



14 FEBRUARY 2000

Security

**INFORMATION SECURITY PROGRAM
MANAGEMENT**

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

NOTICE: A copy of this publication can be found digitally at <http://public.scott.af.mil/hqamc/pubs/pubhome2.htm>. If you cannot access this publication, please contact your local Base Publishing Office.

OPR: HQ AMC/SFOI (Mr. Scott Wobbe)
Supersedes AFI 31-401, AMC1 1 May 1995

Certified by: HQ AMC/SFO (Lt Col McMillian)
Pages: 3
Distribution: F

AFI 31-401, 1 January 1999, *Information Security Program Management*, is supplemented as follows. AMC units on AMC bases will comply with this supplement as well as base supplements. AMC units on other MAJCOM bases will follow that particular MAJCOM Information Security Program. AMC units located on other service component installations or civilian sectors will comply with this supplement. This supplement also applies to USAFR units on AMC bases.

SUMMARY OF REVISIONS

This document is substantially revised and must be completely reviewed.

1.3.5.1. In HQ AMC, provide the name of each directorate or staff agency's primary/alternate security manager to HQ AMC/SFOI. At AMC bases, these appointments will be provided to the Information Security Program Manager.

1.4.3. Semiannual security inspections should be conducted in January and July of each year. The ISPM may count the annual program review as one of the semiannual self inspections.

1.5.1. Unit commanders or staff agency chiefs are authorized to grant/certify access to Critical Nuclear Weapon Design Information (CNWDI) and certify "For the Commander, Air Mobility Command." In HQ AMC, directors and staff agency chiefs accomplish these actions.

2.1.3. AMC original classification authorities are:

<u>TOP SECRET</u>	<u>SECRET</u>	<u>Confidential</u>
AMC/CC	HQ AMC/DS	HQ AMC/IG
AMC/CV	HQ AMC/XP	DCS/CC

4.1. The following guidance will be used for transmission, control, and declassification of exercise messages classified for training only:

4.1.1. At the beginning of the exercise message include, "SECRET OR CONFIDENTIAL FOR TRAINING, OTHERWISE UNCLASSIFIED." Immediately below this include, "Handling Instructions: (Unit) and its tenant units handle this message as (insert classification), all other addresses treat as unclassified." This line may be modified to meet the users needs.

4.1.2. When portion marking use (C-TNG for CONFIDENTIAL and (S-TNG) for SECRET.

4.1.3. Declassify on the last day of the inspection, or date of the termination of the training period.

5.10.1.1. Provide a copy of the Top Secret Control Officer (TSCO) appointment letter to the servicing ISPM. Within HQ AMC send the appointment letter to HQ AMC/SFOI.

5.12. The Standard Form 702, Security Container Check Sheet, will be annotated each time a container is unlocked and locked during a tour of duty. At the end of the duty day, whether the container has been opened or not, ensure the "Checked By" column of the SF 702 is completed. If a container has more than one combination lock, a SF 702 is required for each lock.

5.13.2. Within HQ AMC, HQ AMC/SF approves requests for removing Secret and Confidential material from designated work areas during non-duty hours.

5.15.2. Within HQ AMC, HQ AMC/SF approves secure conference facilities.

5.18. The safeguarding of classified information is an owner/user responsibility.

5.23. Offices with more than one classified storage container will assign a different combination to each container. Combination changes are also required when containers are transferred to other offices or agencies.

5.28.3. Classified clean-out days should be conducted during the semiannual self-inspections. This is the time to destroy classified papers, plans, etc. that are not needed for a specific foreseeable purpose. Check with the local historian before destroying information that may be of historical value. Directorates, units or staff agencies are encouraged to continuously audit classified holdings throughout the year and destroy as necessary.

5.30.1. Within HQ AMC, the Director of Security Forces (HQ AMC/SF) approves alternative or compensatory measures.

9.3.2.1. The investigative official should be an impartial competent individual with an equal or higher grade than the person involved in the suspected compromise. The inquiry official may not be assigned to the same division, branch, or section as any of the people involved in the incident. Within HQ AMC, directors and staff agency chiefs appoint the investigative official.

9.4.1.1. Appointing officials may close investigations after technical review by local ISPM. Within HQ AMC, directors and staff agency chiefs may close investigations after technical review by HQ AMC/SF.

9.6.3. The Information Security Program Manager (ISPM) will submit, preferably via e-mail, RCS: AMC/SFO (Q)8101, Quarterly Security Violation Report, as of the last day of each quarter to reach HQ AMC/SFOI no later than the 12th of January, April, July, and October of each year. Negative reports are required and may be reported by telephone. The report is used to analyze problem areas, provide cross-feed throughout the command and report the health of the information security program to HQ USAF/XOFI.

9.6.3.1. Submit the report in the following format, listing only closed investigations.

9.6.3.1.1. Category of the incident: Compromise or security deviation.

9.6.3.1.2. Brief synopsis of the violation.

9.6.3.1.3. Brief synopsis of corrective action taken.

DENNIS A. HUNSINGER Colonel, USAF
Chief of Security Forces