BY ORDER OF THE COMMANDER
WARNER ROBINS AIR LOGISTICS COMPLEX

WARNER ROBINS AIR LOGISTICS COMPLEX INSTRUCTION 16-1404

12 NOVEMBER 2024
Certified Current, 26 March 2026
Operations Support

SECURITY PROGRAM

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

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

RELEASABILITY: There are no releasability restrictions on this publication

---

OPR: WR-ALC/OMD

Certified by: WR-ALC/OM
(Eric V. Faison)

Supersedes: WR-ALCI16-1404, 22 September 2020

Pages: 23

This instruction implements the Air Force Policy Directive (AFPD) 16-14, *Security Enterprise Governance*, Air Force Instruction (AFI) 16-1404, Air Force Materiel Command (AFMCSUP) Supplement, *Air Force Information Security Program*; Department of Air Force Manual (DAFMAN) 16-1405, *Department Air Force Personnel Security Program*; DODM 5220.32v1, *National Industrial Security Program: Procedures for Government Activities*; AFI 10-701, *Operations Security (OPSEC)*; AFMAN 17-1301, *Computer Security (COMPUSEC)*; and DoDI O-2000.16, Vol 1, *Antiterrorism Program Implementation: DoD Antiterrorism Standards*, and other security directives. This instruction establishes policy and procedures for the proper handling, processing, and safeguarding of classified material entrusted to or under the jurisdiction of Warner Robins Air Logistics Complex (WR-ALC) staff offices. It explains actions taken pertaining to access, dissemination, accountability of classified information, transmission of classified material, protection/removal of classified material, disposal/destruction procedures, security education program, security incidents, and conducting annual self-assessments. It includes security specialist duties, along with processes for conducting annual self-assessments and security training and applies to all personnel, contractors, military, and visitors assigned to or attached to WR-ALC Staff Offices. This instruction applies to controlled unclassified information (CUI) under the purview of relevant statutes, regulations, and directives. This instruction contains procedures on security clearance eligibility for government and contractor employees in accordance with (IAW) DODM 5200.02_DAFMAN 16-1405_DAFGM2023-01, *Air Force Personnel Security Program*, and is applicable to all WR-ALC staff agency civilian personnel and those Department of Defense (DoD) contractors authorized under the terms of a signed Visitor

Group Security Agreement (VGSA) to perform classified contract services IAW DODM 5220.32v2 and contractors performing unclassified contracts who access government automated information systems. This publication may be supplemented at any level, but all direct supplements must be routed to the office of primary responsibility (OPR) of this instruction for coordination prior to certification and approval. Report errors, suggest revisions, and recommend corrective action about this publication to the OPR using the Department of the Air Force (DAF) Form 847, *Recommendation for Change of Publication*. Requests for waivers must come through the chain of command from the civilian director of the squadron seeking relief from compliance. Waiver requests must be submitted to the OPR; waiver authority has not been delegated. This publication is exempt from tiering pursuant to DAFI 90-160, *Publications and Forms Management*. Ensure that all records generated as a result of processes prescribed in this publication adhere to AFI 33-322, *Records Management and Information Governance Program*, and disposed of IAW the Air Force (AF) Records Information Management System Records Disposition Schedule, which is located in the AF Records Information Management System. 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 AF. See **Attachment 1** for glossary of references and supporting information.

SUMMARY OF CHANGES

This publication supersedes AFI 16-1404, WR-ALC Operating Instruction (OI) 16-1, *Emergency Protection or Removal of Classified Material*, and WR-ALC OI 16-2, *Security Program*. This document has been revised to incorporate system updates and regulatory updates. Changes include system of record reflected as Defense Information System for Security (DISS) and updates to regulation name designations.

1. Responsibilities.

1.1. **Overview.** All government employees and DoD contractor personnel have a moral and legal obligation to protect classified material, ensure compliance with applicable directives, and report any deviations.

1.2. **The WR-ALC Commander (CC)/Deputy Director (DD)/Deputy Commander for Maintenance (DCM) will:**

1.2.1. Provide direction for the overall security program within WR-ALC staff offices.

1.2.2. Appoint, in writing, a primary and alternate to oversee the information, industrial, and personnel security programs within the Complex staff offices.

1.2.3. Appoint, in writing, a primary Security Specialist to oversee personnel within the 402d Aircraft Maintenance Group, 402d Commodities Maintenance Group, 402d Electronics Maintenance Group, and 402d Maintenance Support Group.

1.2.4. Grant and terminate access to classified information.

1.2.5. Appoint, in writing, a government inquiry official to investigate any occurrence of a security incident.

1.2.6. Appoint safe custodians and alternates. These custodians will ensure proper safe procedures are followed. A copy of the appointment memorandum will be maintained in each security container and provided to the Security Office.

1.3. **WR-ALC Staff Supervisors will:**

1.3.1. Be responsible for ensuring all assigned personnel meet clearance requirements prior to assigning duties that require access to classified information.

1.3.2. Continually monitor and evaluate personnel with security clearances for indicators that may signal matters of personal concern that could potentially affect national security. Supervisors must recommend the establishment of an incident report to Security for cases meeting this criterion.

1.3.3. Ensure all new-hire and reassignment personnel in-process through the Security Office. They will be indoctrinated to appropriate security access in DISS and complete all initial new hire training before having access to classified information. Further, supervisors will ensure personnel departing staff offices out-process with the Security Office.

