

**BY ORDER OF THE COMMANDER,
374TH AIRLIFT WING**



AIR FORCE INSTRUCTION 31-401

374TH AIRLIFT WING COMMAND

Supplement 1

18 NOVEMBER 2002

Security

**INFORMATION SECURITY PROGRAM
MANAGEMENT**

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: 374 SFS/SFAI (Mr. R. R. Bass, Jr.)
Supersedes AFI 31-401/374 AWSUP1,
9 March 2001

Certified by: 374 MSG/CC (Col M. A. Correll)
Pages: 16
Distribution: F

This supplement implements AFI 31-401, *Information Security Program Management*, and applies to all assigned, attached, and tenant units and staff agencies on Yokota Air Base (AB).

SUMMARY OF REVISIONS

Changes local requirements for aircraft commander, owner, or user to control entry to aircraft with classified material aboard, only if storage standards outlined in AFI 31-401, paragraph 5.16 cannot be met (**5.16.2.4. (Added)**). Changes local requirements which specifies risk analysis for facilities approved for open storage of top secret information or material, be conducted by members of 374th Security Forces Squadron (374 SFS), Air Force Office of Special Investigation (AFOSI), 374th Communications Squadron Communications Security (COMSEC) (374 CS/SCBS), and 374 Operations Support Squadron Intelligence Flight (374 OSS/OSN) to determine if supplemental controls are needed (paragraph **5.20.6.**). Changes local requirements which specifies additional response requirements for Phase I, Emergency Protection of Classified Procedures; (1) specifies additional agencies required to respond; (2) immediate inspection of vaults, secure rooms, and safes damaged as a result of the incident; (3) immediate relocation and destruction of classified information or material which was partially destroyed as a result of the incident; (4) debriefing of uncleared personnel who inadvertently viewed classified information or material while responding to the incident (paragraph A8.3.1.1. [Added]). All references to the classified information destruction facilities, Structures 1306 and 4120, have been deleted from this instruction. The classified information destruction facilities are no longer available for use. New or revised material is indicated by an (|).

AFI 31-401, 1 November 2001, is supplemented as follows:

1.3.5.4. (Added) Unit commanders or staff agency chiefs will appoint a primary and alternate unit security manager in writing.

1.3.6.9. See AFI 31-401/PACAFSUP1, paragraphs **1.3.6.9.**-1.3.6.11 for reference. Unit security managers will:

1.3.6.9.1. (Added) Monitor unit or staff agency personnel security clearances and assist unit personnel with updating security clearances.

1.3.6.9.2. (Added) Manage unit or staff agency security education and training.

1.3.6.9.3. (Added) Advise the unit commander or staff agency chief on the continuous evaluation program or derogatory information concerning unit personnel.

1.3.6.9.4. (Added) Review all original and derivative classified information generated by the unit or staff agency to ensure requirements outlined in DoD 5200.1-R, *Information Security Program*, Chapter 2 and 3, and DoD 5200.1-PH, *DoD Guide to Making Classified Documents*, were followed.

1.3.8.1. (Added) The 605th Air Intelligence Squadron Intelligence Special Security Office (605 AIS/INS) is the base point of contact (POC) for all Sensitive Compartmented Information (SCI) related matters.

1.4.2.1. (Added) The 374 SFS Information Security Office (374 SFS/SFAI) will conduct annual Information Security Program Reviews on all non-exempt agencies.

1.4.2.1.1. (Added) Program reviews are examinations of a unit's Information, Personnel, and Industrial Security Programs. Program reviews are not "compliance inspections" and they are not rated. Instead, they are "assistance" oriented visits to identify noteworthy and problem areas in the security program of the activity visited. The Information Security Program Manager (ISPM) may use a random sampling method, but the examination will be extensive enough to determine overall status of unit programs.

1.4.2.2. (Added) Unit commanders and staff agency chiefs review program review reports and, when necessary, take appropriate corrective action on problem areas identified in the report. Replies to program review reports are not generally required, however, unsatisfactory reports and corrective actions taken to remedy serious management deficiencies will be documented and reported to the 374 Airlift Wing Commander (374 AW/CC).

1.4.3.2. (Added) Unit commanders or staff agency chiefs will appoint, in writing, an individual to conduct the unit semiannual self-inspection. Security managers will not inspect their own programs but will monitor and assist as necessary. Cross inspections which permit one unit security manager to inspect another are encouraged. The inspection of each element of the security program may be made on the basis of random sampling, but the inspection must be extensive enough to show compliance with required security directives. Program reviews, as described in paragraph **1.4.2.1. (Added)** of this supplement, may substitute for the next semiannual inspection. The person conducting the inspection will send a written report of findings to the unit commander or staff agency chief who reviews it to determine adequacy of the inspection and specifies the corrective actions to be taken. Unit Security Managers are required to maintain copies of the last two inspection reports. Use the format at **Attachment 14 (Added)** of this supplement to complete the self-inspection report.

