of DoD 5200.1-R, *Information Security Program*, and outlines the 934 AW Information Security Program. It prescribes procedures and responsibilities of all personnel working on Minneapolis ARS, MN; specifically Commanders; Security Managers (SM); and Classified Account Custodians. 934 AW/IP provides oversight and assistance to all 934 AW units. Each Unit Commander is responsible for ensuring assigned personnel comply with DoD 5200.1-R, AFPD 31-4, AFI 31-401, and this instruction. For the purpose of brevity, the terms Unit and Squadron are interchangeable. Ensure that all records created as a result of processes prescribed in this publication are maintained in accordance with Air Force Manual (AFMAN) 33-363, *Management of Records*, and disposed of in accordance with Air Force Records Information Management System (AFRIMS) Records Disposition Schedule (RDS) located at <https://www.my.af.mil/gcss-af61a/afrims/afrims/>. Refer recommended changes and questions about this publication to the Office of Primary Responsibility (OPR) using the AF Form 847, *Recommendation for Change of Publication*; route AF Form 847s from the field through the appropriate functional's chain of command.

## **1. Program Management.**

### **1.1. Commander Responsibilities:**

1.1.1. Commanders are responsible for implementation of the Information Security Program within their respective area of responsibility. The SM manages the Information Security Program for the Unit.

1.1.2. As the responsible officer in charge of the Information Security Program the Commander appoints a primary and alternate SM to manage the Information, Personnel,

and Industrial Security Programs for the Unit. Larger Units are encouraged to appoint security monitors (in addition to the Alternate) to assist the SM. The primary SM must be a full-time employee/member of the unit. Continuity should receive serious consideration in the selection of security managers. Provide the appointment letter and any updates to 934 AW/IP.

1.1.3. Ensure SM receives training within 90 days of appointment. This training will be conducted by 934 AW/IP.

## 1.2. Security Manager Responsibilities:

1.2.1. Maintain a security manager's handbook. (Attachment 2)

1.2.2. Mandatory attendance is required by primary or alternate security manager at the biannual hosted security manager meetings.

1.2.3. HQ AFRC/SFI conducts Information Security Program Oversight Visits (ISPOVs) at AFRC installations every two years or in conjunction with Staff Assistance Visits (SAVs). 934 AW/IPs assist in the ISPOV.

1.2.3.1. ISPOVs are assistance-orientated visits to identify noteworthy and problem areas in the Information, Personnel, Industrial, and NATO Security Programs. They must be extensive enough to determine overall status of the program and must include an assessment of the security education and training as a special interest item. Replies to ISPOV reports are generally not required; however, corrective action(s) taken to correct identified problem areas should be recorded.

1.2.4. All units will conduct semiannual security self-inspections, one between 1 January and 30 June, and one between 1 July and 31 December. Self-inspections should be completed by a person knowledgeable of the Information Security Program (other than the SM). SMs should monitor the inspection, review the observations (if any) and follow up to ensure they are corrected.

1.2.5. Print Joint Personnel Adjudication System (JPAS) rosters at least monthly.

1.2.6. Security Container Listing.

1.2.6.1. Develop a master security container listing and provide a copy to 934 AW/IP. This list should contain the following: manufacturer of the container, unique ID number, lock type (X-07, 08 or 09), physical location of the container, custodian information and date of last initial inspection or Preventive Maintenance Inspection conducted by the 934 CES Locksmith. If there is a secure room in the unit, enter the location, type of lock and custodian information.

1.2.7. Ensure a visual aid identifying the SM and alternate is posted conspicuously throughout the Unit to ensure assigned personnel are aware of SM appointments.

## 2. Marking.

2.1. Holders must notify originator of improperly marked documents in writing, or record with a memo any telephonic notification. Notification must be kept with the document.

2.1.1. All binders that contain classified information will be marked on the spine with the highest level of classified stored therein. Exceptions would be binders that are too small to have an adequate spine.

