BY ORDER OF THE COMMANDER
434TH AIR REFUELING WING

434TH AIR REFUELING WING
INSTRUCTION 16-1404

2 SEPTEMBER 2021

Operations Support

INFORMATION SECURITY PROGRAM

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

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

RELEASABILITY: There is no releasability restrictions on this publication.

OPR: 434 ARW/IP

Certified by: 434 ARW/CCE
(Maj Samuel Pier)
Pages: 30

This instruction implements Air Force Policy Directive (AFPD) 16-14, *Security Enterprise Governance*. It standardizes the procedure for handling, controlling and safeguarding of classified material/information within all organizations of the 434th Air Refueling Wing (ARW). These procedures do not apply to Special Access Programs that are governed by other instructions. These procedures apply to all personnel within the 434 ARW that handle/control classified information or who have a security clearance eligibility. Use these procedures with DoDM5200.01 Volume 1_AFMAN 16-1404 Volume 1, *Information Security Program: Overview, Classification and Declassification; DoDM5200.01 Volume 2_AFMAN 16-1404 Volume 2, Marking of Information; DoDM5200.01 Volume 3 AFMAN 16-1404 Volume 3, Protection of Classified Information;* DoDM5220.22V2_AFMAN16-1406V2, *National Industrial Security Program: Industrial Security Procedures for Government Activities;* ; DoDM 5200.02_AFMAN 16-1405, *Personnel Security Program Management*; Department of Defense (DoD) 5200.2R, Appendix 1, *Personnel Security Program, Investigative Scope*; DoD Directive (DoDD) 8100.02, *Use of Commercial Wireless Devices, Services and Technologies in DoD Global Information Grid (GIG)*; DoD Manual (DoDM) 5200.1, Volume (V) 1, *Department of the Defense* (*DoD) Information Security Program: Overview, Classification and Declassification*; DoDM 5200.1, V2, *DoD Information Security Program: Marking of Classified Information*; DoDM 5200.1, V3, *DoD Information Security Program: Protection of Classified Information*; AFGM 2020-16-01, AF Guidance Memorandum for *Controlled Unclassified Information (CUI),*; Security Executive Agent Directive 3 (SEAD 3), *Reporting Requirements for Personnel with Access to Classified Information or Who Holds a Sensitive Position*; and Air Force (AF) Enterprise Authorizing Official Memorandum, Subj; Personally Wearable Fitness Devices; along with any base

supplements, for the implementation of the Air Force Information Security Program. This Air Refueling Wing Instruction (ARWI) is intended to standardize the 434th Air Refueling Wing, Information Protection (IP) functions. If an organization has special handling needs or concerns not covered by this ARWI, each commander is encouraged to write additional plans and procedures in conjunction with 434 ARW/IP. Ensure that all records created as a result of processes prescribed in this publication are maintained IAW Air Force Instruction (AFI) 33-322, *Records Management and Information Governance Program*, 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) listed above 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 be supplemented at any level, but all Supplements must be routed to the OPR of this publication for coordination prior to certification and approval. The authorities to waive wing/unit level requirements in this publication are identified with a Tier 3 (T-3) number following the compliance statement. See DAFI 33-360, *Publications and Forms Management*, Table 1.1 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. *Compliance with the attachments in this publication is mandatory.*

1. Responsibilities. The policies and procedures outlined throughout this ARWI apply to all personnel assigned or attached to the 434th Air Refueling Wing. Each person must ensure compliance with these procedures, report any deviations and have the moral and legal obligation to protect classified material.

1.1. **Commander will: (T-3)**

1.1.1. Establish the information security program and execute the program to comply with governing DOD and Air Force policies and instructions.

1.1.2. Review, approve and sign unit operating instruction or standard operating procedure.

1.1.3. Appoint individuals to perform security duties (i.e. Primary and Alternate Security Manager/Assistant, Self-Inspection Officials, Preliminary Inquiry Officials, etc.), as required.

1.1.4. Review security files to determine interim clearance eligibility. Review adverse information to determine if an Incident Report should be established.

1.1.5. Ensure security incidents and potential compromises of classified material are properly investigated.

1.1.6. Endorse Consolidated Compliance Reviews and semiannual self-inspection reports, as required.

1.1.7. Provide couriers with verbal authorizations to hand-carry material outside their normal work area; but remaining on the confines of the installation, if required.

1.1.8. Sign Courier Authorization Letters for hand-carrying classified material aboard a commercial aircraft.

1.1.9. Implement and actively support the information security education and training program.

1.1.10. Ensure management of classified information is a critical element in performance contracts and/or performance evaluations for all unit personnel who manage classified information.

1.1.11. Unit commanders or staff agency chiefs will appoint, in writing, a primary (must be a full time person) and at least one alternate Security Manager/Assistant. Use the current appointment letter template provided by the Wing IP office. Provide a copy of the letter to the Wing IP; letters submitted in the wrong format will be returned for correction. File a copy of this memorandum in the unit continuity book.

1.1.12. Unit commanders or staff agency chiefs will appoint, in writing, a primary (must be a full time person) and at least one alternate Security Container Custodian, when security containers and/or vaults are being utilized by the unit to store classified information. Use the current appointment letter template provided by the Wing IP office. Provide a copy of the letter to the Wing IP; letters submitted in the wrong format will be returned for correction. The safe custodian memorandum shall identify the security container/vault by its serial number and physical location. File a copy of this memorandum in the unit continuity book. Individuals appointed must have a security clearance commensurate with the level of classified being stored and complete the required training.

1.1.13. Establish a Top Secret Control Account when the organization routinely originates, stores, receives, or dispatches Top Secret material and designate in writing, a primary (must be a full time person) and at least one alternate Top Secret Control Officer, to maintain it.

1.1.14. Ensure all assigned unit personnel in/out process through the Security Manager/Assistant. Include the Security Manager/Assistant in the unit in/out processing checklist.

1.2. **Division Chiefs/Flight Commanders will:**

1.2.1. Ensure personnel complete initial, refresher and specialized Security Education and Training.

1.2.2. Ensure Standard Form (SF) 701, *Activity Security Checklist*, is completed when security containers are present and destroyed in accordance with AFRIMS Disposition Schedule.

1.2.3. Identify personnel in writing (AF 4332) who are authorized to Receive Accountable Mail. (Federal Express, Registered, First Class and Express Mail).

1.2.4. Coordinate with the Security Manager/Assistant to ensure civilian employment positions are designated correctly for position sensitivity. Assist the Security Manager/Assistant in the timely submission of periodic reinvestigations or new investigation requirements.

1.2.5. Evaluate cleared personnel to ensure they remain trustworthy for access to classified information. Report knowledge of adverse information to the Commander and assist the Commander in determining appropriate measures when an individual's action reflects non-compliance with adjudication guidelines.

1.2.6. Verify newly assigned individual's personnel security eligibility and access status with the Security Manager/Assistant and assure access is granted only at the appropriate level.

1.2.7. Ensure subordinate personnel who require access to classified information are properly cleared and are given access only to that information, to include sensitive information, for which they have a need–to–know. Make sure work center personnel are advised when newcomers are not cleared.

1.2.8. Ensure subordinates are trained in, understand, and follow work center security procedures and requirements of the information security program.

1.2.9. Provide or arrange for specialized security training when subordinate's duties involve the derivative classification of material or are assigned security container custodian duties.

1.2.10. Continually observe subordinates for personal problems, adverse conduct, or other derogatory information that could have a bearing on their continued eligibility for access to classified information or occupy a position of trust. Any derogatory information will be reported to the respective Unit Commander, Security Manager/Assistant or the Personnel Security Office (434 ARW/IP 688-2590/2587).

1.3. **Individuals will:**

1.3.1. Comply with security requirements and remain proficient in their duties and security responsibilities to prevent unauthorized disclosure of classified information.

1.3.2. Not accept custody of classified material or participate in classified discussions for which they are not properly cleared.