1.4. **WR-ALC Assigned Staff Personnel and Contractors will:**

1.4.1. Maintain compliance and be familiar with the provisions outlined in this instruction. This instruction applies to contractors as indicated in the contract and VGSA.

1.4.2. Upon discovering a security incident, take control of the situation or material, and safeguard it until Security, the responsible custodian, or other official regains proper custody.

1.4.3. Report suspected violations to their immediate supervisor and the Security Office immediately upon discovery.

1.4.4. Before providing access to classified information, ensure the recipient has the proper security clearance and a legitimate need-to-know.

1.4.5. Complete all security-based training prior to the suspense date established by the Security Office.

1.4.6. Contact WR-ALC Privacy Act Monitor immediately if a Privacy Act violation has been identified.

1.4.7. Report to their chain of command any conduct or information that may affect a person's trustworthiness, reliability, or loyalty.

1.4.8. Report all foreign travel to Security Office 30 days prior to travel. See **paragraph 12**.

2. Handling, Marking, Processing, and Safeguarding of Classified Information.

2.1. **Granting Access to Classified Information.** Granting access to classified information is the responsibility of the person who has authorized possession, knowledge, or control of the information.

2.1.1. Before granting access to classified information, the following criteria must be met:

2.1.1.1. Recipient possess a valid security clearance at or above the level of the classified material.

2.1.1.2. Official duties require a need-to-know for access to the classified information.

2.1.1.3. Signed Standard Form (SF) 312, *Classified Information Nondisclosure Agreement*.

2.1.1.4. For contractors, verify the information/accesses are authorized via the Department of Defense (DD) Form 254, *Department of Defense Contract Security Classification Specification*, on the contract for which the information is being released to fulfill the contract.

2.2. **Classified Processing.** The use/possession of personal and government portable electronic devices (PED) inside areas approved/accredited for classified open storage is strictly prohibited. A PED generally includes any easily transportable electronic device that has a capability to store, record, and or transmit data, digital images/video, or audio. Post visual aid signs prohibiting electronic devices where classified is processed.

2.2.1. Examples of prohibited items: cell phones (including blackberries, iPhones, androids, etc.); radio-frequency wireless personal digital assistants (including pocket computers/palm pilots), all electronic readers or tablets (including kindle, nook, iPad, etc.); iPods/MP3 players; AM/FM radios; wireless keyboards/mice; personal external hard drives; Bluetooth equipped devices; cameras; thumb drives (universal serial bus drives); two-way radios and tape recorders; smart trackers (including AirTag, SmartTag, Tile etc), listening devices (ear buds, and headphones) and wearable technology (i.e., smart watches, fitness devices, smart glasses). Post visual aid signs prohibiting electronic devices where classified is processed.

2.2.2. Notify your Security Manager (SM), supervisor, or commander if a security incident has occurred due to violation of above policy.

2.3. **Classified Storage.**

2.3.1. Safe Custodians.

2.3.1.1. Primary and Alternate Safe Custodians. Oversee the continuous purging of administrative file systems containing classified information and the annual clean-out on the second Friday of March each year. Each custodian will maintain a memorandum on file indicating the contents were reviewed and all applicable declassification, downgrading, or destruction have been completed.

2.3.1.2. Ensure combinations are protected and secured based on the highest classification of the items or materials affected.

2.3.1.3. SF 700, *Security Container Information*. The safe custodian or security manager shall maintain a record for each container, or vault or secure room door, used for storing classified information. Only DoD government employees shall be assigned as a primary custodian.

2.3.1.4. SF 701, *Activity Security Checklist*, will be annotated at the end of each day. SF 701 will note weekends, holidays, or down days as appropriate.

2.3.1.5. SF 702, *Security Container Check Sheet*, will be annotated every time the X07/X09/X10 is opened and locked. Post on the outside of the security container.

2.3.1.5.1. Mark "Not Opened" when the container is not opened. Do not leave the day blank. The "Checked By" block must be annotated for each day, even if the safe is not opened.

2.3.1.5.2. Weekends and holidays will not be annotated unless the safe was accessed during those times.

2.3.2. The Security Office will visually inspect all security containers upon receipt and every five years IAW AFI 16-1404_AFMCSUP). Visual inspections will be annotated on the Optional Form (OF) 89, *Maintenance Record for Security Containers/Vault Doors*. Safe custodians will maintain the OF 89 in the control drawer of the security container.

2.3.3. All personnel with safe access are required to complete the annual computer based-safe custodian managed through Employee Information Management Center (EIMC) and the one-time "Marking Classified Information and Derivative Classified" training available through the Center for Development of Security Excellence.

2.3.4. Classified material will be stored in a general services administration (GSA) approved security container. Classified material will be under the constant observation of an authorized individual or secured in an approved security container.

2.3.5. When to Change Combinations:

2.3.5.1. When placed in use (i.e., remove the factory combination setting of 50-25-50).

2.3.5.2. Whenever an individual knowing the combination to the container or vault door no longer requires access, unless other sufficient controls exist to prevent that individual's access to the lock.

2.3.5.3. When it is subjected to compromise (i.e., the container was left unsecured).

2.3.5.4. When the container, vault, or secure room door is taken out of service or is no longer used to store classified information, at which time built-in combination locks shall be reset to the standard combination 50-25-50.

2.3.6. Record and seal combinations to security containers on part 2 of the SF 700 and store in a separate GSA approved safe. Mark SF 700, Part 2 with highest classification level of contents maintained in the container and points of contact if found open. Mark the SF 700 at the top, bottom, front/back, and seal in opaque envelope and provide to Security to maintain.

