BY ORDER OF THE COMMANDER
635TH SUPPLY CHAIN OPERATONS WING

635TH SUPPLY CHAIN OPERATIONS WING INSTRUCTION 16-1404

13 JUNE 2022

Operations Support

INFORMATION SECURITY

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

ACCESSIBILITY: This publications and forms are available on the e-Publishing web site at www.e-Publishing.af.mil for downloading

RELEASABILITY: There are no releasability restrictions on this publication

---

OPR: 635SCOW/OM

Certified by: 635SCOW/CC
(Colonel Chad R. Ellsworth)

Supersedes: 635SCOWI 16-1404, 1 March 2017

Pages: 38

This Instruction (I) establishes policy, procedures and responsibilities for implementation of the Information, Personnel, and Industrial Security Programs within 635 SCOW per DoDM5200.01V1_AFMAN16-1404V1, *Information Security Program: Overview, Classification and Declassification;* DoDM5200.01V2_AFMAN16-1404V2, *Information Security Program: Marking of Classified Information;* DoDM5200.01V3_DAFMAN16-1404V3, *Information Security Program: Protection of Classified Information* and AFI16-1401, *Information Protection.* The OI supplements the referenced directives (Attachment 1) and applies to all personnel (military, civilians and on-site contractors) assigned, detailed, dedicated, or collocated to 635 SCOW. All assigned personnel will adhere to the published security guidance/requirements and are responsible for the protection of classified and controlled unclassified information (CUI).

Ensure 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) 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 instruction requires collecting and maintaining information protected by the Privacy Act of 1974 authorized by Title 10, U.S.C., Section 8013 IAW AFI 33-332, Air Force Privacy Program. Personnel who fail to adhere to this guidance may be punished under the Uniform Code of Military Justice (UCMJ) Article 92(1) or civil equivalent.

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.

SUMMARY OF CHANGES

This Instruction was substantially revised and should be completely reviewed. Major changes include updating the required security systems from Joint Personnel Adjudication System (JPAS) to current system of record Defense Information Security System (DISS). Updates have been made to the Special Security Officer (SSO) to Tinker AFB and removal of Maxwell-Gunter AFB information.

1. Duties and Responsibilities.

1.1. 635 SCOW Commanders Responsibilities.

1.1.1. Ensure implementation of the Unit's security program

1.1.2. Appoint a primary and alternate Unit Security Manager (SM) in writing to 375 AMW Information Protection Office.

1.1.3. Review and approve annually, Security Access Requirement (SAR) codes for each position within the organization.

1.1.4. Approve (or delegate authority) pre-employment waivers/interim security clearances.

1.1.5. Establish SIFs when required.

1.2. Security Managers responsibilities.

1.2.1. Establish/implement policies and procedures of the Unit's Information, Personnel, and Industrial Security Programs.

1.2.2. Serve as the unit focal point to the 635 SCOW.

1.2.3. Attend IP Security Manager (SM) Training within 90 days of appointment.

1.2.4. Develop and update an internal unit security operating instruction (OI) when directed by changes in policies, procedures and guidance.

1.2.5. Maintain a SM Handbook. Use the proper format as outlined by 375 AMW/IP. The handbook format is located in the 635 SCOW Share Drive.

1.2.6. Ensure initial and annual security education training is conducted and documented, to include North Atlantic Treaty Organization (NATO) Security Awareness training.

1.2.7. Process incoming and outgoing collateral classified visit requests.

1.2.8. Ensure annual Information Protection security self-assessments are conducted timely and accurately summarize the status of the unit's security program.

1.2.9. Review and process challenges in classification decisions and notify originators of improperly marked classified documents.

1.2.10. Attend semiannual SM meetings hosted by the Base IP. The alternate SM or an organizational representative will attend in the absence of the primary SM.

1.2.11. Ensure SM visual aid is current and posted throughout the unit.

1.2.12. Report security incidents to Host Base IP office and monitor security incident preliminary inquiries and formal investigations involving classified information.

1.2.13. Manage the Defense Information System for Security (DISS), and Unit Manning Document (UMD) to ensure security clearance data is effectively tracked.

1.2.14. Direct personnel to complete security clearance investigations and periodic reinvestigations (PR) as required.

1.2.15. Review completed SF-86 for completeness prior to submission to Wing IP.

1.2.16. Develop plans for the protection, removal, or destruction of classified material in case of fire, natural disaster, civil disturbance, terrorist activity, or enemy action, to minimize the risk of compromise (**Attachment 2**).