1.3.3. Report, without delay, to their Unit Commander or Security Manager/Assistant:

1.3.3.1. When they become aware of or believe that there may have been a compromise, loss, unauthorized disclosure, or other infraction affecting the safeguarding of classified information.

1.3.3.2. If they believe they have been contacted by an intelligence collector or other unauthorized individual seeking to gain access to sensitive government information.

1.3.3.3. Any information that could adversely reflect on their or a co-worker's suitability for continued access to classified information.

1.3.3.4. Follow the proper reporting procedures of security violations.

1.4. **The Program/Project Managers will:**

1.4.1. Coordinate/discuss program or project security requirements with the Security Manager/Assistant prior to program/project implementation.

1.4.2. Ensure program/project personnel have sufficient classification guidance when programs involve access to classified information.

1.4.3. Notify the Security Manager/Assistant when any contractors will work within the unit for more than 30 days.

1.4.4. Ensure prior to conducting a classified meeting the individual(s) hosting the meeting contact the Security Manager/Assistant and ensure proper procedures are followed. See **paragraph 5** of this instruction.

1.5. **The Security Manager/Assistants will:**

1.5.1. Oversee all aspects of the unit information, personnel, and industrial security programs and be responsible for following security policy, establishing procedures, and providing program guidance. Act as the single point of contact for the security program to outside organizations. Advise and assist the Commander and unit personnel on security matters under their purview.

1.5.2. Ensure security training is conducted and develop organizational specific security training plans as required. Provide or request assistance from outside agencies in providing specialized security training (i.e. derivative classifiers, courier briefings, foreign travel briefings, preliminary inquiry or investigating officials, etc.). Advise the Commander on the status of the unit's security training program. Ensure training is documented and records are properly maintained.

1.5.3. Implement the personnel security program and provide support to the servicing security activity. Use the Joint Personnel Adjudication System (JPAS) and Defense Information System Security (DISS) to review the status of personnel security clearances. Notify the Commander of any unfavorable information that could impact an individual's security clearance or access to classified information.

1.5.4. All permanently assigned military and civilians will be in-processed as "owning". All cleared contractors assigned to the unit will be in-processed as "servicing". Personnel on temporary duty (TDY) to the unit may be in-processed as "servicing". Personnel will not be granted access to classified material prior to JPAS/DISS indoctrination. The unit Security Manager/Assistant will not indoctrinate members into JPAS/DISS until all required security training has been accomplished. All non-SCI access will match the Security Access Requirement (SAR) code on the unit manning document and not necessarily the eligibility reflected in JPAS/DISS. All non-SCI access (US, NATO, Nuclear) will be removed from JPAS/DISS prior to out-processing.

1.5.5. Ensure annual security self-inspections are scheduled and conducted at the required intervals and provide the inspecting official with the appropriate directives, self-inspection checklists and any required guidance or assistance. Initiate corrective actions to any findings, if required.

1.5.6. Coordinate classified equipment copier approval with unit Commander. The Security Manager/Assistant will request the 434 ARW/IP approve secure shredders and facsimile machines for classified information. Shredders authorized for classified destruction will have an *Authorized for the Destruction of Classified Information Label*

and shredders for unclassified destruction will have a *Not Authorized for the Destruction of Classified Information Label* placed conspicuously on the shredder when put in to use.

1.5.7. Conduct access and termination briefings for government civilians and military personnel. The Security Manager/Assistant will execute an AF Form 2583, *Request for Personnel Security Action,* prior to granting an individual access to classified material and the Air Force (AF) Form 2587, *Security Termination Statement* to terminate an individual's access to classified material. If individual refuses to sign the AF Form 2587, the briefer and a witness will sign the AF Form 2587 documenting the refusal. The commander will be notified and form forwarded to appropriate agency. Security Manager/Assistant will confirm the member has an SF 312/Non-Disclosure Agreement (NDA) on file in JPAS/DISS. If the member does not have an SF 312 on file, the Security Manager/Assistant will assist the member in accomplishing one.

1.5.8. Provide guidance to Preliminary Inquiry Officials on conducting Security Inquiries and ensure a briefing is provided by 434 ARW/IP. The Security Manager/Assistant will coordinate with the Original Classification Authority (OCA), when required, for classified material involved in a security violation.

1.5.9. Ensure secure areas/rooms have requisite security approvals prior to storing and/or processing classified information.

1.5.10. Provide technical guidance on all information and personnel security related issues. Act as the conduit between the 434 ARW/IP and unit personnel for clearance and access issues.

1.5.11. Ensure Visual Aids are posted and authorization letters are obtained for security type equipment located in the work area.

1.5.12. The primary Security Manager/Assistant will attend all Security Manager/Assistant meetings hosted/directed by the Wing IP. Alternate Security Manager/Assistants may attend, but are not required to attend unless the primary is unavailable or their attendance is specifically requested by the Wing IP. It is the primary Security Manager/Assistant's responsibility to ensure an alternate Security Manager/Assistant attends these meetings in their absence. The alternate Security Manager/Assistant will assume duties as the primary Security Manager/Assistant when the primary is unavailable or unable to perform Security Manager/Assistant duties for any reason i.e. leave, illness, deployed, etc.

1.5.13. By the 1st of each month, the Security Manager/Assistant will coordinate with the Unit Training Manager and ensure a list of current derivative classifiers (and their respective training dates) has been submitted to wing training. By the 5th of each month, wing training will submit a compiled list to the 434 CS/CFP (Communications Focal Point). This process will ensure the suspension of derivative authority of personnel whose annual derivative classification training has lapsed/expired.

1.6. **The Security Container Custodians will:**

1.6.1. Be knowledgeable of security procedures involving the access, safeguarding, protection and marking of classified information. The primary safe custodian must be a government employee.

1.6.2. Be listed on the SF 700, *Security Container Information.*

1.6.3. Manage classified holdings by periodically reviewing material for currency, need and proper marking.

1.6.4. Establish and maintain document suspense/receipt and destruction files, as required.

1.6.5. Prepare and post required forms for each security container or secured area. Required forms:

1.6.5.1. SF 700 filed in each locking drawer or on locking door.

1.6.5.2. SF 701, *Activity Security Checklist* located adjacent the entryway of room/area where security containers are located or on a clipboard if end-of-day check duty is rotated.

1.6.5.3. SF 702, *Security Container Check Sheet,* located on each locking drawer/door.

1.6.5.4. Air Force Technical Order (AFTO) Form 36, *Maintenance Record for Security Type Equipment* and/or Optional Form (OF) 89, *Maintenance Record for Security Container/Vault Doors*; located in each locking drawer.

1.6.6. Ensure the combination to the security container is changed as required (upon departure of anyone with the combination who may have access to area where the security container is located, when the combination is suspect to compromise, or when brought into or removed from service). Combinations of all new containers and those being removed from service are set to 50-25-50.

1.6.7. It is the Security Manager/Security Assistants responsibility to ensure security containers are properly maintained. Security Managers/Assistants are responsible for conducting the preventive maintenance inspection and the Information Security Program Operation Visual Inspection (OVI), with the assistance of the Security Container Custodian. Maintenance on security containers must be in accordance with DoDM5200.01V3_AFMAN16-1404V3, Information Security Program Operation Visual Inspection (OVI) Checklist for Security Containers, Vault Doors, and Secure Rooms, preventive maintenance inspection upon receipt of DoDM5200.01V3_AFMAN16-1404V3 and every 5 years thereafter. 434 ARW/IP is responsible for assessing discrepancies reported by Security Manager/Assistants and determining if a GSA approved technician is needed to fix the security container or vault door.

1.6.8. Ensure the combination is protected at the same level as classified stored in the container.

1.6.9. Oversee the periodic purge of files in the classified storage containers/areas and, as a minimum, during the designated annual clean-out days (reference **paragraph 15.6**). In conjunction with each retention review, ensure appropriate downgrading/declassification actions are taken.

