

**BY ORDER OF THE COMMANDER
552D AIR CONTROL WING (ACC)**



AIR FORCE INSTRUCTION 31-401

**552 AIR CONTROL WING
Supplement**

**15 AUGUST 2008
Certified Current 10 September 2012**

Security

**INFORMATION SECURITY
PROGRAM MANAGEMENT**

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

ACCESSIBILITY: Publications and forms are available on the e-publishing website at www.e-publishing.af.mil for downloading or ordering.

RELEASABILITY: There are no releasability restrictions on this publication.

OPR: 552 ACW/SF

Certified by: 552 ACW/DS
(Lt Col Carson A. Elmore)

Supersedes AFI31-401_552ACWSUP1,
1 October 1997

Pages: 6

This supplement implements and extends the guidance of Department of Defense (DoD) 5200.1-R, *Information Security Program*, DoD 5200.2-R, *Personnel Security Program*, DoD 5220.22-M, *National Industrial Security Program*, Air Force Instruction (AFI) 31-501, *Personnel Security Program Management*, AFI 31-601, *Industrial Security Program Management*, and Technical Order (T.O.) 00-20F-2, *Inspection and Preventive Maintenance Procedures for Classified Storage Containers*, AFI 31-401, *Information Security Program Management*, 1 November 2005, and AFI 31-401, Air Combat Command (ACC) Supplement, *Information Security Program Management*, 7 April 2006. This supplement outlines the procedures, responsibilities and maintenance for providing an effective Information Security Program within the 552d Air Control Wing (552 ACW). Refer recommended changes and questions about this publication to the Office of Primary Responsibility (OPR) using the AF Information Management Tool (IMT) 847, *Recommendation for Change of Publication*; route AF IMT 847s from the field through Major Command (MAJCOM) publications/forms managers. Ensure all records created as a result of processes prescribed in this publication are maintained in accordance with AFMAN 33-363, *Management of Records*, and disposed of in accordance with the Air Force Records Disposition Schedule (RDS) located at <https://afrims.amc.af.mil>. This supplement is directive and applies to all units assigned to the 552 ACW.

SUMMARY OF CHANGES

This document is substantially revised and must be completely reviewed. This supplement has been revised to reflect new procedures for hand carrying classified off the installation. The Information, Personnel, and Industrial security checklist used for inspections has been dropped from the supplement. The new checklist may be obtained from the 552 ACW/SF. Refer recommended changes and questions about this publication to the Office of Primary Responsibility (OPR) using the AF IMT 847, *Recommendation*

for Change of Publication; route AF IMT 847s from the field through the appropriate functional's chain of command.

1.3.5.1.2. (Added) All 552 ACW squadron and group commanders will appoint, as a minimum, one primary and one alternate security manager, in writing, for a period of no less than 1 year to oversee their unit's information, personnel, industrial security and anti-terrorism programs. Squadron level appointment letters will be maintained by the responsible squadron security managers and a copy will be sent to their respective group security managers. Group level appointment letters will be maintained by the responsible group security managers and a copy will be sent to the 552 ACW/SF. The 552 ACW/SF appointment letter will be maintained by the 552 ACW/SF and a copy will be sent to 72 SFS/S5I.

1.3.5.2.1. (Added) Request for security managers training will be routed through the 552 ACW/SF to 72 SFS/SFAI within ten (10) workdays after appointment to the position of security manager.

1.3.6.11.11. (Added) Security Manager Handbooks will be established IAW the format contained in AFI 31-401, TAFB Supplement. Section 6 of the handbook will contain a listing of all applicable classified storage containers, vaults and secure rooms by identification number and location. In addition, Section 6 will also contain a Joint Clearance and Access Verification System (JCAVS) Eligibility and Access Report current within the last 30 days.

1.4.3.1. (Added) Semiannual self-inspections will be conducted by Security Managers assigned to a different unit under the same group as the inspected unit. For example, 964 AACS may conduct a semiannual self inspection on the 966 AACS program.

1.4.3.1.1. (Added) Security Managers designated to conduct unit security self-inspections will utilize a valid Air Combat Command Information/Personnel/Industrial Security Self-Inspection Checklist.

1.4.3.1.2. (Added) Reports, to include corrective action taken, will be forwarded to the organization commander and security manager no later than five (5) duty days following completion of the inspection.