1.2.17. In-process and out-process assigned unit personnel.

1.2.18. Notify host base IP for initial and follow-up physical security surveys when requesting classified open storage or when new facility design plans require classified open storage. Coordinate a Structural Survey Assessment with host base CES to determine agency construction requirements and costs. For existing approved classified vaults and/or secure rooms that require structural changes (i.e., CE drilling into the wall to install a conduit or communication lines, etc.), notify host base IP immediately.

1.3. **Individual Supervisors and Coworkers Responsibilities.**

1.3.1. Continually monitor and evaluate personnel with clearances for indicators that may signal matters of personal concern that could potentially affect National Security in accordance with (IAW) the Security Executive Agent Directive 4 (SEAD 4), *National Security Adjudicative Guidelines*.

1.3.2. IAW SEAD 3, Reporting Requirements for Personnel with Access to Classified Information or Who Hold a Sensitive Position. Report to the 635 SCOW Commander or SM any conduct or information that may affect an individual's trustworthiness, reliability, or loyalty in protecting classified information (i.e., drug use, alcohol abuse, excessive debt, criminal conduct, foreign influence, etc.).

1.3.3. Appoints a primary and alternate safe custodian for all classified material stored within their section.

1.3.4. Ensure new unit members receive initial security training within 90 days upon arrival and annually.

1.3.5. Review position sensitivity/access adequacy periodically or upon vacancy/duty changes.

1.3.6. Ensure security tasks (i.e., end-of-day security checks) are conducted correctly and timely and annotated as required.

1.4. **All Personnel Responsibilities.**

1.4.1. Be familiar with all provisions of this Instruction.

1.4.2. Submit security clearance updates at required intervals.

1.4.3. Be alert to the presence or absence of classified information in the work area and immediately report security incidents to the SM, immediate supervisor, or 635 SCOW Commander.

1.4.4. Challenge strangers in the work area; find out who they are and what business they have there.

1.4.5. Report contact with individuals of any nationality in which:

1.4.5.1. Illegal or unauthorized access to classified or sensitive information is requested.

1.4.5.2. The employee is concerned they may be the target of exploitation by a foreign entity.

2. Personnel Security Program.

2.1. **Granting Access.**

2.1.1. Granting access to classified material is the responsibility of the person who has authorized possession, knowledge, or control of the material. Before granting access, the following criteria must be met:

2.1.1.1. The individual possesses a valid security clearance at or above the level of the classified material.

2.1.1.2. The individual's official duties require a need-to-know or access to the classified material.

2.1.1.3. The individual has signed a SF 312, *Classified Information Nondisclosure Agreement*.

2.1.2. In addition to the above criteria ensure the individual has been appropriately in-briefed with appropriate program offices prior to granting access (i.e., SAP, SCI, CNWDI, NATO, etc.).

2.1.3. The SM will use the Classified Access Memorandum Letter to document U.S. classified access and AF Form 2583, *Request For Personnel Security Action*, to document CNWDI and NATO accesses and other mission essential caveats. SAP and SCI security representatives will record briefings IAW their standard operating procedures. The 635 SCOW SSO POC for SCI is located at Tinker AFB.

2.1.4. The Commander may grant interim access (Top Secret or Secret) provided the following actions are taken:

2.1.4.1. Appropriate security clearance investigation is submitted to the Defense Counterintelligence and Security Agency (DCSA).

2.1.4.2. Commander reviews the individual's SF 86, *Questionnaire for National Security Positions*, for adverse activity, conduct, or behavior that would affect a person's ability to protect classified information and maintain security clearance eligibility.

2.1.4.3. SM conducts a local files check with the local Medical Group and Security Forces Squadron Reports and Analysis.

2.1.4.4. SM completes an Interim clearance letter based on a favorable review of the SF 86 and local files check and obtains Commander approval and signature.

2.1.4.5. SM has individual read and sign SF 312, Classified Non-disclosure Agreement (NdA), and forwards to appropriate office. SM annotates DISS that an NdA was accomplished.

2.1.4.6. SM annotates the appropriate temporary interim classified access in DISS after providing the classified access briefing.

2.2. **Personnel Security Investigation Submissions.**

2.2.1. SM will manage individual time lines for required personnel security investigation (PSI) submissions. Other actions consist of establishing/coordinating Incident Reporting with the Commander and First Sergeant, and processing Statement of Reasons (SORs), Requests for Information (RFIs) and Suitability Determinations generated by the DOD Consolidated Adjudication Facility (DOD CAF)

2.2.2. The SM will track, notify, and assist individual(s) with completion of their PSI for timely submission. The timeline for updating PSIs are as follows:

2.2.2.1. Individuals requiring access to SAP Top Secret (Tier 5R) or Secret (Tier 3R) information must submit their periodic reinvestigation every 6 years. Initiate either reinvestigations 5 years and 9 months from the date of their previous investigation or reinvestigation.

