

BY ORDER OF THE COMMANDER



**AIR FORCE OPERATIONAL TEST AND
EVALUATION CENTER INSTRUCTION 31-401**

14 MARCH 2003

Security

**THE AFOTEC INFORMATION SECURITY
PROGRAM**

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: HQ AFOTEC/SF (Mr. Floyd L. Collins)

Certified by: AFOTEC/CV
(Col Douglas R. Lincoln, Jr.)

Supersedes AFOTECI 31-401, 6 November 2002

Pages: 16
Distribution: F

This instruction implements AFI 31-401, *Information Security Program Management*, which was substantially revised on 1 November 2001. This instruction establishes procedures and assigns responsibilities within AFOTEC relative to the handling and safeguarding of classified information. It applies to HQ AFOTEC, Kirtland AFB, as well as all Detachments and Operating Locations. It does not apply to Special Access Programs within AFOTEC that are governed by other regulations. Directorates, Detachments, and Operating Locations should publish their own instruction covering specific or unique security practices, procedures, and responsibilities. Ensure that all records created as a result of processes prescribed in this publication are maintained in accordance with Air Force Manual (AFMAN) 37-123, *Management of Records*, and disposed of in accordance with Air Force WEB-RIMS Records Disposition Schedule (RDS) located at <https://webrims.amc.af.mil/rds/index.cfm>

SUMMARY OF REVISIONS

This document has been revised to: reflect position Security Access Requirement (SAR) codes have changed to Investigation codes; change guidance regarding mailing classified reports; delete requirement for Safe Custodians to maintain an inventory of Secret and Confidential material, if practical; and delete requirement for Safe Custodian to maintain records of Secret and Confidential destruction, if practical.

1. RESPONSIBILITIES:

1.1. HQ AFOTEC/SF.

1.1.1. Manage the AFOTEC Information Security Program and Personnel Security Program. Resolve information security/personnel security problems/issues within AFOTEC.

1.1.2. Conduct Information Security Program Reviews (ISPRs) of AFOTEC Directorates and Detachments on an annual basis. Distribute tentative ISPR schedule to Security Managers annually. Personnel Security Program will also be included during ISPRs.

1.1.3. Provide training, assistance and guidance required by referenced publications to Security Managers and assigned personnel.

1.1.4. Provide a basic security orientation to newly-assigned personnel in conjunction with issuance of their AFOTEC badge.

1.1.5. Brief personnel who are appointed to conduct investigations involving the loss or compromise of classified information.

1.1.6. Maintain records of classified storage containers and vaults.

1.1.7. Utilize Sentinel Key Clearance Access Verification System (CAVS) for clearance management and verification. Provide copies of CAVS roster to Directorate and Detachment Security Managers located on KAFB. Note: Sentinel Key will be replaced with Joint Personnel Adjudication System (JPAS).

1.1.8. Obtain a signed SF Form 312, **Non Disclosure Agreement**, from HQ AFOTEC civilian and military personnel upon issuance of initial security clearance. Provide individual a briefing on their responsibility to protect classified information at the time the SF 312 is signed.

1.1.9. Complete AF Form 2583, **Request for Personnel Security Action**, for HQ AFOTEC personnel who require a security clearance or any special access (i.e., NATO, CNWDI or SIOP).

1.1.10. Process HQ AFOTEC personnel for required clearance investigation and submit clearance package to appropriate investigating agency.

1.1.11. Contact adjudication facilities and investigative agencies regarding clearance/investigation status checks on assigned personnel.

1.1.12. Process and maintain copies of Suitability Determinations and Security Information Files (SIFs) on HQ AFOTEC personnel.

1.1.13. Obtain a signed AF Form 2587, **Security Termination Statement**, from HQ AFOTEC civilian personnel who terminate employment and military personnel who separate or retire from military service. Also obtain a signed AF Form 2587 from individuals who have their access or clearance suspended, revoked or denied.

1.1.14. Submit the SF 311, **Agency Information Security Program Data**, report to Information Security Oversight Office (ISOO) by 31 October of each year.

1.1.15. Semi-annually report to HQ USAF/SFI, by 31 January and 31 July of each calendar year, the number and type of violations and infractions.

1.1.16. Submit SIOP access data to HQ USAF/XOFI by 15 January of each calendar year.

1.1.17. Assist personnel who require restricted area badges with completion of the AF Form 2586, **Unescorted Entry Authorization Certificate**, in accordance with AFI 31-101, *The Air Force Physical Security Program*.

