BY ORDER OF THE
932D AIRLIFT WING COMMANDER

932D AIRLIFT WING INSTRUCTION
16-1404

9 JULY 2020

Security

GENERAL RESPONSIBILITIES OF THE SECURITY MANAGERS

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

ACCESSIBILITY: Publications and forms are available for downloading or ordering on the e-Publishing web site at **www.e-Publishing.af.mil**

RELEASABILITY: There are no releasability restrictions on this publication

---

OPR: 932 SFS/SM

Certified by: 932 MSG/CC
(Colonel Lance F. Turner)

Pages: 15

This Airlift Wing Instruction (AWI) implements Air Force Policy Directive (AFPD) 31-4, *Information Security*. This instruction extends the guidance of Air Force Instruction (AFI) 16-1404, *Information Security Program Management (ISPM)*. It outlines responsibilities and procedures for 932d Airlift Wing Security Managers. It applies to all 932 AW Security Managers. Ensure that all records created as a result of processes prescribed in this publication are maintained IAW Air Force Manual (AFMAN) 33-363, *Management of Records*, and disposed of IAW Air Force Records Information Management System (AFRIMS) Records Disposition Schedule (RDS). Refer recommended changes and questions about this publication to the Office of Primary Responsibility (OPR) using the AF Form 847, *Recommendation for Change of Publication*; route AF Forms 847 from the field through the appropriate functional chain of command. This publication may not be supplemented or further implemented/extended. The authorities to waive wing/unit level requirements in this publication are identified with a Tier ("T-0, T-1, T-2, T-3") number following the compliance statement. See AFI 33-360, *Publications and Forms Management*, for a description of the authorities associated with the Tier numbers. Submit requests for waivers through the chain of command to the appropriate Tier waiver approval authority, or alternately, to the Publication OPR for non-tiered compliance items. The use of the name or mark of any specific manufacturer, commercial product, commodity, or service in this publication does not imply endorsement by the Air Force.

1. ROLES AND RESPONSIBILITIES.

1.1. **Commanders Shall.**

1.1.1. Appoint the Unit Security Manager and establish the training requirements. As a minimum, the unit security manager is trained by the 375th Air Mobility Wing Information Protection (AMW/IP) office within 120 days of appointment. They will provide each Security Manager with a letter of completion.

1.1.2. Appoint Safe and Secure Room Custodians for any GSA certified storage containers within their facilities.

1.1.3. Attend quarterly meetings and training sponsored by the ISPM office.

1.1.4. Maintain this instruction in accordance with (IAW) AFI 16-1404.

1.1.5. Review and maintain all semi-annual security self-inspection reports and security incident reports for a period of two years according to AFRIMS.

1.1.6. Provide and document security education training for all assigned unit personnel.

1.1.7. Continuously evaluate cleared personnel to ensure they continue to be trustworthy in accordance with the standards in DOD 5200.2-R, Chapter 2.

1.1.8. Determine the appropriate steps to take when information or actions occur that bring into question a person's compliance with the adjudication guidelines.

1.2. **Wing Security Manager(s) Shall.**

1.2.1. Act as liaison between the Squadron Security Managers and Wing leadership, when required.

1.2.2. Act as liaison between the Squadron Security Managers and the 375th Security Forces Squadron (SFS) and/or 375th Air Mobility Wing Information Protection (AMW/IP) office.

1.2.3. Prepare consolidated Security Manager/Safe Custodian Appointment memos for commander signature.

1.2.4. Provide updated copies of appointment memorandums to the 375 SFS and/or 375 AMW/IP when the primary/alternate Security Managers or safe custodians are appointed or changed.

1.2.5. In conjunction with the Squadron Security Managers, perform semiannual security self-assessments of the entire Security program, and ensure that Information, Personnel, and Industrial Security Programs are evaluated during these assessments.