2.2.2.2. Individuals requiring access to Top Secret/SCI Sensitive or Top Secret must update their investigation every 6 years. Initiate a Top Secret (Tier 5R) 5 years and 9 months from the date of the previous investigation or reinvestigation.

2.2.2.3. Individuals requiring access to Secret information must update their investigation every 10 years. Initiate a Secret (Tier 3R) 9 years and 9 months from the date of their previous investigation or reinvestigation. The **Electronic Questionnaires for Investigations Processing (e-QIP)** must cover the most recent 10-year period or the period since the last investigation.

2.2.2.4. Personnel requiring a Tier 5 initial investigation (formerly known as a Single Scope Background Investigation [SSBI]) or an upgrade from a previous clearance (i.e., you presently hold a secret clearance and because of a duty position change, your position requires a top secret clearance) will coordinate the upgrade with the unit manpower office and the SM processing the request. Interim Top Secret clearances may be requested and processed through the SM after submission of the security clearance paperwork to DCSA.

2.2.2.5. SM will not submit an individual for a T5/T5R investigation without verifying the need for TS or SCI eligibility for current position or is in receipt of PSC/PSA RIP with TS or SCI requirement.

2.2.2.6. Personnel will have 10 calendar days to complete the Electronic Questionnaire for Investigation Processing (eQIP) once initiated by IP.

2.2.2.7. SM will not submit an individual for Periodic Reinvestigation if that individual is within 12 months of separation/retirement. Eligibility and access will persist until separation, or credible disqualifying information becomes known.

2.3. **Clearance Verification.** Use DISS to verify individual security clearance eligibility; DISS is maintained by the SM.

2.4. **Points of Contact.** The SMs are the only authorized points of contact with the host base IP office. Direct security questions through the SM.

2.5. **Continuous Evaluation Program (CEP).** Each individual is responsible to continually evaluate a person's trustworthiness, loyalty and reliability in protecting classified information. Report all adverse information regarding employees, yourself and co-workers to the Commander or Director, your supervisor, or SM immediately.

2.5.1. Commander or Director and Supervisor Responsibilities: Evaluate adverse activity, conduct and behavior with respect to a person's security clearance eligibility IAW the Security Executive Agent Directive 4 (SEAD 4), *National Security Adjudicative Guidelines*.

2.5.2. Co-worker Responsibilities: Report unfavorable or adverse information to the Commander or Director, supervisor, or SM.

2.5.3. Individual Responsibilities: Avoid unfavorable conduct and behavior. Report all contact with individuals of any nationality when unauthorized access to classified or sensitive information is sought or you believe you are a possible target for exploitation by a foreign entity.

2.5.4. Helping Agencies are available to assist individuals in need. Contact the First Sgt and/or SM for a list of referral agencies.

2.6. **Incident Reporting (IR).** IR is a collection of documents generated because of the discovery or development of unfavorable information, which brings into question a person's continued eligibility for a security clearance or access to SCI and SAP. IR may be established by the Commander or Director or by DOD CAF. IR serves as a repository for unfavorable or derogatory information, which requires further review, evaluation, or investigation to resolve any outstanding administrative or adjudicative concerns. The establishment of IR may result in the suspension or revocation of an individual's security clearance. The SM will act as the organization's liaison between the member and the base IP office.

2.7. **Foreign Travel.** Military/civilian/contractor personnel traveling outside Scott AFB for official or leisure travel must conduct travel briefings with the appropriate agencies at least 30 days prior to travel

2.8. **Debriefing Access.** Military/civilian/contractor personnel must be debriefed from all accesses using AF2587 and owning/servicing relationships removed from DISS by SM prior to departure.

2.8.1. Once access is debriefed in DISS, no further access to classified information/areas is permitted

2.8.2. Open incidents must be forwarded to gaining organization or closed with DoDCAF.

3. Information Security Program.

3.1. **Policy:** It is the policy of unit personnel to identify, classify, downgrade, declassify, mark, protect, and destroy its classified information and material consistent with national and higher headquarters policy. This general policy statement also applies to controlled unclassified information (CUI) under the purview of relevant statutes, regulations, and directives.