1.2. Directors and Commanders:

1.2.1. Appoint a Primary and an Alternate Security Manager for the Directorate, Detachment, or Operating Location.

1.2.2. Appoint a Top Secret Control Officer (TSCO) if the Directorate or Detachment stores any Top Secret material.

1.2.3. Appoint individuals to conduct security self-inspection of the Directorate, Detachment, or Operating Location on a semi-annual basis. ISPRs conducted by HQ AFOTEC/SF may count as one self-inspection.

1.2.4. Annually review position investigation codes to ensure investigative and clearance requirements are consistent with mission needs.

1.2.5. Ensure procedures are in place to internally control Secret and Confidential material.

1.3. HQ AFOTEC Security Managers (including Det 1 & Det 3):

1.3.1. Complete required Security Manager training provided by HQ AFOTEC/SF within 90 days of appointment.

1.3.2. Manage the Information Security Program within their Directorate/Detachment.

1.3.3. Provide advice and assistance to the Commander/Director and all assigned personnel on security matters and referenced security guidance.

1.3.4. Provide initial security training to newly assigned personnel upon arrival, and refresher security training to personnel on at least a quarterly basis.

1.3.5. Monitor the unit's copy of the CAVS roster. Process investigation code changes when required. A sample investigation code change is posted on the Security Homepage on the AFOTEC MIN.

1.3.6. Issue Courier Authorization Letters to personnel who act as couriers of classified material. The Security Homepage on the AFOTEC MIN contains a sample Courier Authorization Letter.

1.3.7. Ensure that personnel who travel to foreign countries receive a foreign travel briefing to alert them to possible exploitation by hostile intelligence services. Maintain a record of personnel participating in foreign travel for leisure purposes.

1.3.8. Maintain a record of the combinations to all security containers and vaults within the Directorate/Detachment. Security container combinations must be safeguarded to the highest level of classified stored in the security container.

1.3.9. Designate whether reproduction equipment, shredders, and faxes are authorized for classified information. Utilize AFOTECVAs 31-1, 31-2, 31-3 and 31-4 to identify equipment.

1.3.10. Provide HQ AFOTEC/SF a list of all storage containers, vaults, and open storage areas. The list must show container number, office symbol, and building/room number. Provide an updated list as changes occur.

1.3.11. Certify the AFOTEC Form 12, **Visit Request**, for all unit personnel visiting other organizations.

1.3.12. Provide HQ AFOTEC/SF an SF 311 containing data for item #6 on the form. Sample data for item #6 (Number of classification decisions) during a consecutive two-week period each quarter (Nov-Jan, Feb-Apr, May-Jul, and Aug-Sep).

1.4. Det/OL Security Managers (excluding Det 1 & Det 3):

1.4.1. Complete required security manager training offered by the host Information Security Program Manager (ISPM) within 90 days of appointment.

- 1.4.2. Manage the Information Security program and Personnel Security program within their Det/OL.
- 1.4.3. Provide advice and assistance to the Commander and assigned personnel on security matters and referenced security guidance.
- 1.4.4. Provide a basic security orientation to newly-assigned personnel. Provide refresher training to personnel on at least a quarterly basis.
- 1.4.5. Brief personnel who are appointed to conduct investigations involving the loss or compromise of classified information.
- 1.4.6. Provide couriers of classified material a Courier Briefing and issue a DD 2501, **Courier Authorization Card**, and/or Courier Authorization Letter as appropriate. The Security Homepage on the AFOTEC MIN contains a sample Courier Authorization Letter.
- 1.4.7. Maintain a record of the combinations to all security containers and vaults within the Detachment or Operating Location. Security container combinations must be safeguarded to the highest level of classified stored in the container.
- 1.4.8. Provide HQ AFOTEC/SF a list of all storage containers, vaults, and open storage areas. The list must show container number, office symbol, and building/room number. Provide an updated list as changes occur.
- 1.4.9. Designate whether reproduction equipment, shredders, and faxes are authorized for classified information. AFOTECVAs 31-1, 31-2, 31-3 and 31-4 may be used to identify equipment. Other locally approved visual aids may also be used to identify equipment.
- 1.4.10. Certify the AFOTEC Form 12 for all unit personnel visiting other organizations.
- 1.4.11. Provide HQ AFOTEC/SF an SF 311 containing data for item #6 on the form. Sample data for item #6 (Number of classification decisions) during a consecutive two-week period each quarter (Nov-Jan, Feb-Apr, May-Jul, and Aug-Sep).
- 1.4.12. Obtain a signed AF Form 2587 from civilian personnel who terminate employment and military personnel who separate or retire from military service. Also obtain a signed AF Form 2587 from individuals who have their access or clearance suspended, revoked, or denied.
- 1.4.13. Utilize Sentinel Key CAVS for clearance management and verification. Note: Sentinel Key will be replaced by Joint Personnel Adjudication System (JPAS).
- 1.4.14. Process investigation code changes when required. A sample investigation code change is posted on the Security Homepage on the AFOTEC MIN.
- 1.4.15. Obtain a signed SF 312 from civilian and military personnel upon issuance of initial security clearance. Provide individual a briefing on their responsibility to protect classified information at the time the SF 312 is signed.
- 1.4.16. Complete AF Form 2583 for all personnel who require a security clearance or any special access (i.e., NATO, CNWDI, or SIOP).
- 1.4.17. Notify personnel requiring a clearance investigation and assist them in completing the required clearance questionnaire. Review questionnaire for accuracy, and submit clearance packages to host Security Forces for processing.