1.2.6. Provide and track completion of security training to include Security Orientation, Derivative Classification, Marking Classified Information, Annual Refresher, North Atlantic Treaty Organization (NATO), and others, as required. NATO Indoctrination will be IAW AFI 16-1404, *Air Force Information Security Program*. Personnel that do not require access to NATO, will receive a briefing and sign a briefing certificate acknowledging responsibilities for possible inadvertent access. Any personnel who require NATO classified access will receive the NATO specific briefing on the 375 AMW/IP SharePoint site and be approved for access using the AF 2583. No NATO access will be coded without the AF 2583. Anyone new unit members who have NATO classified access will be debriefed using the AF 2587, by denoting the access removed in JPAS (or successor system).

1.2.7. Attend a minimum of two quarterly meetings and training sponsored by the 375 AMW/IP office, and meet with the CC/CA on an as needed basis to discuss requirements, policy changes, etc.

1.3. **Squadron Security Manager(s) Shall.**

1.3.1. Provide advice and assistance to the commander or staff agency chief concerning security issues.

1.3.2. Schedule annual security self-inspections. Ensure the Information and Personnel Security Programs are evaluated during annual security self-inspections

1.3.3. Attend quarterly meetings and training sponsored by the ISPM office.

1.3.4. Maintain this instruction in accordance with (IAW) AFI 16-1404.

1.3.5. Review and maintain all semi-annual security self-inspection reports and security incident reports for a period of two years according to AFRIMS.

1.3.6. Joint Personnel Adjudication System: Manage the Joint Personnel Adjudication System JPAS) for the organization, to include in and out processing unit personnel and ensuring members have current clearance eligibility. Monitor security clearances via the Joint Clearance Access Verification System (JCAVS) to identify when additional investigative action is required. Notify personnel requiring a periodic reinvestigation (PR) of their security clearance and assist in completing required forms for submission.

1.3.7. Personnel Security Investigations: Personnel Security Investigations (PSI) are due every 5 years for critical sensitive positions (Air Force Specialty Code (AFSC)/position codes requiring Top Secret eligibility/access) and every 10 years for non-critical sensitive positions (AFSC/position codes that require Secret eligibility/access). All military members will undergo the Tier 3 investigation at a minimum. The DoD CAF will adjudicate all military investigations and reinvestigations using the national security adjudicative guidelines. The types of investigations are as follows:

1.3.7.1. Tier 1a Investigation is completed when Low Risk Non-sensitive, including HSPD-12 Credentialing

1.3.7.2. Tier 2a Investigation is completed when Low Risk Non-critical sensitive, including Confidential, Secret, & L access eligibility for contractors & military.

1.3.7.3. Tier 2b Investigation is completed when Low Risk Non-critical Sensitive, including Confidential, Secret, & L access eligibility for federal employees

1.3.7.4. Tier 3a Investigation is completed when Moderate Risk PT Non-sensitive

1.3.7.5. Tier 3b Investigation is completed when Moderate Risk PT Non-critical Sensitive, including Confidential, Secret, & L access eligibility

1.3.7.6. Tier 4a Investigation is completed when High Risk PT Non-sensitive

1.3.7.7. Tier 4b Investigation is completed when High Risk PT Non-critical Sensitive, including Confidential, Secret, & L access eligibility

1.3.7.8. Tier 5 Investigation is completed when Top Secret and SCI access to classified information are required, both military and civilian.

1.3.7.9. New and renewal investigations are submitted to ISPM office via the unit security manager. Fingerprint cards are required for initial investigation submissions only. AF Form 2583, *Request for Personnel Security Action*, is required with all PSI submissions, indicating the investigation or action being requested.

1.3.8. Security Information File Establishment: Security Information Files may be established by the Air Force Central Adjudication Facility (AFCAF) or by the unit commander. Coordinate with respective supervisors and/or commander for the establishment of security information files (SIF). Requests by commanders must be made in writing with supporting documentation to the 375 AMW/IP office. Act as a liaison between unit commander or staff agency chief and ISPM in monitoring SIF.