### 3. Safeguarding.

#### 3.1. Access

3.1.1. Joint Personnel Adjudication System (JPAS) will be utilized to verify an individual's access level. 3.1.2. In absence of verification of a signed SF 312, *Nondisclosure Agreement (NDA)*, complete new form and forward to 934 AW/IP.

3.1.2. 934 AW/IP may forward visit requests in the absence of security managers.

3.1.3. Implement a documented accountability system (such as an inventory sheet) for Secret material retained over 30 days and stored in a General Services Administration (GSA) approved security container not located in a secure environment. The 934 AW/IP determines what constitutes a secure environment. Use an unclassified description of the material and file separately from the classified material. This will facilitate an assessment of a compromise.

3.1.4. Use AF Form 614, *Charge Out Record*, or similar form, when a document is removed from a security container.

3.1.5. Develop plans for the protection, removal, or destruction of classified material in case of natural disaster, fire, civil disturbance, terrorist activities, or enemy action. (DoD 5200.1-R, para 6-303). Include in your unit operating instruction (see sample at Attachment 3).

3.1.6. Each unit and staff agency which stores and processes classified information, do not have to use SF 701, *Activity Security Checklist*, or SF 702, *Security Container Check Sheet*, on security containers, vaults, or secure storage rooms where classified material is stored or handled when manned by cleared personnel on a 24-hour, 7-day-a-week basis. At no time under these conditions may the above be left unattended when opened.

3.1.7. Include on your SF 701 (if applicable): Check all classified computers to ensure that the hard drive has been removed and locked in a GSA approved container. Check all Global Command and Control System (GCCS)/SIPRNET connections to ensure they have been disconnected and properly locked away. 3.1.8. Within AFRC, removing classified information/material from designated work areas for work at home is prohibited.

3.1.8. AFRC installations must include designated overnight repository in their base supplement.

3.1.9. The Security Forces Control Center (SFCC) and Command Post have been designated as the overnight repositories for the 934 AW.

3.1.10. Classified Meetings and Conferences.

3.1.10.1. Installation commanders can delegate this authority in writing to the 934 AW/IP. The following procedures must be accomplished when hosting classified meetings:

- 3.1.10.2. Verify security clearances on attendees prior to any classified briefings or discussions.
- 3.1.10.3. Ensure the door to the discussion area is closed and someone is posted outside the door if sound attenuation and unauthorized entry is not adequate and cannot be controlled.
- 3.1.10.4. Ensure the briefing is kept to need-to-know for those in attendance.
- 3.1.10.5. Ensure classified is kept under constant surveillance. Use of classified cover sheets is required when material is removed from secure storage.
- 3.1.10.6. Return all classified material to secure storage when not under personal observation and control.
- 3.1.10.7. Note taking or electronic recording during classified sessions shall be permitted only when it is determined by the host that such action is necessary to fulfill the U.S. Government purpose for the meeting.
- 3.1.10.8. Classified waste must be destroyed using approved methods (burning, melting, pulping, pulverizing, and cross-cut shredding).
- 3.1.10.9. Ensure that classified documents, recordings, audiovisual material, notes, and other materials created, distributed, or used during the meeting are controlled, safeguarded, and transported as required by this instruction and DoD 5200.1-R, *Information Security Program*.
- 3.1.11. 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 where classified and sensitive information may be discussed. Staff directors, NAF commanders, and wing commanders will determine which work areas are affected and implement this requirement accordingly. 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.
- 3.1.12. 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. AFRCVA 31-404, *Classified Reproduction Rules*, and AFRCVA 31-405, *STOP Do not use this machine for classified Reproduction STOP*, should be used. These visual aids may be obtained from the AFRC Publications web site.