1.4.18. Provides assistance to Det CC on Suitability Determinations and Security Information Files (SIFs).

1.4.19. Ensure that personnel who travel to foreign countries receive a foreign travel briefing to alert them to possible exploitation by hostile intelligence services. Maintain a record of personnel participating in foreign travel for leisure purposes.

1.4.20. Assist personnel who require restricted area badges with completion of the AF Form 2586 in accordance with AFI 31-101.

1.5. **Top Secret Control Officers (TSCOs):**

1.5.1. Ensure Top Secret material is stored only in a security container specifically authorized for Top Secret storage.

1.5.2. Maintain accountability and control of all Top Secret material within the Directorate/ Detachment/OL.

1.5.3. Perform all destruction, reproduction, and transmission of Top Secret material.

1.6. **Supervisors:**

1.6.1. Verify, through the Directorate, Detachment or Operating Location Security Manager, or HQ AFOTEC/SF, the security clearance of newly assigned personnel before allowing such personnel access to any classified information. Provide, or arrange for, any security training that is deemed necessary.

1.6.2. Ensure that subordinates receive recurring security training/guidance throughout their duty assignment. Ensure that security training is properly documented in the individual's official personnel records and that they receive credit for attending and completing security courses.

1.6.3. Continually observe subordinates for personal problems or adverse conduct that could have a bearing on their continued eligibility for access to classified information. Report any derogatory information to the security manager or HQ AFOTEC/SF.

1.6.4. Take into consideration adherence to security requirements and procedures when rating subordinates on their job performance.

1.6.5. Ensure that subordinates terminating employment or separating/retiring from military service out-process through HQ AFOTEC/SF, or through Detachment Security Manager, to accomplish the following required actions:

1.6.5.1. Sign the AF Form 2587.

1.6.5.2. Receive required security debriefings (e.g., NATO, CNWDI, SIOP) as appropriate.

1.6.5.3. Surrender their AFOTEC identification badge, Restricted Area badge (if any), and DD Form 2501 (if any).

1.7. **All Cleared Personnel:**

1.7.1. Understand the standards of conduct required of a person in a position of trust, and the moral and legal responsibilities for protecting classified information.

1.7.2. Comply with all relevant Air Force and AFOTEC security requirements and procedures. If necessary, seek guidance from the Security Manager or HQ AFOTEC/SF.

1.7.3. Report to their Supervisor, Dir/Det CC, Security Manager, or HQ AFOTEC/SF any information that could adversely reflect on their suitability for continued access to classified information, or a co-workers suitability for continued access to classified information.

1.7.4. Report derivative classifications decisions to their Security Manager when requested for tracking purposes.

1.7.5. Verify the security clearance and need-to-know of any person requesting access to classified information **before** allowing that person access. For non-AFOTEC individuals, verify security clearance through their organization's Security Manager or Facility Security Officer (FSO).

1.7.6. Immediately report any security violation or any loss, compromise, or suspected compromise of classified information to their Supervisor, Dir/Det CC, or Security Manager, who in turn notifies HQ AFOTEC/SF. Immediately provide protection to any classified material found unprotected.