3.2. **Security Program Management.** The SM will be listed on the unit's in and out-processing checklist and all assigned personnel will in-process through the security office immediately upon arrival and out-process prior to departing the organization.

3.2.1. In-Processing.

3.2.1.1. SM will use the appropriate in and out-processing checklist to ensure all security actions are completed prior to any individual receiving access to classified information.

3.2.1.2. Complete a Monthly Classified Access Memorandum Letter and obtain 635 SCOW Commander or Director signature for recently assigned military and civilian personnel who require access to classified information. Enter appropriate classified access into DISS.

3.2.1.3. Prior to individuals accessing classified information, initiate actions to complete a Standard Form (SF) 312, *Classified Information Nondisclosure Agreement (NdA)*, when there is no NdA date annotated in DISS. Forward SF 312 to the appropriate agency and annotate the date completed in DISS. When a person refuses to sign an NdA, the Commander will deny the individual access to classified information and complete actions outlined in DoDM 5200.01, Vol 3_AFMAN 16-1404, Vol 3.

3.2.1.4. All military and DoD civilians assigned to the unit must be incorporated into DISS for a complete accountability of personnel and to ensure the individual meets all prerequisites for access to classified information. This is necessary in acquiring individual ownership when a new employee arrives on station. DoD Contractors assigned to the unit will be serviced in DISS.

3.2.1.5. Verify the individual's position code on the UMD and DISS to ensure the individual possesses the correct security clearance and accesses for the position they occupy. Initiate actions for individual security clearances out-of-scope. Process interim clearances and interim computer access waivers when required.

3.2.1.6. Coordinate and verify security clearance eligibility on DD Form 2875, *System Authorization Access Request*, and forward to the unit Cyber Security Liaisons (CSLs)

3.2.2. Out-Processing.

3.2.2.1. Debrief individuals with security clearance eligibility when they terminate civilian employment, PCS, retire, or separate from military service. Use AF Form 2587, *Security Termination Statement,* to debrief personnel and remove access levels in DISS.

3.2.2.2. Debrief individuals with access to Advanced Programs such as Critical Nuclear Weapons Design Information (CNWDI), North Atlantic Treaty Organization (NATO), Restricted Data (RD), and remove their access levels in DISS. Use AF Form 2587 to debrief personnel.

3.2.2.3. Ensure individuals indoctrinated into SCI are debriefed by the respective Special Security Officer (SSO) before their base final out-processing appointment, or their SCI accesses are transferred-in-status for those individuals going to different organizations requiring SCI access. 635 SCOW SSO is located at AFSC Tinker AFB and will work with AMC SSO for debriefing SCI access.

3.2.2.4. Retrieve Contractor Common Access Card (CAC), and work with TASS POC to revoke from the Trusted Association Sponsorship System (TASS) and turn into the local Military Personnel Section (MPS).

3.2.2.5. Release ownership of unit personnel (military and civilian) from DISS when they depart the organization (PCS, TDA, terminate employment, separate, etc.). Remove the servicing relationship for all departing contractors.

3.3. **Security Education and Training Requirements.**

3.3.1. Assigned unit individuals, including assigned contractors, will attend initial security training within 90 days upon arrival to the organization and participate in recurring security training annually.

3.3.2. All cleared personnel with a security clearance are designated as derivative classifiers. Derivative classification training is incorporated into the unit's initial and annual training curriculum. Therefore, all cleared individual's in the unit will participate in the training initially upon assignment and annually thereafter.

3.3.3. SM will ensure all personnel are current on myLearning courses with the unit Training Manager.

3.3.4. SM will track/document the training and follow-up with appropriate personnel/supervisors of individuals who are non-compliant.

3.4. **Security Self-Assessment.**

3.4.1. Conduct the security self-assessment during the unit's scheduled annual self-assessment (May).

3.4.2. Use the Information Protection self-assessment checklist to conduct and document the security self-assessment.

3.4.3. SM will track all findings and document corrective actions approved by the Commander.

3.4.4. SM will file the approved corrective actions in the SM Handbook.

3.5. **Handling, Safeguarding, and Storage of Collateral Classified Information.**

3.5.1. Whenever handling a classified document outside of a security container, it must always be under continuous observation and control. When not actively using that document, ensure it has the appropriate cover sheet.

3.5.2. Prior to the release or disclosure of any classified material, custodians will ensure the individual has a security clearance equal to or above the level of the information being released, a need-to-know to perform their assigned duties and have a signed SF 312 on file.

3.5.3. Work with or discuss classified information only in classified processing areas. Never will anyone read, discuss, or work with classified information in any common areas, such as lobbies, hallways, patios, smoking areas, or any other unsecured area.