1.6.10. Ensure all personnel receive training prior to giving access to the security container. Training will include opening/closing procedures, properly marking of classified materials, completing security container documentation, reporting of security violations, and proper safeguarding of classified information. Security container custodians will complete the Marking Classified Information and Storage Containers &

Facilities courses located on the Center for Development of Security Excellence (CDSE) website, prior to appointment. All personnel who create derivative classification documents must receive initial derivative classification training and derivative classification refresher training every year thereafter. This training is located on the Defense Security Service (DSS) and Joint Knowledge Online (JKO) websites.

2. Access. Use JPAS/DISS as the primary source for confirming access eligibility for DOD military, DOD civilians, and DOD contractor personnel.

2.1. The holder, not the potential receiver of the information, determines the need–to–know and is responsible for verifying the personnel security eligibility and access of the potential receiver.

2.2. Classified information shall only be released to individuals who meet all of the following requirements:

2.2.1. Possess a valid personnel security eligibility and access (equal to or greater than the information being disclosed) that has been verified in JPAS/DISS.

2.2.2. Possess a valid-need-to-know for the information in order to perform a lawful and authorized government function.

2.2.3. Sign a SF 312, *Classified Information Nondisclosure Agreement*, verified through JPAS/DISS or accomplished in person. If a person refuses to sign the SF 312, they will not be granted access to classified information.

2.2.4. Commander must sign the AF Form 2583, cannot be delegated, authorizing access on a one time or continual basis.

2.2.5. Initial Access briefing signed by individual and date of briefing placed on the AF Form 2583.

2.2.6. Verify identity by checking a government issued identification card.

2.2.7. The unit Security Manager/Assistant will verify these elements. Personal assurance shall not be accepted for personnel security eligibility and access verification.

2.2.8. Classified information will not be released to a contractor without concurrence of the government security representative.

2.2.9. All personnel will immediately report to their Commander**,** supervisor, or Security Manager/Assistant any contact with individuals - regardless of nationality, when illegal or unauthorized access is sought to obtain classified or sensitive unclassified information.

2.2.10. The authority to designate classified contractor operations as intermittent visitors, integrated visitor groups, or NISPOM visitor groups has been delegated to the 434 ARW Chief, Information protection (CIP).

2.2.11. The authority to enter into security agreements with contractors by signing visitor group security agreements (VGSAs) has been delegated to the 434 ARW CIP.

2.2.12. Signatory authority for VGSAs is delegated to the 434 ARW CIP.

2.2.13. The Project Manager (PM), Contracting Office Representative (COR) and Security Manager/Assistant are responsible to ensure the Contracting Office provides notification

to the 434 ARW Information Protection office 30 days before the work performance start date.

3. Incoming Visit Requests. Visit requests are normally accomplished through JPAS/DISS and are accomplished by the Unit Security Manager/Assistant or 434 ARW/IP. In the few cases where visit requests are not routed through JPAS/DISS, unit Security Manager/Assistants will ensure personnel are properly cleared prior to classified access. If the visit is a Wing wide visit, contact 434 ARW/IP.

3.1. Receiving Visitor requests:

3.1.1. Incoming visit requests can also be sent to the 434 ARW/IP office via JPAS/DISS, Security Management Office (SMO) code 434ARWIP.

3.1.2. Visit authorization letters will not be used to pass security clearance information unless JPAS/DISS is not available. Procedures to send a visit request(s) if JPAS/DISS is not available, send visit requests to the 434 ARW/IP office at commercial number (765) 688-2590/2587 or DSN 388-2590/2587.

3.1.2.1. Visit requests for contractors:

3.1.2.1.1. Unclassified contractor visit must be on company letterhead and signed by the Facility Security Officer (FSO) or a designated representative excluding the visitor(s).

3.1.2.1.2. Classified contractor visit must be transmitted through JPAS/DISS, accompanied by a Defense Department (DD) Form 254, *Department of Defense Contract Security Classification Specification*, listing Grissom Air Reserve Base as a contract performance location and a Visitor Group Security Agreement (VGSA) if the contractor is performing work on the installation for more than 90 continuous days.

3.1.2.2. Visit requests for DOD civilian and military personnel should be on the service specific form and signed by a security representative.

3.1.2.3. The request must include, as a minimum: full name, social security number, date/place of birth, organization/office symbol (DOD employees only), citizenship, security clearance level and date granted, purpose of visit, date(s) of visit and a point of contact (POC) within the unit.

3.2. The disclosure of information to visitors will be restricted in scope to that information directly related to the purpose of the visit and limited to their personnel security eligibility, access, and need-to-know.

3.3. Visit sponsors are responsible for determining personnel security eligibility and access, need-to-know, and identification validation before releasing classified information to visitors. The Security Manager/Assistant will conduct clearance/access eligibility verifications upon request.

3.4. The visit sponsors, with the assistance and advice of the Security Manager/Assistant, will arrange for installation and facility access.

3.5. Visitors with classified material arriving after hours should be directed to the Grissom Air Reserve Base (GARB) Command Post in building 671 for temporary overnight storage.

3.6. Contractors are not authorized to escort personnel on visit requests per *DoDM-5200.08_Volume 3_AFMAN 31-101_Volume 3, para 6.3d, Installation Perimeter Access Control.*

4. Outgoing Visit Requests. When a government employee requires access to classified information at:

4.1. A non-DOD contractor activity, the supervisor or Security Manager/Assistant must contact the office to be visited to determine the desired clearance verification.

4.2. The unit Security Manager/Assistant will complete a JPAS/DISS visit request for personnel needing to visit another government or contractor facility. The traveler must provide the security office purpose of the visit, sponsor's name and phone number, the duration of the visit, a list of the traveler's names and social security numbers and the SMO code. SMO code can be obtained from the sponsor's Security Manager/Assistant.

5. Classified Meetings. Prior to conducting a classified meeting the individual(s) hosting the meeting will contact the Security Manager/Assistant and ensure proper procedures are followed. The Classified Meeting-Briefing-Conference checklist will be utilized.

5.1. Room/Areas must be checked to determine if sound will travel through the walls/vents/doors. If discernable sound can be heard outside the meeting area, a cleared monitor **must** be posted outside the door/vent/wall to ensure all loitering and/or unauthorized entry is prohibited.

5.2. The security clearance of all attendees must be verified prior to the meeting. Visit requests are to be on file with the security office for all non-government/military meeting participants. If foreign nationals are required to attend, contact 434 ARW/IP to ensure all appropriate action/requirements are met prior to the meeting.

5.3. Prior to the start of the meeting, the meeting area will be checked by the host for suspicious objects or obvious recording devices.

5.4. At the beginning **and** end of the meeting, the facilitator of the meeting must announce classification level of information to be discussed.

5.5. Note taking should be discouraged. If note taking is necessary, all participants must understand that notes become classified working papers and must be marked and protected accordingly.

5.6. All presentation materials must be marked properly. If used, all electronic equipment (computers, projection equipment) must be certified and accredited to the proper security level.

6. Safekeeping and Storage (Internal Control of Classified Material). Classified material will be under the constant observation of a cleared individual or locked in a GSA approved security container or accredited secure room. Any deviations must be reported to the Commander and/or Security Manager/Assistant.

6.1. Personnel will coordinate with the Security Manager/Assistant prior to relocating a container or placing new containers in service.

6.2. High value items and items susceptible to theft (funds, guns, drugs, precious metals, etc.) will not be stored in the container with classified material.

6.3. Temporary storage of classified material is available in the 434 ARW Command Post (434 ARW/CP), Phone 765-688-2124. The Command Post also provides temporary overnight storage for visitors arriving after normal duty hours.

6.4. Ensure the SF 702 is attached to the security container.

6.5. An SF 704, *Secret Cover Sheet*, 01 August 1985 or SF 705, *Confidential Cover Sheet* (as appropriate) will be attached to all classified documents removed from the security container, unless the document is remaining inside an open storage area.