#### **4. Storage of Classified Materials [Reference DoD 5200. 1-R, Paragraph 6-402]**

- 4.1. Security managers will develop and maintain a list of security containers, vaults, and secure rooms located in their organization and include in their security manager's handbook. This list will include make, ID number, lock type, and location.
  - 4.1.1. Secure storage rooms containing open stored classified material, equipment or hardware built after 1 October 1995 must have an intrusion detection alarm operating when appropriately cleared attendants are not present. 934 AW/IPs determine whether open or unattended storage areas provide adequate protection for classified material. If "security-in-depth" practices are used in lieu of alarms, the MAJCOM 934 AW/IP must

grant approval. Examples of “security-in-depth” are: use of perimeter fences, employee and visitor access controls, use of an IDS, random guard patrols throughout the facility during non-working hours, closed circuit video monitoring or other safeguards that mitigate the vulnerability of unalarmed storage areas and security storage cabinets during non-working hours.

4.1.2. 934 AW/IP must send requests to waive any provisions of DoD 5200.1-R and AFI 31-401 to HQ AFRC/SF for concurrence. Post the storage facility approval notices/letters inside the approved area.

4.1.3. FF-L2740 is the specification requirements for the X-07 lock and FF-L2740A.

Below are the national stock numbers:

5340-01-357-6446 = X-07 Container Lock

5340-01-393-7058 = X-07 Door Lock

5340-01-381-6402 = CD X-07 Door Lock with drill resistant plate

5340-01-49-5776 = X-08 Container Lock

5340-01-469-5897 = CD-X08 Combination Deadbolt lock for pedestrian doors with drill resistant plate

5340-01-469-5906 = CD-X08 Combination Deadbolt lock for pedestrian doors with a non-drill resistance plate

4.1.4. Prior to storing classified information in a vault or secure room, the servicing civil engineer (CE) and the 934 AW/IP will survey the facility to determine if it meets the construction requirements outlined in DoD 5200.1-R, Appendix 7 and all other requirements of DoD 5200.1-R and AFI 31-401 for the storage of classified information. If the survey certifies that the facility meets requirements, the installation commander may approve the facility for storage of classified information. If the facility does not meet requirements, consider alternate or compensatory security controls in accordance with DoD 5200.1-R, Section C6.8. Re-evaluate all secure storage rooms every 5 years and accomplish new approval letter and/or waiver requests.

4.1.5. Use of Key Operated Locks.

4.1.5.1. Approve an area using key-operated locks to store bulky secret and confidential material according to paragraph 5.19.1, AFI 31-401.

4.1.5.2. As a minimum, lock and key custodians must be cleared to the level of the information stored in the area.

4.1.5.3. Control and store all keys at the level of security required for the information contained in the area.

4.1.6. Equipment Designations and Combinations.

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

- 4.1.6.2. Security Container combinations shall be changed every 2 years in the absence of one of the conditions specified in DoD 5200.1-R, para 6-404b.
- 4.1.7. Retention of Classified Records. Annual cleanout day is the first Thursday in August.
- 4.1.8. Methods and Standards.
- 4.1.8.1. For a listing of National Security Agency (NSA) evaluated and approved destruction devices see Annex B to NTISSI No.4004.
- 4.1.8.2. Post visual aids at shredders approved and not approved for destruction of classified. Note: Cross cut for shredders approved for destruction of classified must be a minimum of 1/32 x 1/2. AFRCVA 31-402, *AUTHORIZED FOR DESTRUCTION OF CLASSIFIED INFORMATION*, and AFRCVA 31-403, *NOT AUTHORIZED FOR DESTRUCTION OF CLASSIFIED INFORMATION*, should be used and may be obtained from the AFRC Publications web site.
- 4.1.9. Records of Destruction. Safes required to have accountability control must ensure classified destroyed is annotated on accountability records.

