

433AW I31-401

BY ORDER OF THE COMMANDER 433d AIRLIFT WING

433 AW INSTRUCTION 31-401

1

01 Jun 2000

INFORMATION SECURITY PROGRAM (ISP)

OPR: 433 SFS/SFI (SMSgt Anderson J. Childers Jr.)

Certified by: 433 SPTG/CCD (Lt. Col. Harvey T. Sekimoto)

Pages: 7/Distribution: F

This Instruction implements the requirements of DoD 5200.1-R, *Information Security Program Regulation*, AFPD 31-4, *Information Security*, AFI 31-401/AFRC Supplement, *Managing the Information Security Program*, AFI 31-501, *Personnel Security Management*. It prescribes procedures and responsibilities of all 433 AW Organizations; specifically all staff agency chiefs, security managers(SM), security monitors, and Top Secret Control Officers (TSCO). The 76 SFS/SFAI provides information security oversight and personnel security investigation (PSI) support to 433 AW and submits all PSIs to the Defense Security Service (DSS). Each commander/director/staff agency chief is responsible for ensuring assigned personnel comply with DoD 5200.1-R, AFPD 31-4, AFI 31-401/AFRC Supplement and this Instruction.

SUMMARY OF REVISIONS

This revision realigns (Local Procedures) with the current requirements of DoD 5200.1-R, AFPD 31-4, AFI 31-401 AFRC Supplement and AFI 31-501. A (I) indicates revisions from previous edition.

1. Appointments and Responsibilities.

1.1. (Added) Commander/Staff Agency Chiefs will:

1.1.1. (Added) As the responsible officer in charge of the Information Security Program, appoint in writing a Primary and Alternate SM, in the grade of GS-07 or E-6 or above to manage the Information and Personnel Security Programs. Larger units/sections are encouraged to appoint security monitors at each section to assist the SM. Forward the original appointment letter to the 433 SFS/SFI.

1.1.2. (Added) Review self-inspections reports and provide a written endorsement of concurrence on corrective action to be taken.

1.1.3. (Added) Designate a Primary and Alternate Top Secret Control Officer (TSCO) and identify personnel who are authorized to review Top Secret material.

1.1.4. (Added) Designate in writing, Safe/Classified Custodians and those who have access to safe combinations and personnel to perform end of day security checks.

1.1.5. (Added) Review security access requirements (SAR Codes) coded in the Unit Manpower Document (UMD), Automated Security Clearance Approval System (ASCAS) roster annually to

ensure clearance eligibility requirements are consistent with mission needs. Document this review and file in the SMs handbook. SAR codes should accurately reflect day-to-day access. Over inflating SAR codes may be construed as fraud, waste, and abuse.

1.1.6. (Added) Designate in writing, personnel authorized to receive classified material and forward the original letter to the 433 CF/SCB and 433AW/CP. Designate in writing personnel authorized to open the inner wrappers of classified material and who can have access to classified material. Maintain file copies in the unit security manager's handbook.

1.2. (Added) Security Manager (SM) will:

1.2.1. (Added) Maintain a Security Manager's handbook as outlined in the AFI 31-401 and host base supplement.

1.2.2. (Added) Develop Internal Operating Instructions (OIs) and include them as part of the unit initial indoctrination and recurring training programs.

1.2.3. (Added) Brief individual(s) appointed to conduct semi-annual security self-inspections. Monitor the inspection and ensure the commander reviews and endorses the report, and forward a copy of the report with identified corrective action to the Information Security Program Manager (ISPM). Maintain the last two self-inspection reports in the security manager's handbook.

1.2.4. (Added) Ensure SF 312s, *Classified Information Nondisclosure Agreement*, are executed, and forwarded to 433 SFS/SFI to be updated, and forwarded in accordance with AFI 31-401.

1.2.5. (Added) Ensure that personnel having access to TOP SECRET information are given the oral attestation prior to having access.

1.2.6. (Added) Have access to required publications for administering the security program.

1.2.7. (Added) Attend scheduled monthly security manager's meetings, and ensure the information received is disseminated throughout the unit.

1.2.8. (Added) Establish and maintain an aggressive and recurring security-training program in accordance with AFI 31-401, para 9.4. The scope and depth of the security training should be geared toward the unit mission, needs, and the individual receiving the training. See attachment 1 for training requirements.

1.2.9. (Added) Ensure authorized personnel conduct Foreign Travel briefings.

1.2.10. (Added) Ensure computer security officers are assigned to the unit.

1.2.11. (Added) Coordinate restricted area badge and AF Form 2586, *Unescorted Entry Authorization Certificate*, issues with 433 SFS/SFI.

2. Classification or declassification of classified material or information:

2.1. (Added) 4 AF/CC has been designated as a Secret Original Classification Authority (OCA). The authority to originally classify information will be exercised sparingly and only when no promulgated classification guidance exists.