1.7.7. Report foreign travel and suspicious foreign contacts to their Security Manager or HQ AFOTEC/SF.

2. CLASSIFICATION AND DECLASSIFICATION OF INFORMATION.

2.1. Personnel who prepare classified documents shall coordinate with the Security Manager or HQ AFOTEC/SF to ensure the documents are properly classified and marked.

2.2. Consult DoD 5200.1-I, *DoD Index of Security Classification Guides*, to identify guides that apply to OT&E operations. In the absence of classification guidance for a system in the OT&E process, the Commander, AFOTEC, has original classification authority up to and including the Top Secret level. Should original classification of OT&E information be necessary, coordinate with HQ AFOTEC/SF.

2.3. HQ AFOTEC/HO has primary responsibility for ensuring AFOTEC's compliance with the *25-Year Automatic Declassification Plan* mandated by EO 12958. The Plan calls for the identification of any classified documents more than 25 years old, followed by a declassification review of each identified document. Whenever possible, such information shall be declassified. The results of declassification reviews will be reported to HQ USAF/XOFI.

3. MARKING CLASSIFIED INFORMATION.

3.1. All classified documents and other classified material produced within AFOTEC must be marked in accordance with EO 12958 and DoD 5200.1-R, *Information Security Program*.

3.2. Use DoD 5200.1-PH, *DoD Guide to Marking Classified Documents*, for definitive guidance on how to mark classified documents and other material. If in doubt about any marking requirement, contact HQ AFOTEC/SF.

3.3. Refer to AFOTECI 61-204, *Disseminating Scientific and Technical Information*, for required distribution statements and destruction notices on test plans and reports generated within AFOTEC.

4. SAFEGUARDING CLASSIFIED INFORMATION.

4.1. Access to Classified Information:

4.1.1. Before releasing classified information to another individual, confirm that individual's **authorized access level** through his/her security manager or HQ AFOTEC/SF. The Security Man-

ager or HQ AFOTEC/SF will check the CAVS Roster or Sentinel Key for the individual's current authorized access level. If the individual is not a member of AFOTEC, check his or her visit request on file with HQ AFOTEC/SF or Det/OL Security Manager.

4.1.2. In addition to having an authorized access level commensurate with the level of classified information involved, an individual must also have a **need-to-know** the information and must have previously signed the SF 312.

4.1.3. Classified information may not be released outside the Air Force unless such release is provided for on the document itself or the originator of the document has authorized the proposed release.

4.1.4. Only the Commander, AFOTEC, may authorize release of AFOTEC classified information outside the Executive Branch of the U.S. Government.

4.2. Storage of Classified Material:

4.2.1. The first person listed on the SF Form 700, **Security Container Information**, shall be considered the Safe Custodian. The Safe Custodian shall:

4.2.1.1. Ensure that security container combinations are changed when placed in use; whenever an individual knowing the combination no longer requires access; when the combination has been subjected to possible compromise; and when taken out of service.

4.2.1.2. Comply with the restrictions on the use of security containers (i.e., they may not be used to store money, valuables, or weapons).

4.2.1.3. Ensure that any classified material not associated with a current program is destroyed, unless its continued retention has been authorized.

4.2.1.4. Report any security containers or locks that malfunction to HQ AFOTEC/SF, who will make arrangements with contracted locksmith for repairs. Det/OL custodians contact their Security Manager to make repair arrangements.

4.2.1.5. Identify the contents of the safe (in an unclassified manner) in the unit's file plan.

4.2.1.6. Ensure the AFTO 36, **Maintenance Record for Security Type Equipment**, is affixed inside the locking drawer of each security container. Ensure routine maintenance is conducted on security container every five years IAW TO-00-20F-2, *Inspection and Preventative Maintenance Procedures for Classified Storage Containers*. Any maintenance performed on the container must be recorded on the AFTO 36.

4.2.1.7. Ensure Emergency Protection/Removal of Classified Material Plan (**Attachment 1**) is posted on or near each security container used to store classified material.

4.2.1.8. Ensure the AF Form 614, **Charge Out Record**, is utilized when classified material is withdrawn from a security container. The title of documents will be identified on the form in an unclassified manner.

4.3. Removal of Classified Material from AFOTEC Facilities:

4.3.1. Only Commander, Directors, Security Managers, or HQ AFOTEC/SF may authorize the removal of classified material from an AFOTEC facility. All buildings at or near the intersection of Wyoming and Gibson on Kirtland AFB comprise the HQ AFOTEC facility.