5.4.1.5. (Added) 374 SFS/SFAI can also be contacted to verify security clearances.

5.10.1.1.1. Units or agencies having a need to store top secret material must contact 374 SFS/SFAI prior to, or immediately after receiving the information. 374 SFS/SFAI will train all Top Secret Control Officers (TSCO).

5.10.1.3.4. (Added) Annual inventories or audits of all top secret material will be conducted during the month of January, or whenever the TSCO changes.

5.12.1. (Added) End of day security checks will include all areas of an office or building where classified information is stored or may have been handled. Holders of classified information, with assistance from the unit security manager, will develop a system of end-of-day security checks, and document the checks on the SF Form 701, **Activity Security Checklist**. The “Checked By” block of the SF Form 702, **Security Container Check Sheet**, will be initialed to verify the security container was checked as part of the end-of-day security check.

5.14.3. (Added) The in-transit storage repositories for transient classified material are the 374th Operations Support Squadron Base Operations (374 OSS/OSAM) (Bldg 703), the 374 AW Command Post (374 AW/CP) (Bldg 315), and the United States Forces, Japan, Joint Operations Center (USFJ/J34) (Bldg 714). If the transient classified material is too large for these places, it may be stored at the 730th Air Mobility Squadron Special Handling (730 AMS/TRK) (Bldg 79). As a last resort, it may be stored at the Defense Courier Service Station-Yokota (DCSS-YO) (Bldg 97) if it meets the criteria in the Defense Courier Service Manual.

5.15.1.1. (Added) Units or agencies that hold classified meetings will:

5.15.1.1.1. (Added) Develop procedures to ensure all protection requirements outlined in DoD 5200.1-R, paragraph 6-307, and other classified protection requirements are met.

5.15.1.1.2. (Added) The unit or agency conducting the meeting, with assistance from that unit and agency’s security manager, will ensure all classified information is properly protected prior to, during, and after the meeting. Actions to protect classified information during meetings include, but are not limited to the following:

5.15.1.1.2.1. (Added) Limiting access into the room, locking doors, posting personnel outside of briefing location to restrict access, closing curtains, etc.

5.15.1.1.2.2. (Added) Verifying clearances of all personnel in attendance.

5.15.1.1.2.3. (Added) Properly storing, transporting, accounting for, and returning all classified information to approved storage containers.

5.15.1.1.2.4. (Added) Conducting a thorough check of the meeting location after the meeting to ensure no classified information is left behind.

5.15.1.1.3. (Added) Unit or agencies that hold classified meetings infrequently will, with assistance from the security manager, assess the construction of the room to ensure the room poses no risks of compromise of classified information during meetings.

5.15.1.1.4. (Added) Units or agencies that hold classified meetings more than once a week in the same location must contact 374 SFS/SFAI. 374 SFS/SFAI will assess the location, and provide technical assistance as needed.

5.16.2.4. (Added) The aircraft will be parked in the mass parking restricted area if parking is available, demarcated with an elevated barrier, and all classified material will be stored as outlined in AFI 31-401, paragraph 5.16. If standards outlined in AFI 31-401, paragraph 5.16 cannot be met, the aircraft commander, owner, or user will provide entry control to the aircraft. The aircraft commander and/or an on-duty security forces representative will contact the 374 SFS/SFAI to ensure the classified on-board the aircraft is being properly stored.

5.16.2.5. (Added) Units or agencies deploying to foreign locations where there are no approved classified storage facilities, or where no cleared United States Air Force personnel are permanently stationed, will follow guidance outlined in AFI 31-401, paragraph 5.16.4, or contact 374 SFS/SFAI for further guidance.

5.17.4. (Added) The Defense Automated Printing Service (DAPS) on Yokota AB will be contacted prior to reproducing classified information on copier machines. DAPS will determine if the copier machine retains latent images, or poses any other risks to classified information. If not, the copier machine may be used for reproduction of classified information.

5.17.5. (Added) Unit security managers will post unit developed notices on all unit copier machines, stating they are or are not authorized for reproduction of classified information. The notice will be posted and written to easily alert the user if the copier machines has or has not been approved for reproduction of classified information.