1.3.9. Provide subsequent status reports to ISPM concerning SIFs. Ensure deadlines are met within prescribed time frames and assist unit members with file completion

1.3.10. Monitor the implementation of the Personnel Security Program (PSP) requirements to include maintenance of the unit security clearance roster (JCAVS Roster).

1.3.11. Review challenges to classification and assist personnel in complying with the classification markings and transmission procedures.

1.3.12. Ensure special access program authorizations are completed and maintained on file for assigned personnel.

1.3.13. Maintain a Security Manager's Handbook for continuity in accordance with AFI 31-401, Scott AFB Supplement; paragraph 1.3.6.10.

2. INITIAL AND RECURRENT TRAINING. All unit personnel will receive an initial security briefing during in processing. Areas to be covered are: the critical nature of classified material, how to challenge classification of material, AFI 16-1404, releasing and accepting classified material, and squadron procedures for handling and safeguarding classified materials, in addition to other security information pertinent to the unit. Training will be documented in the member's training record and reviewed annually. Additionally, the unit security manager will conduct quarterly security training and annotate what type of training was accomplished and the date training was given.

2.1. **Foreign Travel Briefings/Reporting.** Foreign travel briefings will be given as necessary to unit personnel before traveling overseas or to foreign assignments. Any suspicious interactions or advances by foreign nationals must be reported to the unit security manager immediately. Members must inform unit security managers of all foreign travel plans prior to traveling.

3. ACCESS, DISSEMINATION AND ACCOUNTABILITY OF CLASSIFIED. The final responsibility for determining whether an individual will possess or have access to any element of classified information rests with each individual who has authorized possession, knowledge, or control of the information involved. This determination will be based upon possession of a valid security clearance at or above the level of classified information involved, need to know (whether the individual's official duties require access to the classified information) and validation of a signed SF 312, *Nondisclosure Agreement (NDA)*, on file. No person may have access to classified information unless that person has been determined to be trustworthy and

access is essential to the accomplishment of lawful and authorized Government purposes, meaning, the person has the appropriate security clearance and need-to-know. Security reference manuals are maintained by the Security Manager and are available for use by all personnel.

3.1. **Access, dissemination, and accountability.** Will comply IAW AFI 16-1404, Information Security Program Management. No one will be afforded access to classified material due to rank or position. Each person who removes material from a classified storage container or vault is accountable for that material until it is returned to the appropriate container or transferred to appropriate agencies for movement. Dissemination of classified will be kept to the absolute minimum levels required. The commander will determine distribution of documents that require further dissemination.

3.1.1. Secret and Confidential information, originating within the DoD, may be disseminated within the Executive Branch, unless prohibited by the originator. Each office originating or receiving Top Secret information shall maintain Top Secret accountability registers. Such registers shall be retained for 2 years. Each DoD Component for controlling Secret information shall establish administrative procedures and material originated or received by an activity, distributed or routed to a sub element of such activity, and disposed of by the activity by transfer of custody or destruction. Administrative controls shall be established to protect Confidential information received, originated, transmitted, or stored by an activity.

4. VISITORS REQUIRING ACCESS TO CLASSIFIED INFORMATION.

4.1. **Procedures for visitors who require access to classified informiaton or facilities that contain classified information.** The number of classified meetings, breifings, or conferences involing visitors shall be held to a minimum. The visit sponsor must determine that the visit is necessary and that the purpose of the visit cannot be achieved without access to, or disclosure of, classified information. The security managers will ensure positive identification of visitors, appropriate PCL, and need-to-know prior to the disclosure of any classified information. The security managers will also ensure that visitors are only afforded access to classified information consistent with the purpose of the visit.

4.1.1. Visits that require access to classified information, the host shall verify the visitor’s PCL level. Verification of a visitor’s PCL may be accomplished by a review of JPAS which is the designated database that contains the information. In some cases the Visitor may not have access to JPAS and they may send a visit authorization letter (VAL) provided by the visitor’s employer.