3.5.4. Classified information or material will NOT be removed from officially designated offices or work areas during non-duty hours.

3.5.5. Storage of Classified Materials.

3.5.5.1. Only store classified material in GSA approved security containers (i.e., vaults, safes, etc.) to prevent unauthorized access or compromise.

3.5.5.2. Under no circumstances will funds, weapons, medical items, controlled drugs, precious metals, or any other item of value be stored in a security container with classified material.

3.5.6. The security container custodian as listed on SF 700, *Security Container Information.* The safe custodian will change combinations to security containers. Change combinations:

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

3.5.6.2. Whenever an individual knowing the combination no longer require access, unless other sufficient controls exist to prevent that individual's access to the lock.

3.5.6.3. When compromise of the combination is suspected (i.e., the container was left unsecured).

3.5.6.4. When maintenance is performed by someone other than the custodian.

3.5.6.5. When the container, vault, or secure room is taken out of service or is no longer used to store classified information.

3.5.7. When placed out of service custodians will ensure all safes are purged of their contents and the combination reset to the standard factory setting of 50-25-50. Prepare a 3x5 card and annotate the following information: "The container has been inspected and does not contain any classified material. The lock is set on standard combination (50-25-50)." The safe custodian will date; print his/her name, organization, and phone number, and sign the card. The card will be affixed to the outside of the container.

3.5.8. Change container combinations annually when storing NATO classified information.

3.5.9. Restrict combinations for classified storage containers to appropriately cleared personnel who are authorized access to the classified material stored therein. List and post on the outside of the security container, those personnel authorized access. List will be reviewed and updated as need by the Safe Custodian and clearance will be verify by the Security Manager.

3.5.10. Security container custodians will notify the SM for guidance, if there is a security container with an inoperative combination lock or lockout. Replace inoperative combination locks with KABA-MAS X-10 combination lock for security containers.

3.5.11. Work-centers who store classified information will designate a primary and alternate custodian for each security container. Coordinate associated paperwork with the SM.

3.5.11.1. Use SF 700 to identify the security container custodians.

3.5.11.1.1. SF 700, Part I, is not classified, but contains personally identifiable information (PII) that must be protected by sealing in an opaque envelope conspicuously marked "Security Container Information" on the outside of the envelope. Post the SF 700, Part I, inside the locking drawer of the container or on the inside of the door for vaults, secure rooms and secure classified discussion rooms.

3.5.11.1.2. Record and seal combinations to security containers on SF 700, Part 2. SF 700, Part 2, is classified and must be marked at the top, bottom, front and back with the highest classification level of contents maintained in the container. The classification authority block should be marked:

3.5.11.1.2.1. Classified By: See SF 700, Block 10

3.5.11.1.2.2. Derived From: 32 CFR 2001.80(d)(3)

3.5.11.1.2.3. Declassify On: Upon change of combination

3.5.11.1.3. Either the Part 2 will be stored in another safe other than the one it is intended for or the SM will be responsible for the storage of safe combinations located in the unit. Exception: Safe combinations to COMSEC safes are retained within the COMSEC safe and not collateral safes.

3.5.11.2. Use Optional Form 89, *Maintenance Record For Security Containers / Vault Doors*, to record security container maintenance. OF 89 replaces AFTO Form 36, *Maintenance Record for Security Type Equipment*; however, maintain AFTO Form 36 (for historical purposes) along with OF 89 inside the locking drawer of the safe or on the inside of vault doors or secure rooms. NOTE: Do not record combination changes on the OF 89.

3.5.11.2.1. Operational Visual Inspections (OVI) are required of all security containers (safes and vaults) and container locking mechanisms initially and every 5 years. Use the OVI checklist in DoDM 5200.01, Vol 3_AFMAN 16-1404, Vol 3, Appendix 2 to Enclosure 3, to conduct the inspection.

3.5.11.2.2. The safe custodian is responsible for performing the OVI.

3.5.11.2.3. The inspector will annotate the OVI on the OF 89.

3.5.11.3. Use SF 702, *Security Container Check Sheet*, to record each opening, closing, and checking of security containers, safes, secure storage areas, and vaults.

3.5.11.3.1. Use a new SF 702 at the beginning of the month for each security container (i.e., 1 Jan - 31 Jan, 1 Feb - 28 Feb, etc.).

3.5.11.3.2. Destroy SF 702 one (1) month after all entry spaces are used and replaced by a new log if no longer required (collateral areas only).