## **5. Transmitting Classified Information.**

### 5.1. Transmitting Secret Information.

5.1.1. Incorporate into the internal operating instruction to ensure only properly cleared individuals sign for incoming FedEx (or whoever holds current GSA contract), registered mail, first class mail with caveat "Return Service Requested", and Postal Service Express mail shipments. 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 FedEx, registered mail, first class mail with caveat "Postmaster Do Not Forward," and Postal Service Express mail to send outgoing 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)

### 5.1.2. Escort or Hand carrying of Classified Information.

5.1.2.1. See sample Courier Letter at Attachment 4 and exemption notice at Attachment 5.

5.1.2.2. Use DD Form 2501, *Courier Authorization*, whenever a person hand-carries classified information through an installation entry/exit point (expiration date is one year). The DD Form 2501 must be in their possession. The 934 AW/IP issues and maintains the DD Form 2501's. 934 AW/IP may delegate to SMs.

## **6. Training.**

6.1. As a minimum, training documentation must include the trainee's name and grade, type of training (initial, refresher, or specialized), date of training, and a specific list of completed training subjects and tasks.

6.1.1. 934 AW/IP ensure primary and alternate security managers are trained within 3 months of appointment. Security Managers receive documentation of training. Security

Managers are responsible for providing information security program training to their units.

#### 6.1.2. Cleared Personnel

6.1.2.1. Cleared personnel are those personnel who have access to classified information are assigned to sensitive duties or are assigned to a critical sensitive position.

#### 6.1.3. Uncleared Personnel

6.1.3.1. Uncleared personnel are those personnel who do not have access to classified information, and are not assigned to sensitive duties.

#### 6.1.4. Other Program Related Training Requirements.

6.1.4.1. At all AFRC installations Security Forces, Intelligence, and the command post have the means of contacting their OSI agent and scheduling counterintelligence awareness briefings.

6.1.4.2. At all AFRC installations, prior to units being deployed, the Antiterrorism/Force Protection (AT/FP) representative coordinates with the appointed OSI agent. The AT/FP representative or Level II trained representative will administer the Level I Antiterrorism Awareness Training. OSI will supplement the Level I training by presenting a country specific briefing. The country specific briefing is classified Secret and will cover the current terrorism and criminal threat which exist at the deployed location. Level I training must be current within a six-month period prior to deployment.

6.1.5. Continuing and Refresher Training. SMs ensure this training is accomplished.

6.1.6. Refusal to Sign a Termination Statement. If the person is terminating employment or separating from military service, the Authorized Requester will notify the Air Force Central Adjudication Facility (AFCAF) so that the refusal may be recorded in the DCII.

## 7. Security Incidents

7.1. Appointment of inquiry official must be within 3 days after the incident was reported. The inquiry official will not be assigned to the same division/branch where the suspected incident took place. Provide the 934 AW/IP with a copy of the appointment letter.

7.1.1. Upon appointment, the inquiry official reports to the 934 AW/IP for a briefing.

7.1.2. The inquiry will also determine if the "subject(s) of the investigation" has completed all initial and recurring training requirements. Verification must include the date of initial training and all dates of recurring training.

7.1.3. Appointing official will close the investigation and send the finished investigation to the 934 AW/JAG for review who in turn will send it to 934 AW/IP.

7.1.3.1. The 934 AW/IP has the authority to elevate the decision should he/she disagree with the appointing official.

7.1.4. Retain a copy of the investigation. Maintain and dispose of records according to AFRIMS Records Disposition Schedule.