6.6. Use the SF 702 to record openings and closings for all GSA approved security containers, vaults, and approved secure storage rooms.

6.7. If a security container is taken out of service (no longer needed for classified storage), Security Manager/Assistants will pull out all drawers and closely examine the interior for classified material, set the combination to the default (50-25-50), and place a note on the container stating "Not in use-combination set to default". Do not remove the OF 89 or Air Force Technical Order Form 36. Combinations to security containers, vaults, certified secure rooms will be changed:

6.7.1. When placed in service and taken out of service.

6.7.2. When an individual knowing the combination no longer requires access.

6.7.3. When the combination is compromised, or potentially compromised.

6.7.4. No less than every 12 months if none of the above situations occur.

6.8. Treat and protect all unopened accountable correspondence as classified until the contents are determined to be unclassified. Accountable correspondence consists of First Class (marked "Return Service Requested"), Registered and Certified U.S. mail, and overnight deliveries from authorized GSA carriers such as FedEx and UPS. This correspondence must be stored in a GSA-approved security container if unopened, until hand delivered to the addressee, or opened to determine the contents. Unattended accountable correspondence found to contain classified will be reported to 434 ARW/IP as a security incident.

7. End-of-Day Security Checks (Daily Security Checks): Before departing, personnel who work with classified material will check their work area (to include trash cans, desk tops, in-baskets, printers, and computers) to ensure all classified material has been secured. This security measure is in addition to, not in lieu of, the formal end-of-day security check.

7.1. Administrative Requirements:

7.1.1. SF 702 will be posted on all classified security containers and annotated each time the container is opened and closed. NOTE: If a 5-drawer security container contains 5 separate locking drawers, each drawer is considered a separate security container and each must have its own SF 702. As a minimum, each container will be checked, verified secure (attempt to open each drawer) and the SF 702 annotated during the end-of-day security check. Use the SF 702, "Checked By" column to verify the security status of containers, vaults, and security storage room during the end-of-day check and annotate it whether or not they were opened during the day.

7.1.2. SF 701 identifies items to be checked and will be posted at or near the primary entrance/exit point to each room or area where classified material is stored, handled, or

processed. Additional areas/equipment may be added to the SF 701 as well as lining through preprinted items that are not applicable. Each area utilizing the SF 701 will add the requirement to check computer systems to ensure Common Access Cards (CAC) and Secret Internet Protocol Router Network (SIPRNet) Tokens have been removed from workstations.

7.1.3. Branch, section, or office chiefs must ensure end-of-day security checks are completed.

7.2. Security Check Procedures**.** The designated individual will, as a minimum:

7.2.1. Inspect all equipment and areas, such as desk tops, copiers, fax, computers and peripherals, where classified is handled, stored, processed or destroyed, to ensure classified material is properly secured.

7.2.2. Spin the dial on security containers with mechanical locks at least four (4) times in one direction (for electro-mechanical locks such as the X-07/08/09 spin the dial to ensure the lock is engaged) and attempt to open each drawer or door manually.

7.2.3. Examine secure communications devices such as Secure Telephone Equipment (STE) and remove crypto key. Also check classified computers with removable drives, to ensure the drives have been removed and secured in a GSA approved security container if applicable.

7.2.4. Record the check, the time the check was conducted and initials of the person making the check, on SF 701 and SF 702.

8. Information Processing Equipment: Classified information will only be processed on computer(s) approved and specifically designated for processing classified information. Authorized personnel will process classified information in accordance with the equipment's Authorizing Official (AO) approved security plan.

8.1. Classified hard drives, floppy disks, CD-ROMs, and computer generated products will be properly marked, controlled and safeguarded equal to the level of classified information stored on the item. Review DoDM5200.01V2_AFMAN16-1404V2, *Information Security Program: Marking of Classified Information*, for limitations and unique marking requirements.

8.2. The use of small Universal Serial Bus (USB) type storage devices are prohibited for storing classified information, unless approved with a waiver. Personally owned or unapproved USB devices are not authorized to be used on any government computer.

8.3. Personnel will ensure when utilizing classified computers that the monitors are located in such a way that unauthorized personnel cannot view them. In addition, equipment will not be repositioned without prior approval of the TEMPEST Manager.

8.4. All other small devices (headsets, web cams, exc.) must be justified and approved by the ISSM for the classified system. In addition to computer security requirements, they will:

8.4.1. Be prominently and properly marked with the highest classification of material stored or to be stored on them.

8.4.2. Be stored in a security container approved for classified storage when not in use.

8.4.3. Inventoried and accounted for at the end of the duty day.

8.4.4. The use of "disguised" storage devices are prohibited in any government system.

8.4.5. Personnel in rooms/areas containing computers processing classified information must remain in attendance or if approved for open storage, ensure area is secured when classified hard drives are in the system.

8.4.6. Personnel will consult Air Force Systems Security Instruction (AFSSI) 5020, Remnants Security, when removing classified data from computer systems, components, and media.

8.4.7. Personnel using classified computer systems will never download any document to an unclassified computer system, without proper approval and proper software. Contact the Security Manager/Assistant for any questions.

8.4.8. Commanders and equivalents must justify, in writing, the need for secure room open storage of classified materials that will not fit inside a GSA approved security container. Secure room open storage will not be approved for the storage of products such as paper documents, optical media, and other devices or products that will fit inside a GSA approved security container. Commanders and equivalents may construct vaults for the open storage of classified materials and must coordinate construction and certification with 434 ARW/IP. Commanders and equivalents are responsible for vault and secure room funding and work order submission through appropriate channels. Security Manager/Assistants will coordinate open storage justification, approval, and certification with 434 ARW/IP.

8.4.9. The 434 Civil Engineer (434 CE) will provide an engineer as requested to certify construction standards. The 434 Security Forces Squadron (SFS) will provide Electronic Security Services support for the access control and intrusion detection systems employed. Both entities will do this IAW DoDM 5200.01, Volume 3, *DoD Information Security Program: Protection of Classified Information*, Appendix to Enclosure 3 standards in conjunction with 434 ARW/IP findings of the requested area.

9. Packaging and Transmission of Classified. Packaging and transmission requirements for classified material dispatched via U.S. Postal Service or approved overnight courier.

9.1. Classified document/material will be enclosed in two opaque sealed envelopes or similar wrapping, size permitting. If size prohibits, then the classified material must be enclosed in two opaque, sealed containers, such as boxes or heavy wrapping.

9.2. If the classified material is an internal component of a packable item or equipment, then the outer shell or body may serve as the inner enclosure, providing no classified information is revealed.

9.3. All materials used for packing must be of such strength and durability as to provide security and protection while in transit and to facilitate the detection of tampering. The wrappings must also conceal all classified characteristics.

9.4. Classified written information will be folded or packed in such a manner that the text will not be in direct contact with the inner envelope or container. Avoid mailing written materials of different classifications in a single package.

9.5. Inner wrappers will be marked with the highest classification of material contained in the package along with any special warning or control notices. Outer wrappers must not display classification markings, but will have the official address of the owner/user.

9.6. Review DoDM5200.01V3_AFMAN16-1404V3, for additional information and instructions on modes of transmission and packaging requirements.

10. Receiving Classified: The central 434 ARW mail receiving/distribution offices for Base Information Transfer System (BITS) is Building 427, Room 1304**.** All personnel assigned duties to receive office mail will:

10.1. Have at least a SECRET clearance.

10.2. Be authorized to sign receipts for incoming mail and maintain approval letter on file with BITS.

10.3. Protect all overnight delivery as classified material until proven otherwise. Secure unopened "suspect mail" in an approved security container at the end of the duty day or when the office is unattended.

10.4. Receivers of classified material or "suspect mail" will:

10.4.1. Inspect packaging for signs of tampering. Contact the Security Manager/Assistant and sender if tampering is detected or suspected.