5.19.1. (Added) All security containers will be inspected by 374th Civil Engineer Squadron Locksmith (374 CES/CEORV) prior to use. Each safe will have an AFTO Form 36, **Maintenance Record for Security Type Equipment**, and SF Form 700, **Security Container Information**.

5.20.4. All classified information or material will be stored in General Services Administration (GSA) approved security containers, vaults, or secure rooms when not under physical control of a properly cleared person. See AFI 31-401/PACAFSUP1 for reference.

5.20.5. (Added) All vaults, secure rooms, or open storage locations will be inspected by 374 CES and 374 SFS/SFAI, and approved for storage by the 374 SFS Commander (374 SFS/CC). The 374 SFS/CC will base his or her decision on the following:

5.20.5.1. (Added) The structure's physical construction that meets requirements outlined in DoD 5200.1-R, Appendix G.

5.20.5.2. (Added) A demonstrated operational need to store classified information openly; (amount of classified information or material prevents storage in GSA approved safe, or a classified computer system must remain operational when personnel are not present, etc.).

5.20.6. (PACAF). (Added) Risk analysis will be conducted to determine the need for supplemental controls identified in AFI 31-401, paragraph 5.20.1, for all open storage approved areas storing top secret information or material. The risk analysis will be conducted by representatives from AFOSI Det 621, 374 OSS/OSN, 374 SFS/SFAI, 374 SFS Force Protection Office (374 SFS/SFOFP), and 374 CS/SCBS. Recommendations (as a result of the risk analysis) to implement or not to implement supplemental controls will be documented, and approved by 374 SFS/CC and owning unit commander or staff agency chief.

5.20.7. (PACAF). (Added) Approval letters for vaults, secure rooms, and open storage of classified information, signed by 374 SFS/CC, will be maintained by the unit security manager. See AFI 31-401/PACAFSUP1 for reference.

5.28.4. (Added) Units or agencies with classified holdings will continuously review holdings and destroy classified information that is not needed. Also, units and agencies will conduct a complete review of classified holdings during the month of January each year, and destroy classified information according to its disposition.

5.29.1.1. (Added) Routine destruction of classified information will be accomplished on shredders that produce residue particles not exceeding 1/32 inch in width by 1/2 inch in length. A notice will be posted

on all shredders, notifying users if the shredder is or is not authorized for destruction of classified information.

5.29.2.2.1. (Added) Use AF Form 143, **Top Secret Register Page**, AF Form 310, **Document Receipt and Destruction Certificate**, or AF Form 1565, **Entry, Receipt and Destruction Certificate**, if a record of destruction of secret or classified information needs to be maintained. See AFI 31-401, paragraph 5.29.2 for required documentation for destroying classified information.

5.29.3. (Added) Emergency protection, reduction, and destruction of classified information. Use the plan at **Attachment 15 (Added)** of this supplement during situations that may require emergency protection, reduction, or destruction of classified information. Each unit is responsible for developing emergency procedures that are tailored to unit needs, amount of classified information stored, etc. Use **Attachment 15 (Added)** of this supplement to develop unit level procedures.

6.3.2.1. (Added) Units or agencies will only allow personnel with security clearances to receipt for registered mail. All registered mail must be protected as classified information until opened.

6.6.3.1. (Added) Personnel hand-carrying classified documents will use an inner and outer envelope when carrying classified information, regardless of whether the information is being carried in a briefcase or other outer container. The inner envelope will be marked with the classification of the information, and the unit address. The outer envelope will be marked with the unit address only.

6.8.1. (Added) Use the DD Form 2501, **Courier Authorization**, when hand-carrying classified material outside the legal (controlled) boundaries of the installation or installation entry gates. Unit commanders or security managers are authorized to issue the DD Form 2501. Security managers must develop issue and control procedures for the DD Form 2501 and include these procedures in their Operating Instruction (OI). OIs should include, as a minimum, accountability and issue and turn-in procedures. Each issued DD Form 2501, must have a 374 AWVA 31-5, *Bilingual Attachment to DD Form 2501*, attached to its reverse to meet the requirement of the Status of Forces Agreement. Use 374 AWVA 31-6, *Bilingual Exemption Notice*, when transporting classified material off military installations. When hand-carrying classified materials on-base during increased Force Protection Conditions (FPCON) Charlie and Delta, which implement inspection points at facilities, unit's may use either the DD Form 2501 or a courier authorization letter signed by the unit's commander or security manager. During FPCON Normal, Alpha, and Bravo, no courier documentation is necessary when hand-carrying classified information to activities within the installation.