4.1.2. All persons in attendance at classified sessions shall possess the requisite clearance and need-to-know for the information to be disclosed. Need-to-know shall be determined by the authorizing agency or its designee based on the justification provided. Attendance shall be authorized only to those persons whose security clearance and justification for attendance have been verified by the security officer of the organization represented. The names of all authorized attendees or participants must appear on an access list with entry permitted to the classified session only after verification of the attendee's identity based on presentation of official photographic identification such as a contractor or U.S. Government identification card.

4.1.3. Classified information must be authorized for disclosure in advance by the government agency having jurisdiction over the information to be presented. Individuals making presentations at meetings shall provide sufficient classification guidance to enable attendees to identify what information is classified and the level of classification. Classified presentations shall be delivered orally and/or visually. Copies of classified presentations or slides, etc., shall not be distributed at the classified meeting, and any classified notes or electronic recordings of classified presentations shall be classified, safeguarded, and transmitted as required.

4.1.4. The physical security measures for the classified sessions shall provide for control of, access to, and dissemination of, the classified information to be presented and shall provide for secure storage capability, if necessary.

5. HANDLING, TRANSFER, AND TRANSMISSION OF CLASSIFIED. Transmission of classified material is defined in AFI 16-1404. Transmission of classified material may be in the form of mailing, electrical transmission, and hand carrying. Procedures are established as follows (Travel Management Office (TMO) will adhere to procedures outlined in applicable Transportation regulations and instructions for surface and air movement):

5.1. **Mailing classified material.** Documents will be placed in two opaque envelopes. "SECRET" material will be accompanied with an AF Form 310, *Document Receipt and Destruction Certificate*. The AF Form 310 will be placed in the inner envelope with the document. The last copy of the AF Form 310 will be kept on file. The inner envelope will be sealed using high-grade paper tape (brown) on all seams and completely covering the flap of the envelope. Once this is done, the envelope will have the return address and control number of the document affixed to the top left-hand corner of the envelope. Stamp and mark the classification on the inner envelope, top and bottom, front and back. Place the envelope in another opaque envelope and address and seal it in the same manner as the inner envelope. It is very important not to put the classification on the outer envelope. Prepare a DD Form 2825, *Internal Receipt*, to initiate registered mailing through the postal channels. The DD Form 2825 must accompany the package to the mailroom. Classified materials sent via postal system will not be addressed to a specific individual.

5.1.1. "CONFIDENTIAL" documents mailed off base will be packed in the same manner as "SECRET" material. It is not necessary to use an AF Form 310. On the outer envelope, place the notation "Postmaster: Do Not Forward; Return to Sender." The outer envelope will not be marked with the classification. For this organization, "CONFIDENTIAL" and "SECRET" documents will not be sent through the Base Information and Transfer System. If there is material to be picked up by another activity, they will be notified by telephone.

5.2. **Hand carry or escort classified information off base.** A letter designating an individual as an "official courier" is required. You are required to read this guidance before initiating action for official courier.

5.3. **Procedures for removing classified material from the confines of 932 AW buildings are as follows:**

5.3.1. Ensure documents are marked with the correct classification.

5.3.2. Use proper cover sheet to cover document front and back.

5.3.3. Place material in an unmarked envelope or folder.

5.3.4. Retain envelope or folder in your possession at all times until placed back in GSA security container or destroyed.

5.4. **Transmission of DoD Classified Material via Federal Express (FedEx).** FedEx shall be used only when it is the most cost effective way to meet a program requirement, given time, security and accountability restraints. FedEx may be used for the transmission of SECRET and CONFIDENTIAL material only within the Continental United States (CONUS). To ensure direct delivery to the addressee, the release signature block #7 on the FedEx Airbill Label may not be executed under any circumstances. The SECRET and/or CONFIDENTIAL material must meet FedEx standard size and weight limitations. Packages should be shipped via FedEx only on Mondays through Thursdays so as to ensure that FedEx does not have possession of a package over a weekend. Any problems encountered with the use of FedEx for the transmission of SECRET and CONFIDENTIAL material are to be reported to the unit security manager as soon as possible. A report will be made to the ISPM and they will follow there procedures once the issue is presented to there office.