10.4.2. Compare the contents to items listed on the AF Form 310, *Document Receipt and Destruction Certificate* (note any discrepancies on the receipt) sign and return the AF Form 310 to the sender. Discrepancies are to be reported to the sender and Security Manager/Assistant immediately.

10.4.3. Review the material for content and proper markings prior to entering the material into the classified filing system or security container. Contact the sender/originator to resolve marking problems.

10.4.4. Initiate a challenge when there is a substantial reason to believe classified information is improperly or unnecessarily classified. Challenges may be either formal or informal, with the informal challenge the preferred first step.

10.4.5. To initiate a challenge:

10.4.5.1. Contact the material originator, via secure communications, to discuss your concerns.

10.4.5.2. If unable to resolve the matter by an informal challenge, initiate a formal challenge. Consult security directives and the Security Manager/Assistant to initiate a formal challenge.

10.4.5.3. Classified information undergoing a challenge will be protected and safeguarded at the current classification level and unclassified information will be protected at the proposed classification level, pending final resolution.

10.4.5.4. The Security Manager/Assistant will notify 434 ARW/IP when a formal challenge is initiated.

11. Hand-carrying of Classified Material on the Installation.

11.1. When hand-carrying classified material from one building to another on Grissom ARB:

11.1.1. Enclose classified material in an inner and outer wrapper/container.

11.1.2. The inner container will be marked with the highest classification of material inside.

11.1.3. The outer container will not contain any external classification markings.

11.1.4. Close or seal the containers to prevent loss or inadvertent access to the classified contents.

11.2. All couriers will be briefed by the Security Manager/Assistant on courier responsibilities and will not make intermediate or convenience stops with classified material in their possession.

12. Hand-carrying of Classified Material off the Installation.

12.1. Hand carrying classified material off the installation will be done as a last resort, only after considering alternatives such as mailing or electronic transmission. When approved:

12.1.1. A courier must carry a DD Form 2501, *Courier Authorization*, when traveling off the installation or aboard commercial passenger aircraft.

12.1.2. Material will be double wrapped and addressed as if it were being mailed.

12.2. The DD Form 2501, signed by the 434 ARW/IP will not exceed two years. Member's hand-carrying COMSEC material will follow COMSEC guidelines.

12.3. Couriers will coordinate security arrangements with the Security Manager/Assistant and destination when leaving the local area, using commercial transportation, or a trip that requires an overnight stay.

12.4. Couriers will be briefed and must acknowledge their security responsibilities. The Security Manager/Assistant or supervisor will conduct and record these briefings.

13. Reproduction of Classified. Reproduction of classified material should only be done if absolute necessary. Contact your Unit Security Manager/Assistant for assistance prior to reproducing any classified information. Reproduction will only be accomplished on equipment specifically designated and approved for classified reproduction. Additional reproduction requirements follow:

13.1. Personnel will maintain constant surveillance and control over reproduction equipment and area where the equipment is located when reproducing classified material.

13.2. Personnel will follow the classified reproduction rules posted on the equipment and ensure the equipment is cleared of any latent images after classified reproduction.

13.3. Account for all originals, copies, and waste before departing the copy area.

14. Equipment Control.

14.1. The Security Manager/Assistant will obtain the necessary equipment approvals and post the appropriate visual aid on unit equipment approved for classified reproduction.

14.2. In the event of an equipment malfunction, personnel will attempt to clear the situation by following the equipment instructions. If classified material cannot be removed, summon assistance**. Do not leave the equipment or classified material unattended**. Escort maintenance technicians, if required, and ensure they do not access material they are not cleared for.

14.3. All reproduction equipment must have the appropriate visual aids posted:

14.4. A *Classified Reproduction Rules* label will be posted on equipment approved for reproduction of classified material.

14.5. A *No Classified Reproduction* label will be posted on equipment not authorized for reproduction of classified material.

15. Destruction.

15.1. Classified material will be destroyed when no longer required for operational requirements or by law. The Security Manager/Assistant will obtain necessary approvals and ensures devices have been approved for the destruction of classified material by referencing the National Security Agency/Evaluated Products List (NSA/EPL). Contact 434 ARW/IP at 688-2590/2587 for assistance. Other destruction requirements are as follows:

15.1.1. One cleared person may destroy CONFIDENTIAL and SECRET classified material.

15.1.2. Equipment operators will inspect the debris during and after the destruction session. The inspections are to ensure the equipment is operating properly and ensure the material is adequately destroyed. When a shredder is used, check the functional areas to ensure that no classified material remains intact.

15.1.3. Check the immediate area before departing the shredder to ensure that no classified remains.

15.2. Controlled Unclassified Information will be destroyed in accordance with (IAW) DoDM 5200.1, Volume 4, Enclosure 3.

15.3. Review AFSSI 5020, *Remanence Security*, for instructions on the degaussing, declassification, destruction/turn-in of electronic/magnetic media, equipment and products.

15.4. Classified computer disks, CD-ROMs, and magnetic media may be destroyed in the Wing Destruction Facility located in Building 427, Room 1306 (434 Communication Squadron/Information Assurance).

15.5. When transporting material outside the facility for destruction, place it in an opaque bag or box sealed and marked in a fashion to protect the material from loss or unauthorized disclosure during transport. Material must be protected as classified until destruction is complete.

15.6. The 434th Air Refueling Wing annual clean-out day will be 15 August of each year. The focus of this event will be a retention review and the disposal of all classified material that is obsolete or unnecessary. This does not preclude the units from establishing their own additional clean out days. Document when clean out is conducted.

15.7. Excess material no longer required by law or mission accomplishment will be identified and subsequently destroyed.

15.8. During the retention review, complete any downgrading/declassification actions noted on the material.

15.9. Container custodians will destroy unclaimed material after consulting with the work center supervisor and security.

16. Security Incidents and Violations. All personnel are personally responsible for the protection of classified information. Reporting procedures for security incidents and violations are as follows:

16.1. Any person who has knowledge of the loss or possible compromise of classified information will immediately report such facts to the Security Manager/Assistant, immediate supervisor, or the Commander.

16.2. A person finding classified material unattended or improperly stored is responsible for protecting it until the responsible custodian or other such official regains proper custody.

16.3. The Security Manager/Assistant will advise the Commander on inquiry/investigative requirements. The Security Manager/Assistant is responsible for reporting the incident to the 434 ARW/IP Office no later than the first duty day following the reporting of the incident. **Note:** In incidents where classified material is lost or out of proper controls, all notifications will be made in person or over secure communications.

16.4. The Commander or appointing authority will appoint the preliminary inquiry official IAW DoDM5200.01V3_AFMAN16-1404V3, for all security incidents.

16.5. The inquiry official appointment letter will be accomplished and signed by the appointing authority. Upon notification of appointment, the inquiry official will make an appointment with the 434 ARW/IP office for a briefing on the incident and their responsibilities. The inquiry official will provide a copy of their appointment letter to the 434 ARW/IP. The inquiry official will also contact the 434 ARW/Staff Judge Advocate (SJA) to receive a briefing (if necessary).

16.6. The inquiry official will prepare a written report. The report will at a minimum be marked "Controlled Unclassified Information" and be completed within 30 days of appointment. The report will be routed through the 434 ARW/IP to the appointing official. The Chief, Information Protection will provide technical reviews of the report and concur/non-concur on the findings and forward it to the appointing official.

16.7. The appointing official reviews the report, concurs or non-concurs with findings, make closing remarks, and identify any corrective actions required. The closed report will be forwarded to the 434 ARW/IP.

16.8. The appointing official directs a formal investigation when the initial inquiry is insufficient and it is believed that more information can be obtained through a formal investigation. Refer to 434 ARW/IP and 434 ARW/SJA for assistance.