6.8.2. (Added) During emergency situations that occur during increased FPCON (e.g., relocation of unit or group control center), personnel who need to transport or relocate classified information do not need a DD Form 2501.

6.9. Unit commanders or staff agency chiefs are the approval authority for hand-carrying classified information aboard military and commercial passenger aircraft. See **Attachment 16 (Added)** of this supplement for procedures.

8.1.1. (Added) Security managers will outline in an OI the unit's security education plan. Security education will be based on unit or staff agency mission, functions of the activity, and the degree of involvement with classified material. Develop the unit's security education plan using training standards outlined in AFI 31-401, Attachment 7 (Air Force Information Security Training Standard). As a minimum, units will conduct initial and quarterly training on information security related subjects, and document training conducted. Civilian employees should also be encouraged to take part in the unit's security education program.

8.8.1.1. (Added) 374 SFS/SFAI will provide the following training:

8.8.1.1.1. (Added) Train Original Classification Authorities (OCA) of OCA duties within 30 days of appointment.

8.8.1.1.2. (Added) Train TSCO prior to, or immediately after being assigned TSCO duties.

9.3.2.4. (PACAF) (Added) 374 SFS/SFAI will assign a control number for each security incident, brief the investigating official on his or her responsibilities and provide assistance as needed, and conduct a technical review of the inquiry report.

9.3.2.5. (PACAF) (Added) Unit commanders will appoint investigating officials using the format in PAC-AFPAM 31-2, *Investigations of Actual or Potential Compromise of Classified Information*, no later than the day following the incident.

9.8.1.2. (Added) Investigating officials will contact 374 AW Staff Judge Advocate (SJA) (374 AW/JA) to receive a briefing prior to interviewing personnel involved in the incident, conduct the inquiry, and complete a report using the format in PACAFPAM 31-2.

9.11. (Added) 374 AW/JA will review security incident investigation reports prior to closing by the appointing official.

Attachment 14 (Added)

**SAMPLE SEMIANNUAL INFORMATION SECURITY
SELF-INSPECTION REPORT FORMAT**

(Date)

MEMORANDUM FOR (Inspected Unit Commander/Staff Agency Chief)
374 SFS/SFAI
IN TURN

FROM: (Inspecting Officials Rank/Name/Unit/Office Symbol)

SUBJECT: Semiannual Security Inspection

1. **AUTHORITY AND DATE OF INSPECTION:** This inspection was conducted on (date) under authority of DoD 5200.1-R, and AFI 31-401.

2. **PERSONNEL CONTACTED:** (Identify Key Personnel)

3. **INSPECTING PERSONNEL:** (Self-explanatory)

4. **SUMMARY:** (The inspection should inquire into procedures for handling and safeguarding classified material. Also, check the security education, personnel security, and industrial security programs if applicable. Inspect each element of the security program on the basis of a representative sampling, but extensive enough to evaluate practices in effect for compliance with regulatory guidance. Note any changes, improvement or otherwise, in the overall security program since the last inspection. Identify any repeat discrepancies or other conditions which could result in the loss or compromise of classified material. Ensure you utilize the self-inspection checklist provided by 374 SFS/SFAI. Results of the units' efforts during the annual classified reduction day must be recorded in this report.)

5. **FINDINGS:** (Make a comment on each element examined. List the good as well as deficient areas. Try to include a specific "Recommended Corrective Action" on noted discrepancies. Using checklists provided and following this suggested format assures you address key program areas.)

a. **Security Education:** (Is there a program, and how effective is it? Does it include as a minimum, initial and quarterly training?)

b. **Classified Document Handling and Storage:**

- (1) Classification, Declassification, and Downgrading
- (2) Marking
- (3) Retention
- (4) Safekeeping and Storage
- (5) Access, Dissemination, Transmission, and Accountability
- (6) Reproduction Controls
- (7) Disposal and Destruction

c. Security Incidents: (Have any security incidents occurred since the last inspection? If so, was appropriate action taken to prevent incidents from reoccurring?)

d. Personnel Security Program: (Do persons have the proper security clearance to perform the duty of the position they occupy? Have all personnel with a security clearance executed the SF Form 312, **Classified Nondisclosure Agreement**? Are there any personnel requiring periodic reinvestigation?)

e. Industrial Security Program: (If applicable.)

6. OTHER COMMENTS: (Enter any other information not listed above, but relates to overall management of the security program. This is a good place to recognize individual exceptional performance in following established security practices.)