2.4. **Marking and Transmission of Classified (hard copy documents and material).** All classified information shall be clearly identified by marking. Marking is the principal means of informing holders of classified information about specific protection requirements. For detailed guidance, refer to DoDM 5200.01, Volume 2, *DoD Information Security Program: Marking of Information*, and Volume 3, DoD *Information Security Program: Protection of Classified Information;* Executive Order 13526, *Classified National Security Information*; and Information Security Oversight Office (ISOO) Marking Classified National Security Information.

2.5. **Packaging and Transmission Requirements.** Packaging and Transmission Requirements for Classified (hard copy document and material) dispatched via the Base Information Transfer Center (BITC), Transportation Management Operations, and GSA approved overnight carriers for classified information.

2.5.1. Packaging. Material used for packaging 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. Always examine packages/containers bearing classified material for signs of tampering. If such signs are evident, notify the SM immediately for additional guidance and action.

2.5.1.1. Classified written information will be folded or packaged 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.

2.5.1.2. The outer envelope or container for classified material will be addressed to an official government activity or to a DoD contractor with a facility clearance and approved storage capability and will show the complete return address of the sender. The outer envelope must not be addressed to an individual and will not bear a classification marking (i.e., SECRET).

2.5.1.3. The inner envelope or container will show the address of the receiving activity, the address of the sender, the highest classification of the contents (i.e., SECRET) (including, where appropriate, any special markings such as “Restricted Data”), and any applicable special instructions. The inner envelope shall have an “attention” line with a person’s name. Include an AF Form 310, *Document Receipt and Destruction Certificate*, inside the inner envelope.

2.5.1.4. Prior to sending classified material, ensure recipient can receive/protect classified, and that the mailing address is current for receiving classified material.

2.6. **Transporting.** SECRET material may be transported by United States Postal Service (USPS) registered mail or USPS Express Mail® IAW DoDM 5200.01, Volume 3, Enclosure 4. Material may also be transported to Continental United States (CONUS) locations by a GSA-approved overnight delivery carrier. Contact SM to request an updated list of carriers authorized to transport classified information.

2.6.1. SECRET material to be transported via the USPS will be hand-carried to the BITC or base mail room, 78 Force Support Squadron (building 910), where the package will be dispatched by registered mail. Packages will have a USPS Label 200, *Registered Mail Label*; Postal Service (PS) Form 3811, *Domestic Return Receipt*; and two copies of PS Form 3877, *Firm Mailing Book for Accountable Mail*. Packages to be dispatched by Express Mail® must have two copies of PS Form 3877 and an accompanying letter of justification.

2.6.2. The BITC no longer dispatches via private carrier. In order to dispatch SECRET to CONUS locations via GSA-approved overnight delivery carriers, the group must have an account with the private carrier and follow procedures in DoDM 5200.01, Volume 3, Enclosure 4.

2.6.3. Prior to sending classified material to contractor facilities via approved carrier, contact 78th Air Base Wing Information Protection (78 ABW/IP) with the contractor's cage code to ensure the contractor is approved to send/receive classified material via GSA-approved overnight carrier.

2.7. **Signing for Accountable/Classified Mail.**

2.7.1. The WR-ALC mail room, 155 Richard Ray Boulevard, Suite 100, Building 210, basement, has been designated as the activity distribution office for BITC distribution. Express® and registered mail from BITC, to include first class mail stamped/marked "RETURN SERVICE REQUIRED," is considered accountable mail and will be safeguarded as such. Additionally, packages received via overnight private carriers will be considered accountable and safeguarded as such until opened.

2.7.2. Administrative staff office support personnel designated, in writing by appointment letter, to sign for accountable/classified mail will:

2.7.2.1. Possess a SECRET clearance.

2.7.2.2. Be authorized by the WR-ALC/OM director to receipt/sign for incoming mail.

2.7.2.3. Inspect all approved overnight carrier and BITC accountable mail for signs of tampering. If tampering is suspected, contact the SM immediately.

2.7.2.4. Open all approved overnight carrier and BITC accountable mail immediately to determine if content contains classified material. The address label on the outer wrapper of a classified package will not include a person's name.

2.7.2.5. Generate a DD Form 2825, *Internal Receipt*.

2.7.2.6. Notify the addressee for immediate pickup.

2.7.2.7. Deliver hand-to-hand any classified material received.

2.7.2.8. Ensure the intended recipient or an authorized individual signs the DD Form 2825.

2.7.2.9. Maintain a copy of all DD Forms 2825, or other accountable receipts, for two years. ***Note:*** If the WR-ALC mail clerk is unavailable to receive approved overnight carrier or BITC mail delivery, the alternate will sign for accountable mail. Other employees may be authorized to sign for accountable mail but must be designated by appointment letter. Packages will be kept in the signer's possession until the mail clerk/alternate returns or until it can be secured in the WR-ALC/OMD safe, located in WR-ALC mail room. Do not leave accountable mail unattended.

2.7.3. The intended recipient will:

2.7.3.1. Pickup accountable mail from the WR-ALC mail room when notified and sign the DD Form 2825 to acknowledge receipt of mail.

2.7.3.2. If the package contains classified material, inspect the inner wrapper for tampering.

2.7.3.3. If mail is classified as SECRET, the recipient signs and returns the AF Form 310 to the sender immediately. Individuals need not use the AF Form 310 for CONFIDENTIAL material, unless asked to do so by the sending activity, IAW DODM 5200.1 V3_ DAFM16-1404V3. Maintain a copy of DD Form 2825 and AF Form 310 for two years.