**8. Adopted Forms.**

SF 312, *Nondisclosure Agreement (NDA)*

AF 614, *Charge Out Record*

SF 700, *Security Container Information*

SF 701, *Activity Security Checklist*

SF 702, *Security Container Check Sheet*

AF Form 310, *Document Receipt and Destruction Certificate*

AF Form 12, *Accountable Container Receipt*

DD Form 2501, *Courier Authorization*

AF Form 847, *Recommendation for Change of Publication*

TIMOTHY E. TARCHICK, Colonel, USAFR  
Commander

**Attachment 1****GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION*****References***

DoD 5200.1-R, *Information Security Program*, 17 Jan 97

AFPD 31-4, Information Security

AFPD 31-5, Personnel Security

AFPD 31-6, Industrial Security

AFI 31-101, Air Force Installation Security Program

AFI 31-401, Information Security Program Management

AFI 31-501, Personnel Security Program Management

AFI 31-601, Industrial Security Program Management

***Abbreviations and Acronyms***

**AFCAF**— Air Force Central Adjudication Facility

**AT**— Antiterrorism/Force Protection

**BITC**— Base Information Transfer Center

**FP**—Force Protection

**GCCS**— Global Command and Control System

**GSA**—General Services Administration

**ISPOV**— Information Security Program Oversight Visits

**JPAS**— Joint Personnel Adjudication System

**NATO**— North Atlantic Treaty Organization

**NDA**— Nondisclosure Agreements

**NSA**— National Security Agency

**OI**—Operating Instruction

**SAV**—Staff Assistance Visit

**SFCC**—Security Forces Control Center

**SM**—Security Manager

**Attachment 2****SECURITY MANAGER HANDBOOK**

**A2.1. SECURITY MANAGER HANDBOOK:** The Security Manager maintains a Security Manager's Handbook that is used a reference guide, it will contain information listed in the below table of contents. (NOTE: Privacy Act (Subject to Privacy Act of 1974); For Official Use Only (FOUO); and Sensitive Information (Computer Security Act of 1987) Information will not be placed in the handbook. This includes AF Form 2583 and AF Form 2586. Unit/Unit Joint Clearance and Access Verification System (JCAVS) Report or Person Summary (military or civilian) (SMs should acquire a new summary or roster every 30-45 days); Security Clearance Visit Letters; and Correspondence Relating to JCAVS. This information will be maintained in an office environment and secured, when not being used.

**A2.1.1. TABLE OF CONTENTS** (Suggested)**A2.1.1.1. Appointment Letters** (Keep the most current letters)

A2.1.1.1.1. Primary &amp; Alternate Security Managers

A2.1.1.1.2. Primary &amp; Alternate TSCOs (If Applicable)

A2.1.1.1.3. Primary &amp; Alternate Safe Custodian

A2.1.1.1.4. Personnel Authorized to Reproduce Classified

A2.1.1.1.5. Personnel Authorized to Pickup/Receipt for Classified, AF Form 4332

**A2.2.1.1. 934 AW Operating Instruction (OI) 31-401 and Unit/Unit OIs** (Keep until superseded or rescinded)**A2.3.1.1. Semiannual Self-Inspection (SI) Program** (keep a copy of last two inspections)**A2.4.1.1. Information Security Program Review Visit (ISPR) Reports** (Keep the most current ISPR)**A2.5.1.1. Security Manager Meeting Minutes** (Keep for one year)**A2.6.1.1. Security Inspection Checklists****A2.7.1.1. Current CY Annual Training Plan** (Reviewed and Signed by the Commander or Commander) **& Tracking****A2.8.1.1. List of Security Containers, Vaults, and Secure Rooms located in the organization** (List will include Make of Container; Unique Unit Container Number (A7S #1); Lock Type; Location; Container Custodian to include Telephone Number; and Date of Last Inspection or Preventive Maintenance Inspection conducted by 78 Locksmith).

### Attachment 3

#### EMERGENCY ACTION PLAN

**A3.1.** This plan has been developed for the protection, removal, or destruction of classified documents in the event of fire, natural disaster, civil disturbance, terrorist activities, or enemy action to minimize the risk of its compromise.

A3.1.1. Personnel will not be committed to tasks which are extremely dangerous or life-threatening. If evacuation becomes necessary the senior member evacuates all personnel according to the evacuation plan. When the fire, natural disaster, civil disturbance, terrorist activities, or enemy action has been terminated and it has been declared safe to re-enter the facility, inspect the safes for signs of entry or tampering and report discrepancies to 934 AW/IP.