(Signature Block of Inspecting Official)

1st Ind, (Commander/Staff Agency Chief)

MEMORANDUM FOR: (Unit Security Manager)

I have reviewed the inspection report and concur with the recommended corrective actions, unless otherwise noted. Please ensure discrepancies are corrected as soon as possible. Inform me of the status of any items which cannot be immediately corrected.

(Signature Block of Commander/Staff Agency Chief)

cc: Unit Security Manager

Attachment 15 (Added)**EMERGENCY PROTECTION, REDUCTION, OR DESTRUCTION
OF CLASSIFIED INFORMATION PLAN**

A15.1. (Added) SITUATION. Without warning, natural or man-made emergency situations may occur which impact the physical security of classified information or material. The risk to classified information varies according to the type and severity of an emergency. During these times, it may be necessary to better protect or destroy classified information. Contingency planning reduces the chance of highly sensitive information falling into the hands of unauthorized personnel.

A15.1.1. (Added) Threat. The threat of terrorist or dissident groups whose objectives are to destroy or damage mission essential resources are of primary concern. These people usually are fanatical and have the objective of embarrassing the United States or host governments by committing acts which gain publicity for their group or cause. Yokota AB is also vulnerable to a number of threats from natural phenomena. The primary threats are considered to be from earthquakes and typhoons.

A15.1.2. (Added) Limiting Factors.

A15.1.2.1. (Added) There may not be enough office shredders or other destruction devices to accomplish complete destruction of all classified information. When required, emergency destruction is accomplished by burning, melting, mutilating, pulverizing, or other available means.

A15.1.2.2. (Added) Relocation of all classified information to a more secure location may not be feasible. Transporting classified information from a secure location may create the risk of loss or compromise while enroute to that location. Also, there may not be enough certified vaults, or other secure storage locations to accommodate all classified information.

A15.2. (Added) MISSION. Establish procedures for emergency protection, reduction, or destruction of classified information in case of fire, natural disaster, civil disturbance, terrorist activities, or enemy action.

A15.3. (Added) EXECUTION: Emergency protection, reduction, or destruction of classified information is necessary during fires, natural disasters, or contingency operations, to maintain security and prevent possible disclosure or seizure of information which would result in damage to national security. There are three phases of execution that could be implemented separately or simultaneously.

A15.3.1. (Added) Concept of Operations. Depending on the situation, the installation commander, group commander, or commander or agency chief of the unit owning the classified information implements this plan. The particular operation employed depends on the situation. When the senior individual present in an area containing classified information determines a sufficient threat exists to initiate any of the emergency phases identified in this plan, that person must take immediate action to protect the classified information, and notify his or her chain-of-command immediately thereafter.

A15.3.1.1. (Added) Phase I, Emergency Protection Procedures. The following procedures will be initiated in the event of:

A15.3.1.1.1. (Added) Fire, natural disaster, bomb threat, or other situation in which facilities holding classified information are evacuated or damaged. Since these events generally occur without warning, execution of this phase will normally be initiated by the senior individual present in any area that maintains classified.

A15.3.1.1.1.1. (Added) Return all classified not absolutely necessary for mission accomplishment to an appropriate security container. If the situation warrants, consider moving classified holdings to a more secure area or to another facility that is staffed on a 24-hour basis.

A15.3.1.1.1.2. (Added) If necessary for personnel safety, leave classified in the work area and evacuate the facility.

A15.3.1.1.1.3. (Added) Immediately after evacuation, notify responding fire department and security forces personnel if classified was left unsecured.

A15.3.1.1.1.4. (Added) When classified is left unsecured, place authorized personnel around the affected area to prevent its removal. Maintain strict entry control and allow only responding emergency personnel to enter.

A15.3.1.1.1.5. (Added) Ensure the ISPM or a designated representative, unit security manager, and member of 5th Air Force (5 AF) Special Security Office (SSO) (if a 5AF SSO facility is involved) respond to the scene to provide expertise for control and recovery of classified information or material.

A15.3.1.1.1.6. (Added) Once the affected area has been declared safe, custodians conduct a search to recover all classified. Control entry into the affected area until all classified is recovered and secured.

A15.3.1.1.1.7. (Added) Members of the 374 SFS/SFAI, 374 CES Maintenance Engineering, (374 CES/CEOE) 374 CES/CEORV (Locksmith), and 5 AF SSO (if required) will conduct an inspection of effected classified holding areas (vaults, secure rooms, safes, etc.), to determine if they still meet structural requirements for protecting classified information/material. If classified holding areas no longer meet structural requirements, relocate classified to an approved holding area.