5.5. **Control of classified packages.** The DoD has authorized the transmission of DoD classified material via General Services Administration (GSA) contract Carrier, FedEx. Activity Distribution Offices and Action Offices who receive packages from FedEx should handle them as if they contained classified material; i.e., if the package is passed from one individual/office to another, signature control using a DD Form 2825 will be necessary as it will not be known if the package contains classified material. Additionally, these packages cannot be left unattended.

6. REPRODUCING CLASSIFIED. Should there be any reproduction of classified material, it will be kept to a minimum. The OPR will be consulted prior to reproducing classified material and will designate approved reproduction facility. Reproduction Authority and Persons Designated to Copy Classified Material on Approved Copier will establish unit procedures for reproduction of classified information and identify reproduction limitations, if any, for the material. Individuals will reproduce only the minimum amount of classified needed to support user requirements or files.

6.1. **Unauthorized Reproduction.** All personnel must be continually alert to unauthorized reproduction of classified material. If unauthorized reproduction of classified material is detected, the security manager must be notified immediately.

6.2. **Classified Copier Use.** The following procedures apply to reproduction of classified material using the office copier:

6.2.1. Classified Reproduction Rules will be conspicuously displayed over or near the copier.

6.2.2. The copier itself will be treated as if it contains classified latent images until a minimum of three new copying sequences of blank sheets have been processed through the copier machine as a preventive measure against latent image retention on the machine’s memory.

6.2.3. No service technicians will have access until the above procedure has been accomplished. Also inspect machine for any miss-fed originals or copies that may exist in the machine.

6.2.4. All reproduced copies will be afforded the same protection as the original document(s).

7. DERIVATIVE CLASSIFICATION AUTHORITY. Within DoD, all cleared personnel can perform derivative classification. Derivative application of classification markings is a responsibility of all assigned personnel who incorporate, paraphrase, restate, or generate in new form information that is already classified or those who apply markings according to the office of court administration (OCA) guidance.

8. MARKING CLASSIFIED. The originator of classified information is responsible for proper application of classification markings. The ultimate responsibility rests with the approver or signer of the document or material.

8.1. **Preparing Classified.** Those who prepare classified information are strongly encouraged to consult with their respective Security Manager and review DoD 5200.1R, Chapter 5, and DoD 5200.1PH, *A Guide to Marking Classified Documents, and Information Security Oversight Office (ISOO) Classifies National Information.*. Refer complex marking issues to the Security Manager for assistance.

9. MAINTENANCE OF SECURITY CONTAINERS.

9.1. **Authorized security containers.** A Standard Form (SF) 700, *Security Container Information*, is kept as a record of personnel to notify in the event the security of the material enclosed is affected. The SF 700 will be posted inside the locking drawer of the safe. A new date will be entered in the "date of last combination change" block on the SF 700 each time the combination of the container is changed. **Part 2** of the SF 700 must be re-accomplished each time the combination is changed. Events that may cause the combination to be changed are:

9.1.1. Container is initially placed in use.

9.1.2. An individual aware of the combination no longer requires access to the container (or is reassigned).

9.1.3. A security incident/possible compromise involving the security container (i.e. container was found opened and material inside suspected as being compromised).

9.1.4. When a container is taken out of service, the lock will be set to 50-25-50.

9.1.5. If North Atlantic Treaty Organization (NATO) material is contained within the safe, the combination must be changed every 6 months.

9.1.6. If a need to change the combination arises, contact the Safe Custodian.

9.1.7. A record of maintenance on the security container is very important. All maintenance performed on the container by authorized personnel and safe technicians must be annotated on OF 89, MAINTENANCE RECORD FOR SECURITY CONTAINERS/VAULT DOORS. This form must be maintained in the locking drawer of the classified storage container. Retain the OF 89 in the classified storage container for the life of the safe.

10. SAFEKEEPING AND STORAGE OF CLASSIFIED. The persons listed on the SF 700, are considered safe custodians.

10.1. **Safe custodians.**

10.1.1. Comply with restrictions on use of classified storage containers.

10.1.2. Report containers that malfunction to the security manager who will prepare appropriate paperwork to affect required repairs.