4.3.2. Removal of classified material from an AFOTEC facility will be for one of the following reasons:

4.3.2.1. Destruction at the installation's classified destruction facility.

4.3.2.2. Presentation at an approved classified meeting or conference.

4.3.2.3. In conjunction with official OT&E efforts in the field or at U.S. Government installations.

4.3.2.4. Transmission by courier from AFOTEC to another DoD activity or a cleared contractor facility – **when time does not permit mailing the material to the destination.** Personnel authorized to hand-carry classified material will have a DD Form 2501 and/or Courier Authorization Letter, in their possession. A trip-specific Courier Authorization Letter is required when a courier carries classified information aboard commercial aircraft.

4.3.2.5. When conditions warrant emergency protection/removal. Reference **Attachment 1** of this instruction.

4.4. **Classified Meetings and Conferences:**

4.4.1. Conference rooms and presentation centers will be locked when not in use. The AFOTEC official who arranges for or convenes a classified meeting is responsible for security of the meeting.

4.4.2. Ground rules for conducting classified meetings are stipulated in the pamphlet, "*Classified Meetings*," published by HQ AFOTEC/SF. This pamphlet is available on the Security Homepage on the AFOTEC MIN.

4.4.3. SAF/AA must approve any classified meeting, conference, or seminar to be held at a non-Government, uncleared facility. The AFOTEC official in charge of such meetings must send a formal request through HQ AFOTEC/SF to HQ USAF/XOFI. The request must include a security plan as specified in DoD 5200.1-R, paragraph 6-307.

4.5. **End-of-Day Security Checks.** Individuals appointed to conduct end-of-day security checks must accomplish, as a minimum, the following actions:

4.5.1. Ensure that all classified documents, computer disks, typewriter ribbons, removable hard drives, etc. have been secured in approved security containers.

4.5.2. Check desk tops, tables, file cabinets, credenzas, computer workstations, filing baskets, etc, for unsecured classified material.

4.5.3. Check all secure telephone units (STU and STEs) and secure fax machines to ensure that the crypto ignition key (CIK) and Fortezza Card has been removed and stored.

4.5.4. Check all video teleconferencing equipment to ensure that CIK has been removed and stored.

4.5.5. Check each security container by rotating the dial of each lock at least four times in the same direction and then depressing the handle of each locking drawer. Enter the time of the check and initials on the SF 702, **Security Container Checklist**. Security containers must be checked at the end of each duty day, even if the container was not opened.

4.5.6. After completing the above actions for each assigned office area, fill out the SF Form 701, **Activity Security Checklist**. List the names of any individuals still working within the area and record the safe number of any safe that is open and in use by those individuals. Remind the individuals that **they** are responsible for ensuring that all open security containers are properly secured before departing the area.

4.6. **Reproduction of Classified Information:**

4.6.1. If approved by a supervisor or security manager, any appropriately-cleared AFOTEC member is authorized to reproduce Secret and Confidential material using equipment identified as being approved for classified reproduction.

4.6.2. AFOTEC personnel may **not** reproduce (including facsimile transmission) Top Secret information without the consent of the originator or higher authority. When such approval is obtained, the TSCO will perform the reproduction and record it on the AF Form 143, **Top Secret Register Page**.

4.6.3. Persons performing classified reproduction must ensure that the file copy of the document is annotated with the number of copies reproduced and any secondary distribution.

4.6.4. After classified reproduction has been accomplished, run a sufficient number of blank sheets through the copier to clear it of possible latent images. Treat the blank sheets as classified waste and destroy in a shredder. Thoroughly check the outside and the inside of the equipment for any classified information before departing the area.

4.6.5. Information managers determine which equipment is authorized for classified reproduction. The following criteria should be used when determining which equipment shall be authorized to reproduce classified information:

4.6.5.1. Equipment should be located in a room or area where access to classified information being reproduced can be controlled, such as by a locked door.

4.6.5.2. Equipment that leaves any visible image on a blank sheet of paper run through the equipment immediately after reproducing a printed document should not be approved.

4.6.5.3. Access to the equipment during non-duty hours should be prevented. This can be accomplished by denying access to the room or area in which the equipment is located, by removing and securing the toner cartridge at the end of the day, by hard-wiring the equipment into a key-controlled power outlet switch and securing the key at the end of the day, or by several other methods. Contact HQ AFOTEC/SF if necessary.