3.5.11.4. Use the SF 701, *Security Activity Checklist*, when conducting end-of-day security checks. Destroy SF 701s one (1) month after all entry spaces are used and replaced by a new log if no longer required (collateral areas only).

3.5.12. End-of-Day Security Checks. Each work-center processing and/or storing classified material will establish and perform end-of-day security checks (**Attachment 3**).

3.5.13. After Duty Hours Classified Storage Locations. Should an occasion arise where classified material requires secure storage after duty hours, a 24-hour drop-off for classified (up to Secret) is available at the following locations:

3.5.13.1. Command Post, Bldg #470, 375 AMW/CP, DSN Phone #576-5891 (collateral classified only).

3.5.13.2. HQ AMC/A2 – Senior Intelligence Duty Officer, *Bldg #3189, DSN Phone #779-4781* (for SCI only).

3.5.14. Controlled Unclassified Information (CUI).

3.5.14.1. Properly safeguard CUI to prevent unauthorized disclosure. Use cover sheets when appropriate and secure in a locked file cabinet or desk. A locked office suffices.

3.5.14.2. Encrypt all sensitive and critical information when transmitting via unsecured means (i.e., NIPRNet, fax, etc.). Use DoD SAFE (Secure Access File Exchange) to encrypt and transmit sensitive unclassified information to our industry partners or individual's without encryption capability.

3.5.14.3. Do not transmit sensitive information from Government computer systems to personal home computers (e.g., program & system passwords, CUI, PII [SSNs], etc.).

3.5.14.4. Under NO circumstance should you connect any universal serial bus device to Government computers (including Government laptops). Items include cell phones, battery chargers, cameras, thumb drives, MP3 players, removable hard drives, etc. Anyone failing to comply with established procedures will lose their network privileges until administrative and training requirements are complete. Contact the unit CSL to obtain exceptions and waivers.

3.5.14.5. Unclassified and sensitive information no longer needed must be shredded.

3.6. **Classification Management.**

3.6.1. Only an Original Classification Authority (OCA) can originate classified information. The Commander is designated an OCA up to the secret classification level. Unit personnel must obtain a classification evaluation from the OCA when they develop information believed to be classified.

3.6.2. Mark classified documents and removable Automated Information System (AIS) storage media according to regulatory guidance provided in DoDM 5200.01, Vol 2_AFMAN 16-1404, Vol 2. **The document originator bears the responsibility for proper document markings.**

3.6.3. All classified material received must be immediately reviewed for correct markings before filing or transmitting to another organization. Classified material should be returned to the originator if the markings are not IAW DoDM 5200.01, Vol 2_AFMAN 16-1404, Vol 2, marking procedures. If returning the material would impede operations, send a letter to the originator listing the improper markings and request a corrected copy or instructions to correct the current copy. If a correction letter is received, a copy is kept with the document until corrective actions are taken.

3.6.4. All classified AIS storage media and devices will be either marked with a SF 707, Secret label; SF 708, Confidential label; SF 710, Unclassified label; or SF 902, CUI label (i.e., use the appropriate labels on computer peripherals, hard drives and storage cases; hand print the classification level on CDs/DVDs by using a permanent marker).

3.6.5. The originator/owner of material generated on a classified computer system will mark it with the appropriate classification.

3.6.6. Classified working papers are protected and destroyed IAW DoDM 5200.01, Vol 3_AFMAN 16-1404, Vol 3. Working papers are documents (e.g., notes, drafts, prototypes) or materials, regardless of the media, created during the development and preparation of a finished product. Working papers and materials are not intended or expected to be disseminated. Working papers and materials containing classified information shall be:

3.6.6.1. Dated when created.

3.6.6.2. Marked with the highest classification of any information contained therein and safeguard as required for the assigned classification.

3.6.6.3. Conspicuously marked "Working Paper" on the cover and/or first page of the document or material (or comparable location for special types of media) in larger than existing text.

3.6.6.4. After 180 days (30 days for SAP) or when released outside the originating activity, mark and control as a finished product; otherwise, destroy.

3.6.7. Classified material believed to be improperly or unnecessarily classified should be challenged IAW DoDM 5200.01, Vol 1_AFMAN 16-1404, Vol 1. Challenges to classification are processed through the SM.

3.6.8. Foreign government documents are marked IAW, DoDM 5200.01, Vol 2_AFMAN 16-1404, Vol 2.

3.6.9. Notify the SM of all classified holdings over 25 years old. The SM will assist in a systematic review of these holdings along with the Scott AFB Declassification Office.