10.1.3. Ensure contents of classified storage containers are identified in file plans? Personal "work files" of classified information are strongly discouraged but not prohibited. When necessary, these work files should be limited to specifically labeled folders and stored separately from the contents identified in the file plan.

10.1.4. Ensure that the SF 700 is re-accomplished every time there is a personnel change and is current with the appointment letter on file.

10.2. **Opening classified storage containers.** When opening the classified storage container, you will annotate the SF 702, *Security Container Check Sheet* with the time opened and the individual's initials. Once this action is complete, the "OPEN/CLOSED" sign will be placed in the "OPEN" position.

10.3. **Closing classified storage containers.** After all material is in the classified storage container, it will be locked and the SF 702 will be annotated with the time locked and the individual's initials. After locking is complete, another individual will check to ensure it is locked and then annotate the SF 702 in the "checked by" column. Once this action is complete, the "OPEN/CLOSED" sign will be placed in the "CLOSED" position.

10.4. **Classification level of storage containers.** Only materials classified as "SECRET" and "CONFIDENTIAL" are authorized for storage in the classified storage container.

10.5. **Authorized personnel.** Only personnel authorized in writing by the commander and on file with the squadron security manager are authorized to remove and return classified material from the safe or vault. Storage of any other material such as money, jewelry, weapons and hand-held radios is not authorized in the safe.

10.6. **Storing of NATO Material.** Refer to NATO directives.

10.7. **Storage of Any Other Classified Special Access Required Material.** Consult the security authority for the Special Access Required (SAR) program on unique access and storage requirements. These SAR matters can vary from program to program.

11. END-OF-DAY SECURITY CHECKS. Security checks shall be performed at the close of each working day to ensure the area is secure. This is accomplished on SF 701, *Activity Security Checklist*. The storage of classified material in containers shall be secured on SF 702, Implementing a "Clean Desk Policy" will greatly assist in accomplishing the end-of-day security checks. The SF 701 and SF 702 must be kept on file for 3 months plus current, when dealing with non Communications Security (COMSEC) material.

11.1. **Clean Desk Practice.** All individuals performing classified work will maintain a "clean desk" office environment. At the end of the duty day, all classified material used that day will be collected or turned in for storage in the appropriate container. Before locking the container, the security manager or designated individuals will double check with all offices to

ensure no classified material was overlooked; this includes a cursory check of trash receptacles and shredder destruction areas. After all material has been gathered, material to be returned to the user the next duty day will be placed in the individual's "classified folder" and placed in the back of the safe. At no time will classified material be taken home.

12. DISPOSAL AND DESTRUCTION OF CLASSIFIED. As soon as classified material has served its intended purpose, it should be processed for destruction. Destruction should be accomplished on a monthly basis to preclude the accumulation of unneeded material.

12.1. **Retaining Classified Material Over 10 Years Old.** Classified documents that are not permanently valuable records of the government shall not be retained more than 10 years from the date of origin, unless such retention is authorized by and in accordance with record disposition schedules.

12.2. **Destruction Records.** Destruction records and imposition of a two-person rule, that is, having two cleared persons involved in the entire destruction process, will satisfy this requirement for Top Secret information. Imposition of a two-person rule, without destruction records, will satisfy this requirement for Secret information, as will use of destruction records without imposition of the two-person rule. Only one cleared person needs to be involved in the destruction process for confidential information.

12.3. **Semi-annual clean-out dates.** The semi-annual clean out dates are the first Friday in February and August. Add additional clean out dates as needed.

13. CLASSIFICATION CHALLENGES. If holders of classified information have substantial reason to believe the information is classified improperly or unnecessarily, they shall communicate that belief to their security manager or the classifier of the information to bring about any necessary correction. Challenges needed shall be acted upon within 30 days of receipt to the safe custodian so they can forward the report to the 375 AMW/IP office.