17. Controlled Unclassified Information (CUI): Unclassified information that requires safeguarding or dissemination controls, pursuant to and consistent with applicable law, regulations and Government-wide policies. Some examples of CUI are as follows: For Official Use Only (FOUO), Law Enforcement Sensitive (LES), DoD Unclassified Controlled Nuclear Information (DoD UCNI), Limited Distribution, as well as some of those developed by other Executive Branch agencies. For guidance on CUI refer to AFGM 2020-16-01.

18. Security Education and Training. Commander or equivalents ensure that each individual receives continuing education and training throughout their duty assignment. Flight Commanders, division/branch chiefs, section heads, and supervisors will support and assist in training unit personnel.

18.1. **Initial Training:** All newly assigned personnel will receive initial security training from the Security Manager/Assistant, during in-processing or before accessing classified material. Training will include cleared or un-cleared Information Security training. Training will be documented on the annual training log.

18.2. **Continuing and Refresher Training:**

18.2.1. Annual refresher training will be conducted in accordance with DoDM5200.01V1_AFMAN16-1404V1. Training will be documented on the annual training log.

18.2.2. Security Manager/Assistants are encouraged to intermittently distribute training materials to unit personnel and, with the assistance of division/branch section chiefs and supervisors, ensure all personnel are trained. The Security Manager/Assistant will maintain records identifying the names of personnel trained, subjects presented and date(s) training was completed.

18.3. **Specialized Training:**

18.3.1. Security Manager/Assistant's, security container custodian (primary and alternate) and derivative classifiers to include SIPRNET users, will complete specialized training as required. At a minimum, training will cover the requirements identified on the respective Appointment Memorandums. All personnel with SIPRNET access/accounts will be identified and trained per established procedures as derivative classifiers.

18.3.2. Persons needing specialized training should contact the Security Manager/Assistant to schedule training.

19. Safeguarding North Atlantic Treaty Organization (NATO) Classified. No collateral NATO classified information is currently being stored within any organization. Contact your Unit Security Manager/Assistant should a requirement arise to store, discuss, or process NATO classified material. All personnel that require "Access" will receive the NATO Security Briefing and document the training utilizing the NATO Brief-Rebrief-Debrief form, which will be maintained by the Security Manager/Assistant. Training will be documented on the annual training log.

20. Marking Classified. Marking of Classified Information will be in accordance with DoDM5200.01V2_AFMAN16-1404V2. Derivative classifiers will refer to the proper Security Classification Guides to ensure appropriate classified markings are in place. Any questions or concerns may be directed to the 434 ARW/IP, 688-2590/2587.

20.1. In an environment where both classified and unclassified information is processed or stored, IT equipment will be identified according to highest level of classification contained in, contained on, or destroyed by that item. The SF 710, "Unclassified (Label)" shall be used to identify unclassified media or equipment. Place the label conspicuously to indicate the highest classification of material authorized for processing. The SF 710 is not required in areas where classified information is not processed or stored.

20.2. Grissom ARB does not have Original Classification Authority (OCA); therefore there is no requirement for OCA appointments or training.

21. Secure Communications. Secure Voice Telephone equipment (STE, vIPer, VoSIP, etc.) will be used by unit personnel to discuss classified and sensitive unclassified information.

21.1. Classified and Sensitive Unclassified information will not be discussed via STE, vIPer, VoSIP, etc. in the presence of persons not cleared for access to the information.

21.2. Conversations must be conducted at a volume where they will not be intercepted, intentionally or inadvertently, by unauthorized persons.

21.3. All Secure Voice equipment that can be placed in the non-secure mode will be, unless required for classified/unclassified sensitive information transmission.

21.4. The unit Secure Voice Responsible Officer (SVRO) will provide secure communication devices training and document the training prior to allowing personnel to use secure communication devices. See the unit SVRO to coordinate training.

22. Security Self-Inspections. All wing, tenant and geographically separated units that participate in the Wing's Information, Industrial and Personnel Security Programs will be included in the self-inspection.

22.1. Unit Commander or equivalents, will appoint an individual in writing, to conduct an annual security inspection. A program review may satisfy the requirement for one of the annual self-inspections.

22.2. The Security Manager/Assistant will provide the Inspecting Official with the appropriate directives, self-inspection checklists, and any required guidance or assistance.

22.3. Inspecting Officials will document inspection results in a report to the Commander.

22.4. After review and endorsement by the Commander, the report will be returned to the Security Manager/Assistant for action (if required) and filed in the Security Manager/Assistant's Continuity Book.

22.5. The Wing IP office may conduct no-notice inspections throughout the year to evaluate compliance of security requirements and procedures to safeguard classified and controlled unclassified information.

23. Review of Personnel Security Clearance Status. The Security Manager/Assistant will conduct a monthly review of the unit's Joint Clearance Access Verification System (JCAVS/JPAS/DISS) roster to monitor Periodic Reinvestigation (PR) requirements and will direct any questions to 434 ARW/IP.

23.1. Individuals notified to submit an Electronic Questionnaire for Investigations Processing (e-QIP) are responsible for completing and submitting all required investigative paperwork to 434 ARW/IP upon completion. The Security Manager/Assistant will provide guidance/assistance in the preparation of the e-QIP. The 434 ARW/IP will review/validate the package prior to submission to the Office of Personnel Management (OPM) or referral for Continuous Evaluation Deferment.

23.2. The Security Manager/Assistant will be responsible for preparing the AF Form 2583, *Request for Personnel Security Action and* the DD Form 1879, *Request for Personnel Security Investigation* (when required).

23.3. Unit commanders and supervisors will ensure that Periodic Reinvestigation requests are submitted prior to the anniversary date of the last investigation; 10 years for access to Secret and 5 years (currently 6 years) for access to Top Secret information. Requests for an eQIP

account will be submitted via an email to the 434 ARW/IP office, no sooner than 6 months prior to the expiration date.

23.4. The request can be accomplished via an email that includes the individual's full name, SSAN, date of birth, investigation type and verified email address. The unit Security Manager/Assistant will verify that all of the information is correct and current, prior to submitting a request. Security Manager/Assistants may submit multiple requests in a single email. Security Manager/Assistants will ensure that personnel security investigations are submitted in accordance with the Position Code as stated/identified on the Unit Manning Document (UMD). Unit Security Manager/Assistants will ensure a member has at least 12 months remaining in service or employment.

23.5. The 434 ARW/IP office will initiate the eQIP and notify the unit Security Manager/Assistant who will provide advice and assistance to the member in completing the eQIP. All eQIP requests will be completed within 30 days.

23.6. In the event the member does not complete the eQIP or the system terminates the request, the unit Security Manager/Assistant will notify the 434 ARW/IP office to re-initiate the request. If the member fails to complete the request a second time, the commander will make a determination to establish an Incident Report and will acknowledge he/she counseled the member, via the Failure to Complete Background Investigation letter. Once the letter has been signed by the unit commander, it will be forwarded to the 434 ARW/IP office who will re-initiate eQIP. If the member fails to complete their eQIP a third time, the appropriate group commander will be notified. If it is determined that the member is refusing to complete their eQIP, then the commander will initiate an Incident Report.

23.7. If the member is enrolled in Continuous Evaluation Deferment, the 434 ARW/IP office will send a notification of enrollment letter to the member and the unit Security Manager/Assistant. The 434 ARW/IP office will also notify members and unit Security Manager/Assistants when an investigation is favorably adjudicated. In either event, the unit Security Manager/Assistant should notify the Unit Deployment Manager (UDM).

23.8. In the event that an initial investigation request is required (T3/T5), then the AF Form 2583, *Request for Personnel Security Action* will be utilized to include a local files checks. Once the eQIP is completed, the member will contact the 434 ARW/IP office to obtain a fingerprinting appointment.

23.9. Interim security clearance eligibility for Secret and Top Secret will be requested by the unit Security Manager/Assistant. The unit commander is the final approving authority for interim clearance requests. Interim clearance eligibility requests will be submitted as follows:

23.9.1. All interim requests will be accomplished on the AF 2583, *Request for Personnel Security Action.* It will be used to conduct and annotate the local files check. The local files check will consist of a review the individuals Personal Security Questionnaire and a review of any personnel, medical and security records. The unit Security Manager/Assistant will review the personnel records prior to submitting the request.