3.7. **Transmission, Receipt and Control of Classified Information.**

3.7.1. The Unit's mail representative office is the focal point for receiving/dispatching all classified material on behalf of the unit.

3.7.2. Treat all received United States Postal Service (USPS) registered, First Class, Certified, or Express carrier mail packages as classified until deemed otherwise. Store classified packages in a GSA approved safe, until the intended mail recipient receipts for the package.

3.7.3. For transmission methods of Top Secret, Secret, and Confidential information, see DoDM 5200.01, Vol 3_AFMAN 16-1404, Vol 3.

3.7.3.1. To ensure USPS never leaves unattended material, do not execute the "waiver of signature and indemnity." A signature must be obtained at destinations end to ensure the classified is receipted for and protected at the final destination.

3.7.3.2. AF Form 310, *Document Receipt and Destruction Certificate*, is not required for Confidential information, unless its use is prescribed by an approved Special Access or Advanced Program.

3.7.4. AF Form 310 must be used when sending Secret material through registered mail channels and hand-to-hand transfers.

3.7.5. Personnel preparing classified mail for transmission to a contractor will ensure the contractor facility is cleared to receive the mail. Call the SM to obtain the contractors cleared facility mailing address (provide cage code, if known).

3.7.6. Only cleared personnel will deliver, transmit, or receive classified messages and accountable mail. Personnel authorized to perform these duties will comply with applicable telecommunication and mail regulations.

3.7.6.1. SM will establish and maintain a document receipt file and perform tracer actions when necessary. Send a tracer when the receipt is not returned within 15 business days for classified material sent within the CONUS and 30 business days for classified material sent outside the CONUS. Report all security incidents to the SM.

3.7.6.2. Final recipients of classified mail packages must sign the AF Form 310 accompanying the classified material and promptly return the receipt to the originator. Also, forward a copy of the AF Form 310 to the SM to maintain an active file. Destroy receipts IAW Records Disposition requirements (maintain for two years).

3.7.6.3. Classified information will be wrapped or packaged in 2 opaque envelopes or containers, sealed with brown nylon reinforced tape. The wrapping or packaging will be strong enough to provide protection in transit, prevent breaking out of the container, conceal all classified characteristics, and permit detection of tampering.

3.7.6.4. The Inner Envelope or Package.

3.7.6.4.1. Use appropriate labels and type the official government address of the receiving and sending activities (you may also add "Attention To:" of the individual you are sending the package to).

3.7.6.4.2. The overall classification of the contents will be marked on the top, bottom, front and back. If additional warning notices apply, they will also be included on the inner envelope.

3.7.6.4.3. AF Form 310 will be completed and placed in the inner package.

3.7.6.5. The Outer Envelop or Package.

3.7.6.5.1. Use appropriate labels and type the official government address of the receiving and sending activities (must be addressed to a receiving activity only and not directly to an individual).

3.7.6.5.2. There will be no markings on the outside container indicating the classification of the contents.

3.7.6.5.3. After all of the above actions are complete, hand-carry the classified materials to SCOW OM office further processing. Official Mail personnel will attach proper receipts and mail the materials. Ensure receipts are obtained by the sender for accountability purposes and maintain for two years.

3.8. **Hand Carrying Classified Information.**

3.8.1. Classified material will not be removed from the installation, unless it is deemed that hand-carrying the material is the only method available to provide timely support to the mission. The 635 SCOW Commander can approve the hand-carrying of classified material and should be used as a last resort.

3.8.2. Appropriately cleared individuals who are authorized to escort or hand-carry classified will comply with the procedures outlined in DoDM 5200.01, Vol 3_AFMAN 16-1404, Enclosure 4. Personnel must contact the SM for guidance prior to performing hand-carrying duties. Classified material will not be transported to an individual's residence.

3.8.2.1. When hand-carrying on the installation, and not passing through an inspection point where the information is subject to search, then supervisor verbal approval suffices.

3.8.2.2. When hand-carrying on the installation and passing through an installation inspection point (e.g., controlled areas, restricted areas, facility entry points during increased Force Protection Conditions, etc.), and within a 10-mile radius of the installation, use DD Form 2501, *Courier Authorization*.

3.8.2.2.1. DD Form 2501 is a controlled item and must be protected; secure in a locked file cabinet or desk. SM will be required to account for and protect the courier cards.

3.8.2.2.2. DD Form 2501 is valid for two years or when designation officials are replaced or depart the unit. DD Form 2501 exempts the classified materials from examination.