2.7.3.4. Review document for content and marking requirements prior to entering the documents into the classified file system.

2.7.3.4.1. For additional guidance, review DoDM 5200.01, Volume 3. Contact your security office to initiate challenge for improper or unnecessary classifications and/or markings. The security office is responsible for notifying 78 ABW/IP, DSN 468-3079 whenever a challenge is initiated.

2.8. **Destruction of Classified.**

2.8.1. Classified documents/materials that are no longer required will be destroyed IAW DoDM 5200.01, Volume 3, and AFI 16-1404_AFMCSUP.

2.8.2. Only National Security Agency approved devices are approved for the destruction of classified material. Coordinate with the Security Office on all purchases for classified destruction to ensure it is authorized. When disposing of classified materials, first determine that the material is no longer required and provide protection throughout the destruction process. Classified material is considered to be "destroyed" when the contents are no longer recoverable from the residue of the destruction process.

2.8.3. Secret and confidential material does not require a record of destruction, however an appropriately cleared person must be involved with the destruction process.

2.9. **Reproduction of Classified.**

2.9.1. Best practice to ensure approved reproduction equipment is cleared after reproducing classified material by printing five blank sheets to ensure no residual classified information is on the printing elements.

2.9.2. Copy machines will be posted with the appropriate signs. Obtain applicable signs for copy machines from the 78 ABW/IP SharePoint.

2.10. **Hand-carrying Classified Information.**

2.10.1. If hand-carrying on the installation and not passing through an activity entry/exit point, supervisor's oral approval suffices. An activity entry/exit point is described as a place that is manned by a Security Forces member.

2.10.1.1. Package must be double wrapped in two opaque envelopes with level of classification, name, and address on inner envelope.

2.10.1.2. A locked briefcase can count as the outer wrap. ***Note:*** A DD Form 2501, *Courier Authorization*, is not required for hand-carrying classified on base only.

2.10.2. If hand-carrying classified through an activity entry/exit point and within a 15-mile radius of Robins Air Force Base (RAFB), use the DD Form 2501 signed by the SM, orders approving official, Complex CC/DD/DCM, group commander/director, or staff office chief.

2.10.3. If travelling more than 15 miles from RAFB and within the United States, prepare a courier and exemption letter signed by the orders approval official.

2.10.4. Courier cards expire two years from the date of issuance. The last four digits of the individual's social security number (SSN) will be required instead of the full SSN on the card.

2.11. **Security Incidents and Violations.**

2.11.1. Any person who has knowledge of the loss or possible compromise of classified information will immediately report such facts to the immediate supervisor and SM. The person (military, civilian, contractor) discovering the security incident is responsible for protecting the classified information until the responsible custodian or other such official regains proper custody.

2.11.2. If the incident occurs in a staff office, the staff security office will immediately notify the appropriate staff office chief.

2.11.3. The security office will advise the staff office chief of inquiry or investigative requirements as outlined in DoDM 5200.01, Volume 3. The government inquiry official appointed by the Complex CC/DD/DCM, or staff office chief will be relieved of all other duties until preliminary inquiry is complete.

2.11.4. An inquiry official will be appointed within 24 hours of identification of an incident. An appointment letter will be accomplished, and a copy will be provided to 78 ABW/IP. The inquiry official will receive a briefing by 78 ABW/IP before beginning inquiry. The SM will brief WR-ALC/CC/DD/DCM if it is determined the security incident is of a serious compromising nature requiring immediate notification.

2.11.5. The SM responsible for the area in which the incident occurred will report the incident to 78 ABW/IP, Information Security Program Management (ISPM), DSN 468-3079, by the end of the first duty day. The ISPM will also be contacted if contractor personnel are involved.

2.11.6. A copy of the inquiry official appointment letter and completed inquiry report will be provided to the security office within ten duty days of completion.

2.11.7. Any unauthorized disclosure or spillage of classified or controlled information will be categorized as a Security Violation and a Security Inquiry/Investigation will be initiated to determine if the incident was willful, negligent, or inadvertent.

2.11.7.1. Willful: An incident is willful if the person purposefully disregards DoD security information safeguarding policies or requirements (e.g., intentionally bypassing a known security control).

2.11.7.2. Negligent: An incident is negligent if the person acted unreasonably in causing the spillage or unauthorized disclosure (e.g., careless lack of attention to detail or reckless disregard for proper procedures).

2.11.7.3. Inadvertent: An incident is inadvertent if the person did not know, and had no reasonable basis to know, that the security violation or unauthorized disclosure was occurring (e.g., the person reasonably relied on improper markings).

2.11.8. All reports will be forwarded to the 78 ABW/IP office. Anyone found to have caused a "willful or negligent unauthorized disclosure" will be reported through DISS to the Department of Defense Central Adjudication Facility. Reports may have an impact on security clearance eligibility.

2.12. **Controlled Unclassified Information (CUI).**

2.12.1. CUI is information the government creates or possesses, or that an entity creates or possesses for or on behalf of the government, that a law, regulation, or government-wide policy requires or permits an agency to handle using safeguarding or dissemination controls.

2.12.2. Unlike classified information, an individual or organization generally does not need to demonstrate a need-to-know to access CUI, unless required by a law, regulation, or governmentwide policy, but must have a lawful governmental purpose for such access. DoD CUI may be disseminated to DoD personnel to conduct official DoD and U.S. government business in accordance with a law, regulation, or government-wide policy.