4.7. **Disposal and Destruction of Classified Material:**

4.7.1. Appropriately-cleared AFOTEC personnel may destroy Secret and Confidential paper products using AFOTEC paper shredders identified as approved for the destruction of classified information. Contact your Security Manager or HQ AFOTEC/SF to destroy magnetic media.

4.7.2. Destruction of Confidential. No destruction certificate is required for destroying Confidential information. One cleared AFOTEC member may destroy Confidential material using an approved shredder or disintegrator.

4.7.3. Destruction of Secret. Except for NATO Secret, no destruction certificate is required for destroying Secret information. One cleared AFOTEC member may destroy Secret material using an approved shredder or disintegrator.

4.7.4. Destruction of Top Secret. Only TSCOs may destroy Top Secret material. Two (2) people with Top Secret access must be involved in the destruction process, and the AF Form 143, AF Form 310, or AF Form 1565, **Entry, Receipt and Destruction Certificate**, shall be used to record the destruction.

4.7.5. Annual Classified Clean-out Day. The last Friday in September is designated as “*Annual Classified Clean-out Day*” within AFOTEC. The focus of this event will be on the disposal of all Directorate, Detachment and Operating Location classified material that is obsolete or unneeded. All holders of classified material will participate in this event. (NOTE: Any and all classified material that is of historical value to AFOTEC, the USAF, or DoD OT&E will be forwarded to AFOTEC/HOD, ATTN: Mr Lucious Coats (DSN 246-2579), for review and inclusion in the USAF OT&E Historical Records Depository. Refer to AFOTECI 84-101, *Requirements for OT&E Program Case Files and Other Historical Information*, for a listing of significant historical documents.)

4.7.6. To destroy large amounts of classified material, HQ AFOTEC personnel may schedule use of the Kirtland AFB Destruction Facility (located in Bldg. 20404, Wyoming Blvd. at M Street) by calling 846-7760. Classified documents and certain non-paper products (plastic sheets, ribbons, floppy disks, video and audio tapes, etc) may be destroyed in this equipment provided all metal is removed from the items. Det/OL personnel contact their host base to make arrangement to destroy large amounts of classified.

5. TRANSMISSION OF CLASSIFIED INFORMATION.

5.1. **Top Secret.** Only TSCOs may transmit Top Secret material to other locations within the CONUS. AFOTEC TSCOs will use the Defense Courier Service (DCS) to transmit Top Secret material.

5.2. **Secret.** Material classified at the Secret level will be transmitted only by the following means:

5.2.1. United States Postal Service (USPS) Registered Mail.

5.2.2. USPS Express Mail. (NOTE: Use of street-side collection boxes is prohibited.)

5.2.3. The current holder of the GSA contract for overnight delivery of classified information. Federal Express (FedEx) is the current GSA contract holder. (NOTE: There are limitations and special procedures in effect on using FedEx, so check with the AFOTEC Mailroom or HQ AFOTEC/SF before using FedEx.) Since FedEx may be used to transmit Secret and Confidential material to AFOTEC, all FedEx mail must be protected as if it contains classified information until opened and a determination made otherwise.

5.2.4. Protective Security Service (PSS). Use for Secret hardware that cannot be sent by other approved means. Check with the Military Traffic Management Command for authorized commercial carriers providing PSS.

5.2.5. Approved electronic system. If necessary, contact HQ AFOTEC/SF or Det/OL Security Manager for approved equipment.

5.2.6. Authorized courier. See paragraph 5.7., below.

5.3. **Confidential.** Material classified at the Confidential level will be transmitted only by the following means:

5.3.1. Any means approved for Secret material.

5.3.2. USPS Certified Mail.

5.3.3. Constant Surveillance Service (CSS). Use for Confidential hardware that cannot be sent by other approved means. Check with the Military Traffic Management Command for authorized carriers providing CSS.

5.3.4. USPS First Class Mail. May be used **only** to send Confidential to other DoD activities within the CONUS. May **not** be used to send Confidential to contractors or non-DoD agencies. Mark the outer envelope "RETURN SERVICE REQUESTED." Since first class mail may be used to transmit Confidential material to AFOTEC, all first class mail bearing the notation "RETURN SERVICE REQUESTED" or "POSTMASTER – DO NOT FORWARD" must be protected until it has been opened and a determination made otherwise.

5.4. Classified material transmitted outside AFOTEC must be double-wrapped using substantial, opaque materials. FedEx containers may be used as outside container when transmitting via FedEx. The inner wrapping only is stamped with the highest classification of the contents. Enclose an AF 310 and suspense return of the signed receipt for no more than 30 days. Initiate tracer action if the receipt is not returned within 30 days. If the tracer action does not produce a signed receipt within an additional 30 days, request your Security Manager initiate security incident procedures.