A3.1.2. Each safe will have an easily identifiable number permanently attached to the exterior so it can be identified after any of the aforementioned situations.

A3.1.3. Protection of classified documents in the event of a civil disturbance /implementation of FORCE PROTECTION CONDITIONS (FPCON).

A3.1.4. Personnel will not be committed to tasks which are extremely dangerous or life-threatening. Once notified of a civil disturbance

A3.1.5. Minimize usage of classified information during FPCON implementation.

#### **A3.2. Fire:**

A3.2.1. Return all classified material to the security container, if possible, and lock the container.

A3.2.2. If the material cannot be returned to the security container, the person possessing the material will maintain custody until relieved or the material is secured in an approved security container.

A3.2.3. If classified cannot be removed from the building or security container cannot be locked, the Fire Chief will be notified immediately.

A3.2.4. When the Fire Chief declares the area safe, all classified material or its remains will be secured and HQ 934 AW/IP notified immediately.

#### **A3.3. Tornado or Natural Disaster.**

A3.3.1. Upon receiving warning of a tornado or severe weather, all classified material, which is not absolutely mission essential, should be placed in the security container and the container locked.

A3.3.2. If the classified material or security container is destroyed, scattered, or spirited away by natural forces, every effort will be made to find and secure the material or its remains and contact HQ 934 AW/IP for additional guidance.

A3.3.3. Should a container be found following a severe storm, which damages the base and buildings housing containers, contact HQ 934 AW/IP, who maintains a listing of containers.

**A3.4. Civil Disturbance:**

A3.4.1. All agencies will normally be warned in advance; however, should a disturbance occur without warning, return all classified material to the security container immediately and lock the container.

A3.4.2. The unit commander or staff agency chief determines if any additional protection is needed.

**A3.5. Terrorist Activities, or Enemy Action.**

A3.5.1. All agencies upon receiving information that a high threat of terrorist activities, or enemy action is announced , all classified material, which is not absolutely mission essential, should be placed in the security container and the container locked.

A3.5.2. The Force Protection Condition (FPCON) Checklist identifies FPCON measures from AFI 10-245, *The Air Force Antiterrorism (AT) Standards, Attachment 3*, and HQ AFRC added measures. This FPCON checklist **ONLY** incorporates those measures that apply to HQ AFRC personnel and facilities.

**Attachment 4**  
**SAMPLE COURIER LETTER**

(USE LETTERHEAD STATIONERY)

*Date*

MEMORANDUM FOR WHOM IT MAY CONCERN

FROM: *Office Symbol*

SUBJECT: Designation of Official Courier

1. Mr. John Doe, 022-22-2222, *office symbol, installation address*, is designated an official courier for the United States Air Force. Upon request, he will present his official identification card, number B0333444 and/or his DD Form 2501, Courier Authorization Form.
2. Mr. Doe is hand carrying two sealed packages, 8" x 8" x 24", addressed from *office symbol, installation address*, and addressed to *office symbol, installation address*. Each package is identified on the outside of the package by the marking "OFFICIAL BUSINESS. MATERIAL EXEMPTED FROM EXAMINATION" bearing the signature of the undersigned.
3. Mr. Doe is departing *Airport name* with a final destination to *Airport name*. He has a transfer point at *Airport name*.
4. This courier designation can be confirmed by contacting the undersigned at *office symbol, commercial number and DSN number*. This letter expires on *Date (not to exceed 7 days from date of issue)*.

JOHN G. SMITH, Col, USAF

Commander

**Attachment 5**  
**SAMPLE EXEMPTION NOTICE**

**Department of the Air Force**

**Organization/Office Symbol**

**Installation**

---

**OFFICIAL BUSINESS**

---

**MATERIAL EXEMPT FROM EXAMINATION**