2.12.3. CUI requires safeguarding measures identified in Part 2002.14 of Title 32, Code of Federal Regulations (CFR) and, as necessary, in the law, regulation, or government-wide policy with which it is associated. No individual may have access to CUI information unless it is determined he or she has an authorized, lawful government purpose. The person with authorized possession, knowledge, or control of CUI will determine whether an individual has an authorized, lawful government purpose to access designated CUI.

2.12.4. CUI information and material may be transmitted via first class mail, parcel post or bulk shipments. When practical, CUI information may be transmitted electronically (e.g., data, website, or e-mail), via approved secure communications systems or systems utilizing other protective measures such as public key infrastructure or transport layer security (e.g., https). CUI transmission via facsimile machine is permitted; however, the sender is responsible for determining whether appropriate protection will be available at the receiving location before transmission (e.g., facsimile machine attended by a person authorized to receive CUI; facsimile machine located in a controlled government environment).

2.12.5. Guidance for destroying CUI documents and materials is provided in Department of Defense Instruction (DODI) 5200.48_DAFI 16-1403, *Controlled Unclassified Information* (CUI), the CUI Registry, and ISOO Notice 2019-03. When destroying CUI, including in electronic form, agencies must do so in a manner making it unreadable, indecipherable, and irrecoverable. If the law, regulation, or government-wide policy specifies a method of destruction, agencies must use the method prescribed. Do not place any work-related documents in the blue recycle bins. The blue recycle bins are not authorized source for storing CUI, personal identifiable information or unclassified information.

2.12.6. DoDI 5200.48_DAFI 16-1403, provides guidance on other types of CUI information and their associated markings.

2.13. **Classified Meetings.**

2.13.1. Classified meetings hosted by Staff personnel must be coordinated through Security at least 30 days prior to the event. A security plan must be developed to address issues related to DoDM 5200.01, Volume 3, Enclosure 2.

2.13.2. All personnel will adhere to the following procedures for classified meetings/discussions:

2.13.2.1. Access to classified meetings will be limited to persons who possess an appropriate security clearance and need-to-know. The person releasing the information must be satisfied that cleared recipient has a need-to-know.

2.13.2.2. All attendees must have their clearance verified by Security before entering the meeting.

2.13.2.3. Ensure the meeting classification level is announced prior to information being disseminated. Personnel without a valid security clearance can attend unclassified portions of the meeting but will need to depart the area before classified information is released. During classified meetings, ensure all doors and windows are closed/covered to prevent inadvertent access. Post signs identifying classified discussion in progress.

3. Emergency Protection or Removal of Classified Material.

3.1. **General Information.**

3.1.1. Natural disasters, civil disturbances, terrorist activities, or enemy action may require relocation of classified material to minimize the risk of its compromise.

3.1.2. The responsibility for protection or removal of classified material under emergency conditions rests with the owner/user organization.

3.1.3. Emergency situations require written procedures to ensure classified material does not fall into unauthorized hands. In the event something happens to the user while carrying a classified container or material (i.e., accident), finder will notify the WR-ALC Control Center (Readiness Section, WR-ALC/OMD), WR-ALC Security Manager (WR-ALC/OMD), or the commander/director of the organization where material originated. Organizational symbol should be marked on the outside of all containers

3.2. **Procedures.**

3.2.1. All WR-ALC organizations storing classified material will use attached checklist (**Attachment 2**), when applicable. A copy of the checklist will be placed in an unclassified folder inside each safe.

3.2.2. During an emergency, secure classified only when time and circumstances permit before evacuating an area. Do not risk life or injury to secure classified material.

3.2.3. Re-enter a declared emergency area to recover/secure classified only when emergency response forces allow it. If, upon returning, classified material is missing or compromised, comply with AFI 16-1404_AFMCSUP, Chapter 7.

3.2.4. The WR-ALC Control Center is the primary contact point for the Complex. The WR-ALC security manager in WR-ALC Control Center is the secondary contact point. The WR-ALC Control Center or the WR-ALC security manager will notify the commander/deputy director and all WR-ALC groups if relocation occurs.

3.2.5. All groups storing classified material will keep a copy of this instruction in a convenient location for easy access. This instruction will not be stored inside the security container.

4. Personnel Security.

4.1. **In-processing.** All individuals (civilian and integrated DoD contractors) will in-process through the Security Office.

4.2. **Interim Security Clearances.** The Security Office will process new-hire personnel for an interim security clearance. A copy of the SF 86, *Questionnaire for National Security Positions*, will be provided to the Security Office for interim clearance processing.

4.3. **Periodic Re-investigations.** Personnel are required to complete questionnaires for security clearances as requested by Security every five years for both Secret and Top Secret clearances.

4.4. **Completed Investigation Package.** Security will assist in preparation and review the completed investigation package prior to submission.

4.5. **Unfavorable Information Received.** Supervisors and/or co-workers will immediately notify Security when unfavorable information is revealed which could have a direct impact upon an individual's security clearance eligibility IAW DoDM 5200.02, (i.e., driving under the influence, excessive indebtedness, criminal conduct, illegal drug use, etc.). Squadron directors will review, evaluate, and consider the situation and take any necessary action IAW DoDM 5200.02 and AFMAN16-1405 (formerly AFI 31-501).