23.9.2. If adverse information is discovered during the local files check, the AF 2583 will be annotated and returned to the unit Security Manager/Assistant. If upon review of the adverse information, the unit commander may submit a memorandum stating that the individual has been interviewed and the individual represents an acceptable security risk.

The memorandum will be attached to the AF 2583 and maintained at the unit. Once approved the interim security clearance eligibility will be annotated in JPAS/DISS.

23.10. Each unit Security Manager/Assistant will be given access to JPAS/DISS upon submission of the appropriate System Access Request (DD 2962) and completion of the required training. JPAS/DISS will be used to monitor security clearance eligibility, personnel investigation status, log the completion of non-disclosure agreements and when the commander has granted access to classified information.

23.11. Unit Security Manager/Assistants are responsible for maintaining their unit's Personnel Security Management network (PSM Net). The USM will in process personnel as they are gained by the unit and out process as they are discharged, retiring or separating from the unit. The PSM Net must be kept current.

23.12. Security Manager/Assistants will execute the AF 2587, *Security Termination Statement* to remove access to classified material prior to out processing a member from their PSM if the member is transferring to another organization, separating or retiring. The AF 2587 will be maintained at the unit level for two years and then destroyed. Contact the 434ARW/IP office if the member refuses to sign the AF 2587. If the member is not available to sign, make attempts to orally debrief the member and annotate the AF 2587 as such. If the member cannot be debriefed then mark the form as "Not available for Debriefing".

24. Incident Report Establishment.

24.1. Supervisors and/or the Security Manager/Assistant will immediately notify the Commander when derogatory information is revealed which could have an impact upon an individual's continued security eligibility. Commanders will notify the 434 ARW/IP office within 72 hrs. of the discovery of derogatory information.

24.2. Similarly, any individual who becomes aware of information that may call a person's loyalty, trustworthiness, and reliability into question (i.e., unexplained wealth, personal, criminal or immoral conduct, excessive use of alcohol, use of illegal drugs, mental or emotional instability, misuse of computers, etc.) must report such information to the Commander, Security Manager/Assistant, or supervisor.

24.3. The Commander will review and evaluate the derogatory information against the standard security criteria as outlined in DOD 5200.2R, Appendix I and AFI 31-501, Ch. 8, *Personnel Security Program Management*. Based on the facts available, the Commander will decide whether to establish an Incident Report and also determine whether or not to suspend the individual's access to classified information/systems, withdraw unescorted access to Restricted Areas and access to the Local Area Network (LAN).

24.4. Unless otherwise specified by the Commander**,** the Security Manager/Assistant will act as liaison with 434 ARW/IP on Incident Report actions.

25. Emergency Protection, Removal and Destruction of Classified Material. In case of emergency such as fire, bomb threat, natural disaster, civil disturbance, terrorist activities, or upon direction of the commander, Installation Control Center, or other authority, classified material will be returned to its security container and the container locked. When time is of the essence, material may be secured in any available security container, evacuated with the holder, or as a last resort, left behind. All personnel who work with classified information shall be aware of these procedures.

25.1. DO NOT risk injury or loss of life to secure classified material.

25.2. If the emergency is such that classified material cannot be secured, the holder will evacuate the area taking the material with them. The holder will notify the senior government official at the central evacuation point that they are holding classified material or that classified materials have been left unsecured in the work area. The holder will provide the location, type of classified (media, documents, etc.) and the approximate amount.

25.3. Protect the classified material until the emergency is terminated or take action to secure it in an approved security container. Individual is responsible for returning the classified information to the proper security container unless otherwise directed by the commander or the Security Manager/Assistant.

25.4. Under no circumstances will the classified material be transported to the holder's private living quarters.

25.5. The Grissom ARB Command Post, Building 671, may be used for the temporary storage of classified material.

25.6. Immediately following an emergency and by direction of the Commander or ranking officer, personnel will return to their work areas and check for any unsecured classified information. Immediately report to the Security Manager/Assistant or the Commander when un-cleared emergency response personnel obtain access to classified or classified information is lost or destroyed. As soon as possible, obtain the names of all persons entering the area for any debriefings which may be necessary.

25.7. In the event facilities are made uninhabitable, the Security Manager/Assistant will advise Commander/staff agency chief on protection alternatives.

25.8. During exercises, classified material will be secured prior to evacuation.

25.9. **Emergency Action Plans.**

25.9.1. **Fire:**

25.9.1.1. Whatever actions are taken, give utmost consideration to safety of personnel. Security of classified material is secondary.

25.9.1.2. Upon discovering a fire, call 911; notify personnel to evacuate the building and active the manual fire alarm. Depart the facility and await the arrival of FD personnel at the designated assembly area.

25.9.1.3. Firemen will be granted access to fight the fire. Firemen ***will not*** be delayed entry to secure classified.

25.9.1.4. When the fire has been extinguished and facility reentry is permitted, take a complete inventory of the classified material to ensure it is still accounted for and in a usable condition. Immediately notify the Security Manager/Assistant of destroyed or unusable classified material and/or unauthorized access of classified information.

25.9.1.5. At no time during or after the event will other than authorized personnel be allowed to enter the area without the permission of the on-scene responsible official. Security representatives, if available, will assist in access control. Ensure they are advised if any classified material could not be secured.

25.9.1.6. When the emergency is over, obtain the names of all persons entering the area for any debriefings which may be necessary. When facility reentry is permitted, take a complete inventory of classified information.

25.9.2. **Natural Disaster:**

25.9.2.1. Natural disasters of a magnitude that can disrupt operations can happen with little or no notice. Different types of occurrences will require different actions, thus, the senior person present must use good judgment to determine necessary actions. Whatever actions are taken, give utmost consideration to safety of personnel and the security of classified material.

25.9.2.2. Many natural disasters are short-lived in nature (earthquakes, tornadoes, severe lightning storms, etc.), but can often create other emergency situations (fire, chemical spills, etc.). Remain alert to quickly changing situations.

25.9.2.3. Other disasters can occur which are not natural, but can disrupt operations. Some of these include aircraft crashes, hazardous chemical spills, and radiological accidents. Protective measures for classified material, according to the situation, would be required in these instances also.

25.9.2.4. If a disaster should occur which requires implementation of emergency procedures, at no time during or after the event will other than authorized personnel be allowed to enter the area without the permission of the on-scene responsible official. Security Forces and/or security representatives, if available, will assist in access control. Ensure they are advised of any classified material which could not be secured.

25.9.2.5. When the emergency is over, obtain the names of all persons entering the area for any debriefings which may be necessary. When facility reentry is permitted, take a complete inventory of classified information.

25.9.3. **Bomb Threat:**

25.9.3.1. The chances of a bomb threat occurring at Grissom ARB are possible. If such an event should occur, the senior person present must use good judgment to determine necessary actions. Whatever actions are taken, give utmost consideration to safety of personnel and the security of classified material.

25.9.3.2. Bomb threats may be received by various means (e.g., telephone, letters, notes, etc.) which relates the possible or actual presence of explosive devices. These threats must be considered factual and should be acted upon accordingly. Without prompt and decisive action by the recipient of the communication, the threat could result in injuries or fatalities and destruction of property. If the threat is a prank or hoax, the result will be a temporary disruption of operations.

25.9.3.3. The majority of bomb threats are received by telephone. The following general rules apply:

25.9.3.4. If possible, keep the caller on the phone as long as possible. Using the AF Form 440, *Bomb Threat Aid*, located at all telephones, make note of the person's vocal characteristics and background noises. Attempt to find out as many facts as possible about the explosive device.