2.6.6. (Added) Units will ensure a copy of security classification guides (SCGs) involving systems or programs related to weapons systems or programs assigned to the 552 ACW are provided to the respective Group Security Manager and the Wing Security Forces Liaison office (552 ACW/SF). SCGs which involve Special Access Programs (SAPs) need not be provided; however, agency POCs for these programs must be prepared to provide sound security classification guidance based upon approved SCGs for those programs. Agency POCs will consult with the respective Group Security Manager and/or the 552 ACW/SF, if necessary, should questions concerning classification guidance for a SAP arise. If required, the agency POC may in-brief and out-brief the Group Security Manager and/or the SF Liaison to resolve conflicts with assigned SAP guidance IAW applicable instructions.

4.3.1.6. (Added) All individuals creating working papers will review them every 60 days until the document is destroyed. Once the working papers have been reviewed, the individual will annotate on the front of the folder the date it was reviewed, the next review date, print and sign his/her name. Once completed, re-file the papers in the safe. The working papers will be created into a finished document 180 days from the original creation date of the working papers or destroyed.

5.8.8. (Added) Classified material may be received by registered, certified, first class, and/or express mail. All mail received by these channels will be treated as classified material and protected accordingly until it has been delivered to the addressee and determined if it contains classified. If the addressee can not be contacted, the mail will be stored in a General Services Administration (GSA) approved safe until such time the addressee is contacted and takes custody of the mail.

5.9.3.1. (Added) Each agency maintaining classified material will prepare applicable emergency planning security instructions. The security instructions must be realistic and reviewed at least annually to ensure a viable plan exists. These instructions will be posted on or near their respective safes/vaults.

5.9.3.2. (Added) Open Telephone Line Procedures. Individuals using unsecured telephone equipment in areas where classified or critical information is discussed will first announce the presence of an open line, and then ensure classified or sensitive conversations have ceased before placing or answering a call.

5.9.3.2.1. (Added) Cell Phone Handling Procedures. All 552 ACW offices with classified material must provide a cell phone holding area outside the main office entry door with signs posted accordingly. Prior to any classified discussion, personnel will be reminded to turn off all cell phones and place them in the holding area.

5.9.3.3. (Added) 552 ACW Classified Meeting Procedures.

5.9.3.3.1. (Added) Classified discussions/meetings held inside 552 ACW offices. Members will secure all doors and windows and place a "classified meeting in progress" or "open classified" sign on the main door.

5.9.3.3.2. (Added) Classified discussions/meetings held at mass gathering areas (i.e. OG auditorium, base theater, etc.). If such areas cannot be secured (locked doors and windows locked and covered) and/or allows personnel outside the area to hear the briefing, guards will be posted in a way to allow all exits/windows to be adequately observed. Personnel will not be allowed to loiter around exits/windows during the classified discussion/meeting. NOTE: All briefings involving Intel will require posting of adequate guards.

5.13.3.1. (Added) Prior to any foreign visitors receiving classified or unclassified briefings it must be coordinated through the 552 ACW/FDO and approved by 552 ACW/DS.

5.18.2.5. (Added) All 552 ACW units will notify their respective security managers in writing, who in turn, will notify 552 ACW/SF when a new classified safe is being activated or an existing classified safe is being moved/deactivated. As a minimum, security managers will provide safe updates to 552 ACW/SF quarterly.

5.18.2.6. (Added) All 552 ACW units will notify their respective security managers in writing, who in turn, will notify 552 ACW/SF when there is a change in classified safe custodians. Appointment letters will be signed by commanders and maintained by the respective security managers. As a minimum, security managers will provide safe custodian updates to 552 ACW/SF quarterly.

5.18.3. (Added) Units and agencies maintaining security containers for the storage of classified information will maintain a copy of T.O. 00-20F-2, *Inspection and Preventative Maintenance Procedures for Classified Storage Containers*, within the unit/agency for use by security managers and classified custodians.

6.8.1. (Added) Individuals requesting authorization to hand carry classified material off the installation must have a valid courier authorization letter IAW AFI 31-401, Tinker AFB Supplement. Courier letters must be validated through JPAS every 30 days as a minimum. This may be accomplished by annotating the date the security verification took place and the signature of the security manager conducting the verification at the bottom of the letter.

6.8.1.1. (Added) Requests will be forwarded to the appropriate approval official no later than five (5) duty days prior to the date of travel except for situations involving short-notice taskings/deployments. In

such cases, requests must be approved prior to departure. Requests will be in letter form and contain sufficient justification for hand-carrying the material.

6.8.1.2. (Added) The following are the appropriate approving officials:

6.8.1.2.1. (Added) 552 ACW Commander for Wing Staff

6.8.1.2.2. (Added) 552 ACW Group Commanders for their respective squadrons and staff agencies.