14. SECURITY INCIDENTS AND VIOLATIONS. Anyone who knows or believes there may have been a compromise, loss, unauthorized disclosure, or other infraction affecting the safeguarding of classified information must report it without delay to the ISPM.

14.1. **Appointing Investigation Officials.** The commander/director who has responsibility for the area where the information security incident occurred appoints an investigator to conduct an investigation of information security incidents.

14.2. **Briefing Requirements.** 375AMW/IP briefs the individual appointed to conduct the investigation. During these briefings the investigator is provided other technical guidance, such as consulting the local Staff Judge Advocate's office for legal guidance.

15. EMERGENCY PROTECTION PLAN. This outlines procedures for removal and protection of classified material. These instruction implements procedures outlined in AFI 16-1404 and pertain to all individuals who have access classified information.

15.1. **Responsibilities.** The Emergency Protection Plan is for planning purposes only, until activated by the Squadron Commander or Unit Security Manager. Once an Emergency Plan is established, the procedures will be briefed to all office staff and a copy placed in close proximity of the security container.

15.2. **Procedures.** Classified material maintained by the squadron is classified no higher than "SECRET" and is normally originated by higher authority. A very limited file is

maintained. The following information should be implemented in case of fire, natural disaster, or civil disturbance.

15.2.1. If a civil defense alert signal (3-5 minute steady-tone siren) is sounded or flooding occurs, all classified material must be removed from the immediate work area and secured in the appropriate security container as long as time permits

15.2.2. Removal: When removed, documents will be placed into a large envelope or container, marked with the security classification, office symbol, building and room number, sealed, and hand carried to (932 AW, Command Post(CP)).

15.2.3. In case of civil disturbance or terrorist/enemy action, secure all classified material in the appropriate security container. When an analysis presents evidence that classified documents may fall into unfriendly hands, consideration will be made to determine time allotment for destruction of documents by shredding or emergency burning.

15.2.4. All Emergency Personnel who are entering an area where classified information is displayed will be allowed immediate access. After the emergency is terminated the personnel who entered the room will sign in on an AF Form 1109.

16. STU-III PROTECTION AND RESPONSIBILITIES. (Reference: AFI 33-209)

16.1. **Responsibilities.** The STU-III or STE Responsible Officer will ensure all personnel authorized access to the STU-III adhere to the procedures outlined below at all times.

16.2. **Procedures.** The STU-III or STE Responsible Officer will accomplish the following:

16.2.1. Only unclassified phone calls will be made on terminals that are in UNKEYED mode. Removing the Crypto Ignition Key (CIK) makes the terminal UNKEYED and not secure.

16.3. **Keyed Mode.** When the terminal is in the KEYED mode, it must be afforded protection commensurate with the level of the key it contains and may only be used by authorized personnel. When unauthorized personnel who are not cleared to the level of the keyed terminal are in the area, the terminal must be under the operational control and within the view of at least one appropriately cleared and authorized person.

16.4. **Securing CIK.** STU-III or STE terminals not operational 24 hours a day will have the CIK removed at the close of business. The CIK will be stored in a safe. Secure infrequently used keys until required.

16.5. **Authentication displayed.** Strict attention must be paid to the authentication display to ensure the classification level of the conversation does not exceed the highest clearance level between the two parties. The information displayed indicates the system’s capacity and does not authenticate the person using the terminal.

16.6. **Discussing Classified.** Before discussing classified information on the STU-III or STE, the person making the call will ascertain each individual within hearing distance of their side of the conversation is cleared to the classification level being discussed and the need to know exists for those personnel. If possible, isolate phone from high traffic areas in an enclosed office.

16.7. **Emergency Action Procedures.** In the event of fire, natural disaster, or covert threat, the CIK will be removed from the phone and kept on the person of an authorized individual or secured in the normal classified storage container.