4.6. **Oversight of Personnel Security Programs.** The WR-ALC Staff Security Office oversees the Personnel Security programs for all groups within the Complex. This does not relieve the security specialists assigned to the groups of performing daily tasks (e.g., in-and-out processing in DISS, indoctrination functions in DISS, etc.). Further, the issuing and retrieval of access badges used by these groups will be processed by the security personnel assigned to the group, not the Staff Security Office.

5. Industrial Security.

5.1. Classified Contract Preparation and Execution.

5.1.1. When contractor procurement requests are prepared for classified contracts, the Technical Program Manager, Program Manager (PM), or Contract Management Officer, in concert with Security, will identify program unique security requirements in solicitations and contract documents, to include drafting and incorporating program specific security classification guidance into the DD Form 254, *Department of Defense Contract Security Classification Specification*. DD Forms 254 will be coordinated through Security and 78 ABW/IP.

5.1.2. Contractor personnel performing classified operations governed by a DD Form 254 and assigned to WR-ALC (residing within the facility more than 90 days) are designated as an integrated visitor group and will abide by the long term VGSA. ***Note:*** Supervisors will report all long-term contractors to Security.

5.1.3. Integrated visitor groups will operate IAW DoDM 52.00.01 Volumes 1-4, AFI 16-1404_AFMCSUP, DODM5220.22V2_AFMAN16-1406V2, and supplemental guidance thereto, which is applicable under the terms of the executed VGSA. Integrated visitor groups will handle, generate, process, and store classified information per Air Force guidance. The exception is that their access is limited to need-to-know contract-specific classified performance information.

5.2. DD Form 254 Preparation.

5.2.1. During the solicitation phase of a contract, the PM will prepare a solicitation DD Form 254 for each classified contract, and coordinate with the contracting officer and Security. Security will route the draft DD Form 254 to 78 ABW/IP for approval and signature. Once signed by 78 ABW/IP, the PM will forward the DD Form 254 to contracting for signature.

5.2.2. Prior to a classified contract being awarded, the PM will prepare a DD Form 254 for the contract award. The DD Form 254 used for the solicitation phase cannot be used for contract award. The PM will forward the award DD Form 254 to Security, who in-turn forwards the DD Form 254 to 78 ABW/IP for approval and signature. Once the DD Form 254 is signed by 78 ABW/IP, the PM will forward the DD Form 254 to contracting for signature.

5.2.3. DD Form 254 and associated security classification guides will be reviewed every five years to ensure accuracy and currency. When changes are necessary, the contract will be modified, if appropriate, and revised guidance issued.

5.3. **In-processing Responsibility.** Security is responsible for in-processing all integrated contractor personnel for clearance verification/validation.

5.3.1. Security will ensure contractors are included in the semi-annual security self-assessment to ensure classified operations are complied with and are abiding by contract security requirements.

5.3.2. The PM will notify security when contractual services and/or performance has been completed or terminated. Security will out-process all integrated contractor personnel and will notify 78 ABW/IP.

6. Secret Internet Protocol Routable Network (SIPRNet) Operations.

6.1. **For those who do not leave SIPRNet terminals on continuously.** Per Installation Commander and 83rd Network Operating Squadron, 24th AF, SIPRNet terminals must be turned on every Tuesday and Wednesday from 0900 – 1500 to install patches and updates. If the SIPRNet terminal is not available on those days every week, they will be removed from the SIPRNet domain.

6.2. **SIPRNet Monitors.** SIPRNet monitors will be appointed, maintain a SIPRNet account, ensure token is protected, and maintain security clearance. SIPRNet monitors adhere to, ensure users are aware of procedures, and verify users' need-to-know. Individuals are responsible for the end-of-the-day security check and ensure room/area is clear of classified material.

7. Operations Security (OPSEC).

7.1. **OPSEC Defined.** The process of denying information to our adversaries about friendly capabilities and intentions by identifying, controlling, and protecting indicators associated with planning and conducting military operations and other activities in support thereof.

7.2. **OPSEC Events.**

7.2.1. OPSEC events consist of the inadvertent disclosure of critical information or OPSEC indicators that could jeopardize operations. OPSEC events can be identified as part of in-house surveys or discovered by any member of a unit who observes an event during day-to-day operations. Reporting a possible OPSEC event is not intended to assign blame or initiate punitive action. It is intended to highlight potential vulnerabilities, identify trends, and improve service-wide OPSEC posture.

7.2.2. Personnel who become aware of a possible OPSEC event will immediately report it to their chain-of-command and the Security Office.

7.2.3. Refer to AFI 10-701 for additional information and guidance on OPSEC.

7.3. **Critical Information.**

7.3.1. Definition: Critical information (CI) is information that is unclassified but sensitive. However, when CI is brought together with other information, it can be damaging to national security. All personnel are responsible for protecting CI.

7.3.2. Staff Security Office maintains a critical information list (CIL). The CIL can be found on Security SharePoint. It is also provided to all personnel as part of the initial and refresher training. All personnel must be fully aware of the contents of the CIL, its purpose, and the reasons CI must be protected at all times.

7.3.3. Discussions or transmissions of CI over non-secure media such as telephones, e-mails, facsimile, or in uncontrolled/unrestricted areas have been found to be a prime target for exploitation. Seemingly harmless information when combined with data from other conversations or documents could be classified, even though separately the pieces are unclassified. Always use secure means to discuss critical information (i.e., encrypt e-mail). Destroy related documents and working papers when no longer needed by shredding in an approved shredder.

8. Antiterrorism.

8.1. **Random Anti-terrorism Measure (RAM).** A dynamic and proactive RAM program visibly communicates the Command's resolve to prepare for and counter the terrorist threat. Unpredictability is the key to deterring terrorist attacks.