3. Classification challenges:

3.1. (Added) All personnel must challenge classification decisions, which they believe, are improper. If information is received which is believed to be improperly classified, or an overly restricted period of continued classification has been assigned, the ISPM and security manager will be contacted.

3.2. (Added) The classified information being challenged will be safeguarded at the highest level of classification. If the information is SECRET and the challenge is for downgrading to CONFIDENTIAL, the information must still be safeguarded as SECRET until the challenge has been resolved.

3.4. (Added) The ISPM and security manager will ensure challenges are acted upon within thirty (30) days.

4. Marking Classified Information.

4.1. (Added) The originator of classified information is responsible for proper application of classification markings. This includes derivative classification decisions and working papers.

4.2. (Added) Those who prepare derivative classified documents are strongly encouraged to consult with their SM and review Executive Order 12958, chapter 4 in DoD 5200.1-R, AFI 31-401 and DoD 5200.1PH, *A Guide to Marking Classified Documents*.

4.3. (Added) Marking Working Papers. Date and annotate all working papers with the OPR/action officer in ink, keep a record of all "DERIVED FROM" sources attached to the working paper, and properly mark the working paper with the highest overall classification and term "WORKING PAPERS" at the top and bottom of each page.

5. Safekeeping and Storage.

5.1. (Added) Offices storing small numbers of classified documents that do not warrant an entire security container (approved GSA safe) may request courtesy storage from another office. In this case, a letter of agreement between the two offices is maintained in the safe with the documents. Additionally, the documents must be separated from the safe contents by placing them in a sealed envelope/container.

5.2. (Added) Safe Custodians. The first person listed on the SF 700, *Security Container Information*, is considered the primary safe custodian. Safe custodian responsibilities:

5.2.1. (Added) Ensure safe combinations are changed at required intervals.

5.2.1.1. (Added) Combinations are changed when placed in use; whenever an individual knowing the combination no longer requires access; when the combination has been subject to compromise; at least every 2 years; or when taken out of service.

5.3. (Added) Report container malfunction to 76 CES customer service desk.

5.4. (Added) Ensure all documents placed in the safe are properly marked.

5.5. (Added) Ensure safe contents are identified in unit office file plans.

5.6. (Added) Become familiar with T.O. 00-20F-2, *Inspection and Preventative Maintenance Procedures for Classified Storage Containers*, requirements.

5.7. (Added) Properly mark each safe with an easily identifiable number (for example, XP-01) permanently attached to the exterior so it can be identified after natural disasters.

5.8. (Added) Emergency protection and removal of classified material:

5.8.1. (Added) The possibility of fire, civil disturbance, terrorist activity, or natural disaster at Kelly AFB, TX. requires development and possible implementation of special procedures for safeguarding and emergency removal of classified material to preclude the material from falling into unauthorized hands. A situation may develop that requires higher headquarters, 4th Air Force commander, 433 AW commander, 433 SFS commander or a designated representative to direct implementation of emergency protection or removal of classified material.

5.8.2. (Added) Procedures:

5.8.2.1. (Added) Upon notification of emergency removal of classified material implement the following emergency procedures:

5.8.2.2. (Added) Remove all classified from security containers and computers.

5.8.2.3. (Added) Place the classified material in a large envelope(s), boxes, or appropriate container and mark same, using the highest classification of the contents therein. If time permits accomplish accountability with records/receipts.

5.8.2.4. (Added) Safeguard the classified material and wait for further instructions from the 433 wing commander or designated representative.

5.8.2.5. (Added) Upon notification of emergency evacuation of classified material, transport the classified material to the location designated by the 433 AW commander, installation commander, or their designated representative for evacuation.

5.8.2.6. (Added) Upon notification of termination of emergency protection/evacuation procedures:

5.8.2.7. (Added) Retrieve the classified material from the designated location and return it to its proper storage area.

5.8.2.8. (Added) Inventory all classified material prior to returning it to the security container.

5.8.3. (Added) In case of fire or natural disaster (tornado, hurricane, earthquake, etc), which results in damage to the building, 433 AW commander or his designated representative will manage available personnel resources to ensure classified material within the building is protected.

5.8.4. (Added) Order of Priority when removing classified:

5.8.4.1. (Added) First Priority. Top Secret

5.8.4.2. (Added) Second Priority. Secret

5.8.4.3. (Added) Third Priority. Confidential.

6. Destruction of classified material:

6.1. (Added) Destruction of classified material must be approved by the unit commander, security manager, or classified custodian. Classified material belonging to 433 AW can be destroyed by using the unit's approved cross-cut shredding machine located in the 433 Command Post or by taking the material to 433 CF/SCM for large volume shredding.

6.2. (Added) Annual Clean out Week. The annual cleanout week for Kelly AFB is the first week of August. Each commander/staff agency responsible for maintaining/storing classified will ensure that the safe custodians to review all classified documents for destruction. Provide a written response to 433 SFS/SFI in reference to how many pages of classified were destroyed.