5.5. The HQ AFOTEC Mailroom, located in Bldg. 20202, receives all outgoing USPS Registered and Certified Mail, as well as all FedEx packages from AFOTEC personnel. Mailroom personnel will take custody of all such mail/packages and ensure proper transfer to either the Base Information Transfer Center (BITC) or FedEx personnel.

5.6. OPRs submitting classified reports from locations geographically separated from Kirtland will provide the HQ AFOTEC Mailroom a distribution listing when the report is mailed for signature. The HQ AFOTEC Mailroom is responsible for distributing these reports, to include preparation and tracking of the AF 310.

5.7. Hand-carrying Classified Material:

5.7.1. Hand-carrying of classified information, especially aboard commercial aircraft, is highly discouraged, and should only be used as an absolute last resort to meet mission requirements.

5.7.2. Only AFOTEC personnel who are officially authorized as DoD couriers may hand-carry classified material from AFOTEC to another location. Contractor personnel may hand-carry classified material from an AFOTEC facility only if they have been designated as a courier and briefed by their Facility Security Officer. To be eligible for courier authorization, an AFOTEC member shall (a) possess an appropriate security clearance; (b) be designated by a Commander, Director, Program Manager, Project Leader, or Security Manager to hand-carry classified material in connection with an AFOTEC program or project; (c) receive a courier briefing and sign a briefing statement; and (d) be issued a DD Form 2501, and/or courier authorization letter, by HQ AFOTEC/SF or Det/OL Security Manager.

5.7.3. If the courier's travel will involve use of a commercial airline, the courier's security manager or HQ AFOTEC/SF will prepare a trip-specific Courier Authorization Letter. The purpose of this letter is to facilitate the courier's passage through airport/airline security checkpoints. A sample Courier Authorization Letter is available on the Security Homepage on the AFOTEC MIN.

5.7.4. Before departing AFOTEC, the courier shall provide to his/her Security Manager a listing of all classified material being hand-carried. Upon return, courier must provide a copy of signed AF 310 for material that is not returned.

5.7.5. While en route, the courier shall keep the classified material in his or her personal possession at all times. The courier may not remove the classified material from its package or container under any circumstances. If overnight storage of the material is necessary, the package or container must be stored in a GSA approved safe or vault at a U.S. military installation, Federal Bureau of Investigation (FBI) office, Defense Security Service (DSS) office, or a cleared contractor facility DSS-certified for safeguarding capability at the level of information being transported. If leaving the classified material at the destination, the courier shall obtain a signed receipt for the material.

5.7.6. The courier shall immediately report any loss or theft of classified material to the nearest FBI, Office of Special Investigations (OSI), or DSS office. HQ AFOTEC/SF will also be notified at the earliest opportunity.

6. LOSS OR COMPROMISE OF CLASSIFIED INFORMATION.

6.1. Anyone who has reason to believe that a loss, compromise, or unauthorized disclosure of classified information may have occurred must report it without delay to his or her supervisor, Dir/Det CC, or Security Manager, who in turn will report the information to HQ AFOTEC/SF by the end of the work day on which it occurred or ASAP. Keep all items related to the incident (mailing wrappers, boxes, signed receipts, safe check records, etc) until completion of the investigation.

6.2. HQ AFOTEC/SF will arrange for an official investigation of the incident by a member of a Directorate, Detachment, or Operating Location other than the one involved in the loss, compromise, or unauthorized disclosure of classified information. HQ AFOTEC/CV will issue this individual an official appointment letter. Det CC issues official appointment letter at their locations.

6.3. HQ AFOTEC/SF, or in the case of remote Detachments/Operating Locations the Security Manager, shall brief and provide instructional material to the person appointed to conduct the investigation before any actions are initiated. The Investigating Official must complete the investigation within thirty (30) duty days from the date of appointment.

6.4. The Investigating Official may seek guidance from the AFOTEC Legal Counsel before, during, or after the investigation.

6.5. HQ AFOTEC/SF will report information developed during an investigation that concerns any foreign intelligence activity or criminal activity to OSI and HQ USAF/XOFI. In addition, HQ USAF/XOFI must be notified if the loss or compromise involves NATO, Restricted Data, Formerly Restricted Data, foreign government classified information, or classified information in the public media.