6.8.1.2.3. (Added) Unit commanders for 552 ACW geographically separated units, unless prohibited by local host base procedures.

6.8.2. (Added) The following information will be on the letter:

6.8.2.1. (Added) Explanation of arrangements made for storage at final destination and any enroute stops.

6.8.2.2. (Added) Classification of the material involved.

6.8.2.3. (Added) Complete itinerary and mode of travel for entire trip.

6.8.2.4. (Added) Name, rank, office, and duty phone of traveler(s).

6.8.2.5. (Added) State specific reason why the material cannot be transmitted by other approved means (e.g., registered, certified, first class, or express mail).

6.8.3. (Added) Unit letterhead will be used on all Courier Authorization Letters and will be signed only by those individuals identified in subparagraph **6.8.1.2.1. (Added)**, **6.8.1.2.2. (Added)**, **6.8.1.2.3. (Added)**, or their designated representative.

8.3.3.1.1. (Added) Security managers are responsible for developing training material for their respective units. Security managers will brief commanders on the unit's training program. (See **Attachment 11 (Added)** for sample training plan.)

9.8.2.1.1. (Added) All squadron security managers will notify their respective group security managers, who in turn, will notify 552 ACW/SF when a security incident occurs. Coordination with 72 SFS/S5I will be conducted and a security violation number will be obtained and tracked by the respective 552 ACW unit and group security managers.

9.8.2.1.2. (Added) All squadron security managers will obtain an IMT form 100 for respective 552 ACW squadron personnel, pending SIF action, separating from the military. The form will be forwarded to his/her respective group security manager, 552 ACW/SF and the 552 ACW/SSO.

9.9.1.3. (Added) Squadron commanders will appoint a preliminary inquiry official to conduct an inquiry for violations within their squadrons.

Attachment 11 (Added)**SECURITY EDUCATION TRAINING PLAN (ADDED)**

A11.1. (Added) General. Commanders and staff agency chiefs must ensure personnel understand the compelling need to protect classified/sensitive resources. To accomplish this, the security manager/supervisor will provide an initial security briefing upon arrival of newly assigned personnel (within 90 days). Do this in a one-to-one setting or as group discussion using training aids. Thereafter, security managers provide quarterly refresher training directly or by using guest speakers. **NOTE:** Training requirements vary depending on activity size, mission, location, type/amount of classified holdings, required access to restricted/controlled areas, etc. However, the below topics must be covered during initial training and at least once annually thereafter.

A11.2. (Added) Schedule:**A11.2.1. (Added) First quarter:**

A11.2.1.1. (Added) Marking, classifying, declassifying, transmitting, mailing, reproducing, storing, and destroying classified.

A11.2.1.2. (Added) Anti-Terrorism awareness briefing for all personnel.

A11.2.1.3. (Added) Counter-Intelligence/foreign travel briefing (as required).

A11.2.2. (Added) Second quarter:

A11.2.2.1. (Added) Human Intelligence (HUMINT) threat.

A11.2.2.2. (Added) Penalties for espionage and security violations and their adverse impact on national security.

A11.2.2.3. (Added) Security of classified and end-of-day checks.

A11.2.3. (Added) Third quarter:

A11.2.3.1. (Added) Operations Security (OPSEC).

A11.2.3.2. (Added) Entry control procedures to restricted areas and escort official responsibilities.

A11.2.3.3. (Added) Discuss the correct ways to transmit classified information.

A11.2.3.4. (Added) Procedures for granting access to classified information.

A11.2.3.5. (Added) Protection of NATO classified information (if applicable).

A11.2.4. (Added) Fourth quarter:

A11.2.4.1. (Added) Personnel security standards, special security files, initial and periodic reinvestigations.

A11.2.4.2. (Added) Supervisors responsibilities for security education training.

A11.2.4.3. (Added) Continuing evaluation of personnel.

A11.2.4.4. (Added) Anti-Terrorism awareness briefing.

A11.2.4.5. (Added) Safekeeping and storage of classified material.

NOTES:

1. In addition to training requirements above, provide localized orientation training (to include 25 question security awareness test) to all newly arrived personnel and discuss select topics from quarterly security manager's meeting and security incidents (if applicable) each quarter.
2. The above sample plan is not all inclusive of items that can be part of your unit security education training plan. However, unit commanders/staff agency chiefs and security managers must ensure the training requirements are outlined in DOD 5200.1R, Chapter 10, are met. Methods for conducting security training may be the use of lectures, visual aids, videos, and/or guest speakers.

LORI J. ROBINSON, Brig Gen, USAF
Commander, 552d Air Control Wing