17. PROHIBITED ITEMS.

17.1. **Personal Electronic Devices.** Personal Electronic Devices, whether personal or government-owned, are not permitted in any of the designated restricted areas throughout the wing. This includes personal cellular/Personal Communications Service (PCS) and/or radio frequency, infrared wireless devices, and other devices, such as cell phones, tablets, smart watches, Fitbits, and devices that have photographic or audio recording capabilities. Any devices found in the restricted area will be confiscated with subsequent actions determined by the Squadron Commander.

17.2. **Photography limitations in areas within the Wing whre classified information is discussed or processed.** The use of cameras to take photographs in areas containing classified information is prohibited unless the following criteria have been met and approved by the appropriate Security Manager.

17.2.1. Photography requirements must be conveyed to the appointed Squadron Security Manager for the area to be photographed and all appropriate tenant Security Managers for the area to be photographed.

17.2.2. Contact will be between the squadron appointed Security Manager and Security Manager of the requesting organization.

17.2.3. Photos must be for official purposes only.

17.2.4. Cameras used must be government-owned/purchased and remain under control of government personnel, and it is the responsibility of the owner of the camera to ensure that there is no wireless capabilities, e.g., Wi-Fi and Bluetooth.

17.2.5. The Security Manager of the unit taking the photographs must coordinate with all impacted tenants 24 hours prior to the scheduled photography session(s).

17.2.6. All areas photographed are clear of classified and sensitive content.

17.2.7. Once photography is complete, the Squadron-appointed Security Manager for the area to be photographed and all appropriate tenant Security Managers for the area to be photographed will work with the requester to review and clear photos prior to release.

GLENN COLLINS, Colonel, USAF
Commander

Attachment 1

GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

References

Air Force Instruction (AFI) 31-401, *Information Security Program Management (ISPM)*

Air Force Manual (AFMAN) 33-363, *Management of Records*

Air Force Policy Directive (AFPD) 31-4, *Information Security*

DoD 5200.1PH, *A Guide to Marking Classified Documents*.

Adopted Forms

AF Form 2583, *Request for Personnel Security Action*

AF Form 310, *Document Receipt and Destruction Certificate*

AF Form 847, *Recommendation for Change of Publication*

OF 89, *MAINTENANCE RECORD FOR SECURITY CONTAINERS/VAULT DOORS*

DD Form 2825, *Internal Receipt*

SF 312, *Nondisclosure Agreement*

SF 700, *Security Container Information*

SF 701, *Activity Security Checklist*

SF 702, *Security Container Check Sheet*

Abbreviations and Acronyms

AF—Air Force

AFCAF—Air Force Central Adjudication Facility

AFI—Air Force Instruction

AFMAN—Air Force Manual

AFPD—Air Force Policy Directive

AFRIMS—Air Force Records Information Management System

AFSC—Air Force Specialty Code

AFTO—Air Force Technical Order

AMW—Air Mobility Wing

ANACI—Access National Agency Check and Inquires

AW—Airlift Wing

CIK—Crypto Ignition Key

COMSEC—Communications Security

CONUS—Continental United States

CP—Command Post

DoD—Department of Defense

FedEx—Federal Express

GSA—General Services Administrations

IAW—In Accordance With

IP—Information Program

ISPM—Installation Security Program Manager

ISSO—Information Security Oversight Office

JCAVS—Joint Clearance Access Verification System

JPAS—Joint Personnel Adjudication System

MAJCOM—Major Command

NACLC—National Agency Check with Law and Credit

NAC—National Agency Check

NATO—North Atlantic Treaty Organization

NDA—Non-Disclosure Agreement

OCA—Office of Court Administration

OG—Operations Group

OI—Operating Instructions

OPR—Office of Primary Responsibility

PR—Periodic Reinvestigation

PSI—Personnel Security Investigation

PSP—Personnel Security Program

RDS—Records Disposition Schedule

SAR—Special Access Required

SF—Standard Form

SFS—Security Forces Squadron

SG—Surgeon General

SIF—Security Information File

SM—Security Manager

SSI—Security Self Inspection

STE—Secure Telephone Unit

STU-III—Subscriber Terminal Unit-Third Generation

TMO—Travel Management Office