8.2. **RAM Unpredictability.** To maintain unpredictability, RAMs will be incorporated into daily operations at varying times during all force protection conditions. RAM exercises will be unannounced, and cooperation of all personnel is required.

9. Bomb Threat Procedures.

9.1. **Remain Calm.** When notification of a bomb threat is received by phone or courier, it is important to remain as calm as possible. Any overreaction may cause the caller to prematurely detonate the device or cause the device itself to detonate. Remaining calm also allows a person to focus on the gathering of information to pass on to law enforcement officials.

9.2. **Preserve written threats as evidence, if possible.** For phone call threats, try to prolong the conversation to obtain pertinent information. Initiate AF Form 440, *Bomb Threat Aid*.

9.3. **Notify 911.** While the caller is still on the phone, immediately notify a co-worker to call 911 and inform them of the telephone number the threat was phoned in on, the building number, and location/area involved.

9.4. **DO NOT HANG UP THE TELEPHONE RECEIVER.** Replace the phone receiver only when instructed to do so by 911 Operator.

9.5. **Evacuate.** Evacuate the facility using the designated evacuation plan posted on or near building entrances and room doors. Ensure that evacuation point is not in close proximity to the facility.

9.6. **Do not turn lights/equipment on or off.**

9.7. **Do not use cell phones or radios in the immediate area (300-foot radius).**

9.8. **Make sure classified material is secured.** However, safety is of paramount importance and under no circumstance shall anyone jeopardize his/her safety to safeguard classified information. Refer to applicable emergency classified handling procedures.

9.9. **Notify chain of command.**

9.10. **Assist Security Forces (SF) unit response, as requested.**

10. Unattended Suspicious Package.

10.1. **Definition:** An unattended package can be defined as any package (suitcase, box, backpack, etc.) left unattended.

10.2. **Unattended/suspicious package procedures.**

10.2.1. Evacuate the immediate area/room and post guards, as necessary, to prevent access to the affected area/facility until properly relieved by SF personnel.

10.2.2. Do not open or handle the package.

10.2.3. Do not turn lights/equipment on or off.

10.2.4. Do not use cell phone or radios in the immediate area of package (300-foot radius).

10.2.5. Make sure classified material is secured.

10.2.6. Notify chain of command, as appropriate.

10.2.7. Call 911 and notify them of an unattended package.

10.2.8. Have an individual (preferably the individual who found the unattended package) meet SF responding units to identify the location and the package itself.

11. Continuing Security Education, Training, and Awareness.

11.1. **Annual Security Training.** Security training for all government employees and contractors will be conducted semi-annually utilizing the EIMC.

11.2. **Managing Training Requirements.** The Security Office will initiate training in EIMC and the system will send an automated e-mail with training requirements. The system will automatically track training completion dates, eliminating the need to print and maintain certificates.

11.3. **Training for New Personnel.** Newly assigned personnel to the organization must receive initial security orientation training via EIMC within 30 days of arrival or prior to accessing classified information, whichever comes first.

12. Foreign Travel Briefings and Reporting.

12.1. **Notification of Foreign Travel.** All personnel will contact Security 30 days prior to traveling outside the U.S., to include Mexico, Bahamas and Canada, for official or unofficial travel. The employee will complete the Air Force Office of Special Investigation foreign travel questionnaire located on the AF Portal. In addition, all travelers will review electronic foreign clearance guide to ensure all Aircraft and Personnel Automated Clearance System requirements have been met, if required. ***Note:*** All Special Access Program (SAP)/Sensitive Compartmented Information indoctrinated personnel have additional foreign travel reporting requirements through their respective Government SAP Security Officer Special Security Representative. The SM will add the foreign travel into DISS upon members return.

12.2. **Reporting Contact with Foreign Individuals.** Personnel will report to Security contacts with individuals of any nationality within or outside the scope of the employee's official activities when: illegal or unauthorized access is sought to classified or sensitive information and individuals are concerned they may be the target of exploitation by a foreign entity.

13. In-and Out-Processing.

13.1. **In-processing New Personnel.** Supervisors will ensure all new-hire and reassignment personnel in-process through the Security Office. They will be indoctrinated to appropriate security access in DISS and complete all initial new hire security training before having access to classified information.

13.2. **Debriefing Out-processing Personnel.** Security will debrief all individuals (civilians) with security clearance eligibility when they depart the organization (i.e., separation, termination, retirement, permanent change of station, permanent change of assignment) or have their security clearance terminated or administratively withdrawn. An AF Form 2587, *Security Termination Statement*, will be used to document the debriefing.

13.3. **Out-Processing Personnel.** Security will out-process all personnel in DISS and notify the 78 ABW/IP office to out-process personnel departing the base.