A15.3.1.1.1.8. (Added) Conduct debriefings on all uncleared personnel who had to enter and inadvertently viewed classified information. If a 5 AF SSO facility is involved, debriefings will be conducted in accordance with 5AF SSO guidelines.

A15.3.1.1.1.9. (Added) Completely destroy any remaining classified that was partially destroyed during the incident.

A15.3.1.2. (Added) Phase II, Emergency Reduction Procedures. This phase is normally initiated prior to serious incidents of civil disturbance or the threat of terrorist or enemy action, where prior warning is received giving sufficient time to implement this phase. In the absence of an order by an appropriate commander, the senior individual present may make the determination to initiate this phase. The following procedures apply:

A15.3.1.2.1. (Added) Units will identify what classified information in their possession is or is not absolutely essential for mission accomplishment. As a general rule, classified information not absolutely essential for mission accomplishment includes; copies of classified plans, information, or material to which the original document, or another copy, exists at another unit, base, or higher headquarters, or plans, information, or material that is not required to be on hand to perform a certain mission.

A15.3.1.2.2. (Added) Destroy all non-mission essential classified information using the following methods:

A15.3.1.2.2.1. (Added) Use routine destruction equipment within the unit (e.g., classified shredders).

A15.3.1.2.2.2. (Added) For mass quantities of classified information, the base incinerator (Bldg 1526) may be used if unit shredders are not available or inadequate. Units must provide enough personnel to monitor burning of their classified when the base incinerator is used.

A15.3.1.2.3. (Added) Holders of classified information, or a person designated by the unit commander will ensure the unit's classified information is destroyed.

A15.3.1.2.4. (Added) Prepare mission essential classified information for evacuation, in accordance with (IAW) **Attachment 16 (Added)** of this supplement.

A15.3.1.3. (Added) Phase III, Emergency Destruction Procedures. This phase is executed when an imminent threat exists that the installation may be overrun or lost to an attacking enemy. Under these conditions, destruction of classified must begin early enough to preclude loss or compromise. The effect of premature destruction is considered inconsequential when measured against the possibility of loss or compromise of the information or material. In the absence of an order by the implementing authority, the senior individual present may make a common sense determination to begin emergency destruction.

A15.3.1.3.1. (Added) Destroy the classified information using unit shredders or any means possible by shredding, burning, pulping, melting, mutilating, or pulverizing. Ensure classified information can not be reconstructed after destruction.

A15.3.1.3.2. (Added) If the installation is being evacuated, units will, if needed, hand-carry mission-essential classified information with them as they deploy. Each unit will be responsible for destroying, or transporting their classified. If personnel are not deploying from or evacuating the installation, destroy all mission-essential classified information if there is the risk of compromise.

A15.3.1.3.3. (Added) Maintain a listing of destroyed material by documenting AF Form 310. Also provide 374 CS Record Management (374 CS/SCBR) information on all classified destroyed.

A15.4. (Added) Task Organizations:

A15.4.1. (Added) The 374 AW/CC or senior 374 AW Battle Staff or Survival Recovery Center (SRC) member. Implements this plan through a wing recall, or through implementation of battle staff directives to group and unit control centers.

A15.4.2. (Added) 374 SFS/SFAI coordinates security matters and provides technical guidance to all base organizations.

A15.4.3. (Added) The 374 CES Commander (374 CES/CC) will:

A15.4.3.1. (Added) Provide advice to units when developing destruction plans involving burning of classified material.

A15.4.3.2. (Added) Arrange to have Bldg 1526 opened during phase II, if needed.

A15.4.4. (Added) The 374 CS Commander (374 CS/CC) will:

A15.4.4.1. (Added) Provide technical advice concerning emergency procedures for classified computer systems.

A15.4.5. (Added) 374 CS/SCBR will:

A15.4.5.1. (Added) Notify Headquarter Pacific Air Forces Record Management Section (HQ PACAF/SCXPR) of the emergency destruction of records as soon as possible after destruction begins.

A15.4.6. (Added) All units or staff agencies storing classified will:

A15.4.6.1. (Added) Continuously reduce and maintain classified holding to the absolute minimum.

A15.4.6.2. (Added) Identify all mission-essential classified information, and maintain sufficient equipment to prepare it for evacuation if needed.

A15.4.6.3. (Added) Develop emergency destruction kits in the event other means for destruction are not available, or time does not allow use of shredders or destruction facilities.

A15.4.6.4. (Added) Report the following information to 374 CS/SCBR, IAW AFI 37-138, *Records Disposition-Procedures and Responsibilities*, as soon as possible:

A15.4.6.4.1. (Added) The name of your organization.