7. Transmitting Classified Materials:

7.1. (Added) 433 CF/SCB is responsible for processing incoming and outgoing distribution.

7.2. (Added) Protect all first class, registered, certified, and Federal Express (or whoever holds current GSA contract), mail as classified information until opened.

7.2.1. (Added) Accountable mail received with the incorrect or improper address is referred to the respective commander/staff agency chief. In these cases, the commander/director or SM opens the container to determine the proper addressee. The receipt and container are annotated with the appropriate address before forwarding.

7.3. (Added) Removal of Classified Documents from HQ 433 AW (On Base):

7.3.1. (Added) Commanders/staff agency chiefs or supervisors approve appropriately cleared personnel to remove classified information from the work area for the following purposes:

7.3.1.1. (Added) Routine destruction at the base destruction facility.

7.3.1.2. (Added) For official duties on Kelly AFB for handcarrying classified documents the following will be accomplished: obtain supervisor's permission to remove/pick-up the classified material from the workplace, attach the appropriate cover sheet, that is , SF 704, *Secret Cover Sheet*, or SF 705, *Confidential Cover Sheet*, and enclose the material in an outer container such as a sealed envelope, folder (closed with a lock, tie, or Velcro), briefcase, zipper bag, etc.

NOTE: Classified markings must not appear on the outer container.

7.4. (Added) Removal of Classified Documents from HQ 433 AW (Off Base):

NOTE: Within AFRC, removing classified documents/equipment from designated work areas to work on at home is strictly prohibited.

7.4.1.1. (Added) For transmission off the installation see DoD 5200.1-R and AFI 31-401.

7.4.1.2. (Added) Personnel authorized to remove classified information must be briefed on their responsibilities for protection of classified by their supervisor or SM. This briefing can be annotated on DD Form 2501, *Courier Authorization (Accountable)*, or letter.

7.4.1.3. (Added) Additional written authorization is required when traveling by aircraft. Consult with your SM and ISP directives listed above.

8. Reporting a security incident:

8.1. (Added) The unit commander and unit security manager will be notified immediately when classified material is compromised, suspected of being compromised, or administratively mishandled and will immediately notify the 433 SFS/SFI for action.

8.2. (Added) The unit commander will appoint, in writing, a disinterested Noncommissioned Officer (E-7 or above), a commissioned officer or a civilian employee (GS-7 or above) to conduct inquiries or investigations into the events surrounding the suspected violation per AFI 31-401. Provide a copy of the appointment letter to 76 SFS/SFAI and 433 SFS. The inquiry/investigation report will be completed within 10 working days and forwarded to 76 SFS/SFAI . If the investigation official needs more time, he/she will, in writing, request additional time from the 433 AW commander and forward this request to 76 SFS/SFAI.

8.3. (Added) Security Violation Involving Electronic Mail (e-mail).

8.3.1. (Added) Once there is suspected security violation involving e-mail, contact the network system administrator, network control center, and the 433 SFS/SFI.

8.3.2. (Added) Comply with the requirements outlined by the network system administrator, network control center and 433 SFS/SFI, and assist the inquiry official during their investigation.

9. Automated Information Systems (AIS):

9.1. (Added) Computer systems must be approved by the designated approving authority prior to processing classified.

9.2. (Added) All removable AIS and word processing media are marked externally with the highest overall classification contained therein via SF 706, *Top Secret ADP Media Classification Label*; SF 707, *Secret ADP Media Classification Label*; or SF 708, *Confidential ADP Media Classification Label*.

9.3. (Added) Sections using Global Command Control Systems (GCCS) to produce classified documents will log all printed documents on an AF Form 3137, *General Purpose Form*, to ensure accountability. All documents will be protected and destroyed in accordance with DoD 5200.1-R. Once documents are destroyed record their destruction date on the AF Form 3137.

10. Personnel Security.

10.1. (Added) The SM will monitor the Personnel Security Program to ensure that a current ASCAS roster is maintained in the SM Handbook.

10.2. (Added) For newly assigned personnel, the SM will conduct initial security briefings and check the ASCAS roster to validate security clearances and past security clearance history.

10.3. (Added) Ensure timely notification of personnel identified for a periodic reinvestigation (PR) and assists them with completing appropriate forms and entering the date into EPSQ. Maintain the Electronic Personnel Security Questionnaire (EPSQ) on selected computers for personnel to update their clearances.

10.3.1. (Added) The SM will ensure that the AF Form 2583, *Request for Personnel Security Action* is completed and EPSQ is free of errors prior to being forwarded to 433 SFS/SFI.

10.4. (Added) If the commander believes a condition exists that may affect the security eligibility of an individual, a recommendation will be to the base ISPM through the wing security manager to establish a Special Security File (SSF). The request must be fully justified and supported by clear rationale based on facts in the case.

BERNARD J. PIECZYNSKI, Brig Gen, USAFR
Commander