25.9.3.5. DO NOT hang up the phone, even if the caller does.

25.9.3.6. If a bomb threat is received, use extreme caution in taking any action. Detonation devices come in many different forms, do nothing more than look for suspicious objects without moving anything. If evacuation is warranted, leave quickly and quietly; open doors carefully. Persons or animals trained in bomb detection will search for the device; this is NOT your responsibility.

25.9.3.7. If the communication is received in writing, do not excessively handle the correspondence. Handling the correspondence can easily interfere with law enforcement investigations.

25.9.3.8. At no time during or after the event will other than authorized personnel be allowed to enter the area without the permission of the on-scene responsible official. Security Forces and security representatives, if available, will assist in access control. Ensure they are advised if any classified material could not be secured.

25.9.3.9. When the emergency is over, obtain the names of all persons entering the area for any debriefings which may be necessary. When facility reentry is permitted, take a complete inventory of classified information.

26. Personally Wearable Fitness Devices and Other Personal Portable Electronic Devices near Classified Processing or Discussion. The use of Portable Electronic Devices (PED) including personal wearable fitness device (PWFD) defined in DoDD 8100.02, *Use of Commercial Wireless Devices, Services, and Technologies in the Department of Defense (DoD) Global Information Grid (GIG),* 23 April 2007, in collateral classified processing areas, is **prohibited**. This prohibition includes in proximity to classified discussion and where proper sanitization of the area or room has not occurred. Units should periodically screen their affected areas for unauthorized devices.

27. Reporting Requirements for Personnel with Access to Classified Information or who hold a Sensitive Position.

27.1. To meet requirements of SEAD 3 all individuals on Grissom ARB that have been granted "Access" to classified information must report all "unofficial" foreign travel. Any travel to Puerto Rico, Guam or other U.S. possessions and territories is not considered foreign travel and need not be reported. Unplanned day trips to Canada and Mexico shall be reported upon return.

27.2. Required Foreign Travel reporting must be approved by Commander, through unit Security Manager/Assistant prior to any foreign "unofficial" travel. While emergency circumstances may preclude full compliance with the pre-travel reporting requirements, the covered individual at a minimum, shall verbally advise their supervisor/management chain of the emergency foreign travel with all pertinent specifics. In any event, full reporting shall be accomplished when the individual returns.

27.3. Required Foreign Travel reporting must be completed within 5 days of return if possible, no later than the first UTA after travel.

27.4. Unit Security Manager/Assistant will log the members travel in DISS.

27.5. Any Person "Read" in to Top Secret Special Access Program (SAP) information will comply with their program managers respective instructions and need not duplicate reporting travel for collateral classified information.

28. The Standard Form 311, *Agency Security Classification Management Program Data*, will include the total number of classification decisions on finished products, regardless of media or whether produced in electronic form. The SM will collect numbers of classification decisions for the SF 311 for the IP office. The IP office will designate a 2-week period during the FY between April and June and record 100% of decisions during the sample periods on the SF 311.

29. Areas Not Covered in this Operating Procedure: For procedures not covered in this ARWI, contact the Security Manager/Assistant.

THOMAS O. PEMBERTON, Colonel, USAF
Commander, 434 Air Refueling Wing

Attachment 1

GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

References

AFI33-322, *Records Management and Information Governance Program*, 23 March 2020

AFI31-501, *Personnel Security Program Management*, 27 January 2005

AFMAN31-113, *Installation Perimeter Access Control (FOUO)*, 02 February 2015

AFMAN33-363, *Management of Record*, 1 Mar 2008

AFPD16-14, *Security Enterprise Governance,* 31 December 2019

DAFI33-360, *Publications and Forms Management*, 1 December 2015, Correction 7 August 2020

DoD5200.2R, Appendix 1, *Personnel Security Program, Investigative Scope*, 1 January 1987

DoDD 8100.02, *Use of Commercial Wireless Devices, Services, and Technologies in the Department of Defense (DoD) Global Information Grid (GIG)*, 23 April 2007

DoDM5200.01V1_AFMAN16-1404V1, *Information Security Program: Overview, Classification and Declassification*, 11 January 2021

DoDM5200.01V2_AFMAN16-1404V2, *Information Security Program: Marking of Classified Information*, 7 January 2021

DoDM5200.01V3_AFMAN16-1404V3, *Information Security Program: Protection of Classified Information*, 23 December 2020

DoDM5220.22V2_AFMAN16-1406V2, *National Industrial Security Program: Industrial Security Procedures for Government Activities,* 8 May 2020

AFGM 2020-16-01 *Air Force Guidance Memorandum for Controlled Unclassified Information CUI*, 23 July 2020

SEAD 3 - *Reporting Requirements for Personnel with Access to Classified Information or Who Holds a Sensitive Position*, 12 June 2017

Adopted Forms

AF Form 310, *Document Receipt and Destruction Certificate*

AF Form 440, *Bomb Threat Aid*

AF Form 847, *Recommendation to Change for Publication*

AF Form 2583, *Request for Personnel Security Action*

AF Form 2587, *Security Termination Statement*

AFTO Form 36, *Maintenance Record for Security Type Equipment*

DD Form 254, *Department of Defense Contract Security Classification Specification*

DD Form 2501, *Courier Authorization*

OF 89, *Maintenance Record for Security Containers/Vault Doors*

SF 312, *Classified Information Nondisclosure Agreement*

SF 700, *Security Container Information*

SF 701, *Activity Security Checklist*

SF 702, *Security Container Check Sheet*

SF 704, *Secret Cover Sheet*

SF 705, *Confidential Cover Sheet*

Abbreviations and Acronyms

AF—Air Force

AFI—Air Force Instruction

AFMAN—Air Force Manual

AFPD—Air Force Policy Directive

AFRCVA—Air Force Reserve Command Visual Aid

AFRIMS—Air Force Records Information Management System

AFSS—Air Force Systems Security Instruction

AFTO—Air Force Technical Order

ARB—Air Reserve Base

AMW—Air Mobility Wing

AFRI—Air Mobility Wing Instruction

CAC—Common Access Card

CC—Commander

CDSE—Center for Development of Security Excellence

CE—Civil Engineer

CIP—Chief, Information Protection

COMSEC—Communication Security

COR—Contracting Office Representative

CP—Command Post

CS—Communication Squadron

CUI—Controlled Unclassified Information

DAA—Designated Approval Authority

DD—Defense Department

DISS—Defense Information System Security

DoD—Department of Defense

DoDD—Department of Defense Directive

DoDM—Department of Defense Manual

DSS—Defense Security Service

EMSEC—Emissions Security

EPL—Evaluated Products List

e-QIP—Electronic Questionnaire for Investigations Processing

FOUO—For Official Use Only

FSO—Facility Security Officer

GARB—Grissom Air Reserve Base

GIG—Global Information Grid

GSA—General Services Administration

IAW—In Accordance With

IP—Information Protection

JCAVS—Joint Clearance Access Verification System

JPAS/DISS—Joint Personnel Adjudication System

LAN—Local Area Network

LES—Law Enforcement Sensitive

MICT—Management Internal Control Toolset

NATO—North Atlantic Treaty Organization

NSA—National Security Agency

OCA—Original Classification Authority

OF—Optional Form

OPM—Office of Personnel Management

OPR—Office of Primary Responsibility

OVI—Operation Visual Inspection

PED—Portable Electronic Devices

PM—Project Manager

POC—Point of Contact

PR—Periodic Reinvestigation

PWFD—Personal Wearable Fitness Device

RDS—Records Disposition Schedule

SAP—Special Access Program

SEAD—Security Executive Agent Directive

SF—Standard Form

SFS—Security Forces Squadron

IR—Incident Report

SIPRNet—Secret Internet Protocol Router Network

SJA—Staff Judge Advocate

SM—Security Manager/Assistant

SMO—Security Management Office

STE—Secure Telephone Equipment

SVRO—Secure Voice Responsible Officer

UCNI—Unclassified Controlled Nuclear Information

USB—Universal Serial Bus

V—Volume

VGSA—Visitor Group Security Agreement