A15.4.6.4.2. (Added) A general description of the records destroyed.

A15.4.6.4.3. (Added) The security classification.

A15.4.6.4.4. (Added) The dates of each file.

A15.4.6.4.5. (Added) The place and date of destruction.

A15.4.6.4.6. (Added) The reason for destruction.

A15.5. (Added) COORDINATING INSTRUCTIONS. All units or staff agencies storing classified material will develop implementing instructions, and coordinate all implementing instructions with 374 SFS/SFAI. Implementing instructions must address actions for all three phases of this plan.

A15.6. (Added) ADMINISTRATION AND LOGISTICS. Sufficient personnel, supplies, and equipment are readily available to support this plan's operations. Shortfalls are noted as needed.

A15.7. (Added) COMMAND AND SIGNAL:

A15.7.1. (Added) The installation commander exercises authority over all aspects of this plan. In his or her absence, the normal succession of command authority will be followed.

A15.7.2. (Added) Unit commanders and staff agency chiefs must protect all classified information under their jurisdiction, administration, custody, or control, according to procedures in this plan.

Attachment 16 (Added)**HAND-CARRYING CLASSIFIED MATERIAL ABOARD MILITARY AND COMMERCIAL AIRCRAFT**

A16.1. (Added) Purpose. To establish procedures for hand-carrying classified material on military and commercial aircraft. This includes packaging, marking, and safeguarding procedures.

A16.2. (Added) Responsibilities. Commanders, supervisors, and users of classified material are responsible for the safeguarding of classified material. 374 SFS provide technical advice to units deploying with classified material.

A16.3. (Added) Classified material should be hand-carried between locations only when other means of transmission or transportation cannot be used. Commanders must base decisions to hand-carry classified material on the following:

A16.3.1. (Added) The information is not available at the destination and is required by operational necessity.

A16.3.2. (Added) The information cannot be sent via a secure facsimile, registered mail, or by other secure means.

A16.4. (Added) Procedures. When classified material must be hand-carried to a deployment or temporary duty (TDY) location on military or commercial aircraft, unit commanders will ensure the following is accomplished prior to departure of the courier:

A16.4.1. (Added) Appoint appropriately cleared deploying unit personnel as couriers for top secret, secret, and confidential material as defined in AFI 31-401. Final selection is based on demonstrated stability, reliability, maturity, and judgment. Issue the courier an unclassified official courier letter (see example below), and a DD Form 2501 (maintained by unit security manager) along with 374 AWVA 31-5, as outlined in paragraph **6.8.1. (Added)** above. Commanders will ensure couriers are thoroughly familiar with their responsibilities prior to assigning them courier duties.

A16.4.2. (Added) Classified couriers and cargo couriers can be one and the same, as long as other duties do not impede the ability of the classified courier to protect the classified material.

A16.4.3. (Added) Arrange to have the classified material hand-carried aboard the aircraft by coordinating with the aircraft commander or airline agency. Avoid hand-carrying classified material aboard commercial aircraft if possible.

A16.4.4. (Added) Unit security managers, TSCOs, or other designated personnel will brief couriers on their responsibilities. Conduct the briefing using DoD 5200.1-R, paragraphs 7-300 b, (1)-(8), and any other applicable information security items outlined in AFI 31-401, and AFI 31-401/PACAFSUP1. The courier acknowledges awareness of their responsibilities by signing the DD Form 2501.

A16.4.5. (Added) Prior to the courier departing, the unit security manager will coordinate all documents with the 374 SFS/SFAI to ensure the courier letter and DD Form 2501 are all in order.

A16.4.6. (Added) Classified custodians, TSCOs, and other personnel responsible for accounting for the classified material will prepare two inventory lists of all classified material being hand-carried. One copy of the inventory will remain with the classified material being transported. The second copy will be maintained at the originating location until all classified material has been returned. The unit security manager, TSCO, or other responsible personnel will maintain the inventory.

A16.4.7. (Added) Use AF Form 310 as needed, or when the person transporting the classified material must relinquish it to another person.

A16.4.8. (Added) Use AF Form 12, **Accountable Container Receipt**, when the material will be placed in sealed containers.

A16.4.9. (Added) TSCOs will use AF Form 143 as needed.

A16.4.10. (Added) Packaging and Marking:

A16.4.10.1. (Added) As a general rule, classified material shall be enclosed in two opaque, sealed envelopes, wrappings, or containers, durable enough to properly protect the material from accidental exposure and facilitate detection of tampering. The inner wrapper will display the address of the receiving activity or the name of the unit to which the person hand-carrying the material is assigned to (if the material will not be turned over to another unit), the address of the sending unit (if different from receiving activity), the highest classification of the contents, and any applicable caveats or special instructions. Ensure the classified material cannot be viewed or read by looking through the inner wrapper.