6.6. Dets/OLs forward a copy of all incident reports to HQ AFOTEC/SF upon completion.

7. NATO CLASSIFIED INFORMATION.

7.1. Operational test and evaluation efforts by AFOTEC may require access to NATO classified information. AFOTEC/RMSI is designated as the focal point for NATO classified information within HQ AFOTEC.

7.2. Access to NATO classified information will be approved at the Director level and recorded on AF Form 2583. NATO security briefings and debriefings will be accomplished and records maintained by HQ AFOTEC/SF. A listing of NATO briefed personnel will be provided to HQ AFOTEC/RMSI to ensure that incoming NATO documents are distributed only to authorized personnel.

7.3. HQ AFOTEC/RMSI is responsible for receiving, distributing, and transmitting NATO classified material for all HQ AFOTEC Directorates and Detachments. Accordingly, all incoming and outgoing NATO classified documents shall be routed through HQ AFOTEC/RMSI. HQ AFOTEC/SF will provide assistance on marking and safeguarding NATO classified information.

7.4. NATO Secret and Confidential documents may be stored in a security container that stores non-NATO documents, provided the NATO material is physically separated from the non-NATO material. Use file dividers, accordion folders, or separate drawers to satisfy this requirement. Only NATO cleared individuals shall have access to the combinations to these security containers.

FELIX DUPRÉ, Major General, USAF
Commander

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

DoD 5200.1-R, *Information Security Program Regulation*

DoD 5200.2-R, *Personnel Security Program Regulation*

AFI 31-401, *Information Security Program Management*

AFI 31-501, *Personnel Security Program Management*

Attachment 2

HQ AFOTEC EMERGENCY PROTECTION/REMOVAL OF CLASSIFIED MATERIAL PLAN

A2.1. PURPOSE: IAW DoD 5200.1-R, these instructions will be used for the emergency protection or removal of classified material in the event of a natural disaster or civil disturbance. A copy of this instruction will be posted on or near security containers in each area where classified information is stored or processed.

A2.2. SITUATION: HQ AFOTEC and Dets/OLs may be threatened by severe weather conditions such as tornadoes, hail storms and flash floods. The possibility of fire always exists. Civil disturbances may consist of small groups of dissidents to large-scale riots. In any of these cases, classified material becomes vulnerable to compromise due to loss or theft and requires additional protection.

A2.3. EXECUTION:

A2.3.1. Emergency Protection.

A2.3.1.1. Fire. If time permits, before evacuation of an area, secure classified material in a vault or safe within the immediate area. Personnel will not, however, risk injury or loss of life to secure classified material. If classified material cannot be properly stored, personnel will evacuate the area to the limits established by emergency response forces. If this occurs, place the material in or on a desk, or if possible, hand-carry the information out of the area. Personnel will notify the primary or alternate Security Manager of any classified left unsecured at the time of evacuation. The Security Manager will alert police and fire personnel of unsecured classified and its location. Immediately after the emergency and authorized by emergency response forces, personnel will return to their area and check for unsecured classified material. If material is missing or inadvertent access or compromise is suspected, the Security Manager will comply with DoD 5200.1-R, Chapter 6. Emergency response forces will be debriefed if necessary after the situation is terminated.

A2.3.1.2. Natural Disasters. When no warning of severe weather is received, secure classified as prescribed in the paragraph above. If advance warning is received, individual Commanders should plan for increased security of classified material before the disturbance occurs. Classified tests conducted in open areas and handcarrying of classified documents should be suspended. Classified should be maintained within the work area until termination of the incident.

A2.3.2. Emergency Removal. If intelligence sources reveal a terrorist attack is imminent, emergency removal of classified from AFOTEC facilities will be ordered by HQ AFOTEC/CC or Det/OL CC. To ensure the most important and sensitive materials are evacuated/destroyed, the following priorities are assigned:

A2.3.2.1. PRIORITY ONE. All cryptographic keying material including Crypto Ignition Keys (CIK) encrypted for TOP SECRET, TOP SECRET SCI, TOP SECRET SAR, and TOP SECRET collateral material.

A2.3.2.2. PRIORITY TWO. CIKS encrypted for SECRET information, SECRET SCI, SECRET SAR, and SECRET collateral material.

A2.3.2.3. PRIORITY THREE: CONFIDENTIAL SCI, CONFIDENTIAL SAR, AND CONFIDENTIAL collateral material.