JON A. EBERLAN
Brigadier General
Commander

Attachment 1

GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

References

AFI 10-701, *Operations Security (OPSEC)*, 24 July 2019, *Incorporating Change 1*, 9 June 2020

AFI16-1404_AFMCSUP, *Air Force Materiel Command Information Security Program, Certified Current, 4 August 2020*

AFPD 16-14, *Security Enterprise Governance*, 31 December 2019

DoDI 5200.48_DAFI16-1403, *Controlled Unclassified Information*, 5 October 2021

DODM 5220.32v1, *National Industrial Security Program: Industrial Security Procedures for Government Activities*, 1 August 2018, *Incorporating Change 2, 10 December 2021*

AFMAN 17-1301, *Computer Security (COMPUSEC)*, 12 February 2020

DAFI 90-160, Publications and Forms Management, 14 April 2022, *Incorporating Change 1*, 21 June 2023

AFI 33-322, *Records Management and Information Governance Program,* 23 March 2020, *Incorporating Change 1,* 28 July 2021

DoDI O-2000.16, Vol 1, DoD Antiterrorism (AT) *Program Implementation: DOD Antiterrorism Standards*, 17 November 2016, Change 3, 7 May 2021

DoDM 5200.01, Volume 1, *DoD Information Security Program: Overview, Classification, and Declassification*, 24 February 2012, Incorporating Change 2, 28 July 2020

DoDM 5200.01, Volume 2, *DoD Information Security Program: Marking of Information*, 24 February 2012, Incorporating Change 4, 28 July 2020

DoDM 5200.01, Volume 3, *DoD Information Security Program: Protection of Classified Information*, 24 February 2012, Incorporating Change 3, 28 July 2020

DoDM 5200.02, *DoD Procedures for the DoD Personnel Security Program (PSP)*, 3 April 2017, Incorporating Change 1, 29 October 2020

Executive Order 13526, *Classified National Security Information*, 29 December 2009

ISOO, *Marking Classified National Security Information*, December 2010; Revision 4, January 2018

DoDD 5400.07, *DoD Freedom of Information Act (FOIA) Program*, 5 April 2019

Part 2002 of Title 32, *Code of Federal Regulations (CFR), Controlled Unclassified Information* (CUI)

Adopted Forms

AF Form 310, *Document Receipt and Destruction Certificate*

AF Form 2587, *Security Termination Statement*

DAF Form 847, *Recommendation for Change of Publication*

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

DD Form 2501, *Courier Authorization*

DD Form 2825, *Internal Receipt*

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

SF 86, *Questionnaire for National Security Positions*

SF 312, *Classified Information Nondisclosure Agreement*

SF 700, *Security Container Information*

SF 701, *Activity Security Checklist*

SF 702, *Security Container Check Sheet*

PS Form 3811, *Domestic Return Receipt*

PS Form 3877, *Firm Mailing Book for Accountable Mail*

USPS Label 200, *Registered Mail Label*

Abbreviations and Acronyms

78 ABW/IP—78th Air Base Wing Information Protection

AF—Air Force

AFI—Air Force Instruction

AFMAN—Air Force Manual

AFMC—Air Force Materiel Command

AT—Antiterrorism

BITC—Base Information Transfer Center

CC—Commander

CFR—Code of Federal Regulations

CI—Critical Information

CIL—Critical Information List

COMPUSEC—Computer Security

CONUS—Continental United States

CUI—Controlled Unclassified Information

DCM—Deputy Commander for Maintenance

DD—Department of Defense

DISS—Defense Information System for Security

DoD—Department of Defense

DoDD—Department of Defense Directive

DoDI—Department of Defense Instruction

DoDM—Department of Defense Manual

DD—Deputy Director

EIMC—Employee Information Management Center

FOIA—Freedom of Information Act

FOUO—For Official Use Only

GSA—General Services Administration

GSSO—Government SAP Security Office

IAW—In Accordance With

ISOO—Information Security Oversight Office

ISPM—Information Security Program Management

NOSC—Network Operating Squadron

OF—Optional Form

OPSEC—Operations Security

OPR—Office of Primary Responsibility

PC—Pocket Computer

PED—Portable Electronic Device

PII—Personal Identifiable Information

PM—Program Manager

PS—Postal Service

PSP—Personnel Security Program

RAFB—Robins Air Force Base

RAM—Random Antiterrorism Measure

RF—Radio Frequency

SAP—Special Access Program

SCI—Sensitive Compartmented Information

SF—Standard Form

SF—Security Force

SIPRNet—Secret Internet Protocol Routable Network

SM—Security Manager

SSN—Social Security Number

SSR—Special Security Representative

USPS—United States Postal Service

VGSA—Visitor Group Security Agreement

WR-ALC—Warner Robins Air Logistics Complex

WR-ALC/OMD—Warner Robins Air Logistics Complex Readiness Section

Attachment 2

EMERGENCY PROTECTION AND REMOVAL OF CLASSIFIED MATERIAL CHECKLIST

Table A2.1. Emergency Protection and Removal of Classified Material Checklist.

Primary/Alternate Safe Custodian or Responsible Official will:	
___	Increase vigilance during heightened and/or threatening conditions.
___	Ensure all classified material is properly secured (without risk of injury or loss of life) before leaving the area when evacuation of building or area is necessary.
___	When directed, be prepared to relocate classified material.
If Relocation of Classified Material is Required:	
___	Place documents to be transported to relocation site in cardboard boxes or other suitable containers. Mark organizational symbol on the outside of the container. DO NOT mark the outside containers with security classifications, (i.e. Secret) when transporting classified material.
___	Seal and/or lock the containers.
___	Physically accompany containers containing classified material to relocation site. Use private vehicles or government transportation as necessary.
___	Ensure responsible individual or organization official will assume charge of material. Ensure classified material reaches the destination, is properly accounted for, and is secured or released to an authorized individual.
Upon Return-to-Work Area:	
___	Review all classified material as soon as re-entry is authorized by emergency response forces.
___	If all classified was not relocated due to time factor, and unauthorized access is apparent and/or there is missing or compromised classified material, notify the Security Assistant and comply with AFI 16-1404_AFMCSUP, Chapter 7.