A16.4.10.2. (Added) The outer wrapper will display the address of the receiving activity (or unit to which person hand-carrying the material is assigned to if the material will not be turned over to another unit), and will be signed by the official who signed the courier letter. The outer wrapper will display the following information:

Department of the Air Force

374 AW

(374 unit)

Yokota AB Japan 96326-5500

Official Business

MATERIAL EXEMPTED FROM EXAMINATION

ROBERT A. DOE, Colonel, USAF

(Unit)

A16.4.10.3. (Added) The outer wrapper will NOT bear a classification marking or any other unusual marks that might invite special attention to the fact that the contents are classified.

A16.4.10.4. (Added) For guidance on bulk classified items, see paragraph [A16.4.11.2. \(Added\)](#) below, or refer to DoD 5200.1-R, Chapter 7, or contact 374 SFS/SFAI.

A16.4.10.5. (Added) All material should be sealed in the presence of the responsible officer who signs the courier letter or outer wrapper.

A16.4.10.6. (Added) Ensure arrangements are made to have the classified material properly stored upon arrival at the deployment location. See paragraph [A16.4.11.3. \(Added\)](#) below, or contact the unit security manager or 374 SFS to determine storage requirements.

A16.4.11. (Added) General Courier Responsibilities. The courier is responsible for safeguarding the classified material while hand-carrying to the deployment location, and upon arrival at the deployment location until the material is properly secured. The courier will release the material only to individuals who have an absolute need-to-know, and who have been granted a security clearance and access authorization at the required level.

A16.4.11.1. (Added) Couriers will ensure envelopes and other classified containers that are shipped as hand-carried baggage remain immediately accessible and in constant view of the courier.

A16.4.11.2. (Added) Place bulk classified items, or other classified items not being shipped as hand-carried baggage in either a compartment on the aircraft that is not accessible to any unauthorized persons, or in a specialized, safe-like container. Couriers must observe these classified items while they are being loaded on and off the aircraft.

A16.4.11.3. (Added) Couriers will ensure the classified material is stored in authorized GSA approved safes, vaults, or secure rooms, immediately upon arrival at the deployment location.

A16.4.11.4. (Added) Upon completion of the deployment, destroy the classified material using approved means if original copies of the material are maintained at the home unit, or arrange to have the classified material mailed (secret and confidential only) if possible. Hand-carry the classified material back to the home unit as a last resort. Follow all procedures listed above when returning classified to home unit.

A16.4.11.5. (Added) If classified material is destroyed at the deployment location, use AF Form 143 (for top secret) or AF Form 310 to document the destruction.

A16.4.11.6. (Added) Prior to mailing secret or confidential material, or destroying any classified material, contact the unit security manager or 374 SFS for guidance.

A16.4.12. (Added) Emergency Protection Procedures. In the event of disaster or enemy action where classified material faces the risk of loss or compromise, attempt to secure the classified in a safe, vault, or secure room at another Department of Defense installation, or destroy the material by burning, shredding, or other means that renders the material unreadable. Couriers must apply common sense and best judgment in these situations to protect the classified material as best as the situation allows.

OFFICIAL COURIER APPOINTMENT LETTER

(Letterhead Stationary)

MEMORANDUM FOR

FROM:

SUBJECT: Authorization to Hand-carry Sealed Package

1. (Grade, name, organization, address) is designated an official courier for the United States Government. He/She will be traveling aboard _____ Airlines departing _____ on _____ and will arrive at _____ on _____.
2. Upon request, (he/she) will present his/her official identification card, a DD Form 2, bearing the number _____.
3. (Grade, name) is hand-carrying three sealed packages, sized 9" x 8" x 24" addressed from (organization, office symbol, location, ZIP code) and addressed to (organization, office symbol, location, ZIP code). Each package is identified by the marking "OFFICIAL BUSINESS-MATERIAL EXEMPTED FROM EXAMINATION", and bearing the signature of the undersigned. The packages are not to be opened or removed from (his/her) possession.
4. (Grade, name) is departing (location) with a final destination to (location). He/She has a transfer point at (location).
5. This courier designation can be confirmed by contacting me at (organization, commercial phone, and defense switched network [DSN] phone). This letter expires on (date).

(Commander's Signature Block)

MARK E. STEARNS, Colonel, USAF
Commander