3.8.2.2.3. The SM will maintain the DD Form 2501 and only issue the card when personnel hand-carry classified.

3.8.2.3. When hand-carrying classified materials off the installation, a Courier Authorization Letter and Exemption Notice must be prepared and signed by the Commander. Only the Commander can sign and approve these documents for couriers traveling via commercial air.

3.8.3. Courier of Classified.

3.8.3.1. When classified material is transported, it shall be enclosed in two opaque, sealed envelopes, wrappings, or containers, durable enough to properly protect the material from accidental exposure and facilitate detection of tampering. A locked container (i.e., briefcase, mail pouch, etc.) may serve as the outer wrapper. The inner

envelope should be marked front, back, top and bottom, with the highest classification level of the contents, to include warning notices. The outer envelope or single container shall not bare a classification marking or any other unusual marks that may invite special attention to the fact that the contents are classified. Both the inner/outer packages should include the organizational addresses.

3.8.3.2. Individuals designated to hand-carry are briefed by the SM on their responsibilities for protecting the classified material while in transit. They will acknowledge receipt of the briefing and the understanding of their responsibilities by signing the Hand-carrying Classified Material Briefing Statement.

3.8.3.3. Classified material to be carried by the courier shall be inventoried; a copy of the inventory shall be retained by the SM and the courier. Use AF Form 310 to document the list of items being inventoried.

3.8.3.4. Advance coordination should be made with the airline and the Transportation Security Administration to obtain authorization of classified packages through screening points when the mode of travel is by air.

3.8.3.5. The classified material is not, under any circumstances, to be left unattended. During overnight stops, U.S. military facilities, embassies, or cleared U.S. contractor facilities must be used to secure the materials. Classified material shall not be stored in hotel safes, hotel rooms, and vehicles.

3.8.4. For verbal classified discussions, use a STE or other authorized secure communications and follow the procedures for that equipment.

3.9. **Reproduction of Classified and Unclassified Information.**

3.9.1. The Commander or Director will approve all copiers in the unit used for classified reproduction, in writing. The SM will produce the letter and coordinate with the unit CSL to ensure the copier meets requirements.

3.9.2. All personnel in the unit with the proper security clearance and need-to-know are authorized to reproduce classified information, provided classified reproduction is kept to a minimum.

3.9.3. Copiers, facsimiles, or other machines capable of and approved for reproduction of classified material must have the appropriate visual aids posted on the equipment.

3.9.4. Post the appropriate visual aids on or near other machines used for reproduction of unclassified material.

3.9.5. The unit CSL must engage with copier vendors prior to purchasing or utilizing a copier to reproduce classified. Specifically, obtain and document procedures to clear the memory and hard drives of copiers (if copiers have them) and the removal of latent images.

3.9.6. The unit CSL must engage with office equipment vendor prior to having any data storage capable office equipment maintained/serviced, prior to allowing a data storage capable device to leave the organization, and prior to decommissioning and/or turn-in. Specific procedures to clear the equipment’s memory and/or hard drives must be obtained and documented.

3.9.7. Classified reproduction equipment will be located where it is under continuous observation or in a locked room. Do not keep reproduction equipment in hallways, closets, or empty rooms. The SM approves placement of this equipment.

3.9.8. Personnel authorized to reproduce classified material will be familiar with the following procedures:

3.9.8.1. The reproduction process for collateral classified information requires one cleared individual for Secret and Confidential information.

3.9.8.2. All reproduced copies are subject to the same controls as the original.

3.9.8.3. When reproduction is complete, check the machine to ensure that the original and all copies are removed.

3.9.8.4. Check the last copy to ensure it is complete. If it is not complete, remove the portion remaining in the machine.

3.9.8.5. For machines retaining latent images, at least 3 blank sheets will be ran through the copying machine after reproducing classified to clear the image from the copier drum. Procedures will be posted for each machine approved.

3.9.8.6. Protect and destroy the blank copies as classified waste.

3.9.8.7. Do not reproduce Top Secret or special access information without the written consent of the originating activity or higher authority.

3.10. **Destruction of Classified Information.**

3.10.1. The second Friday in March of each year is designated the installation's annual classified "clean-out day." All classified materials being retained and no longer needed for mission requirements will be purged and destroyed.

3.10.2. When disposing of classified materials, first determine if the material is no longer required and provide protection throughout destruction process. Classified is "destroyed" when the contents are no longer recoverable from the residue of the destruction process.

3.10.3. The only method authorized to destroy classified information in the unit is by shredding.

3.10.4. All unit classified shredders in use meet the National Security Agency (NSA) standards for residue particle size requirements of 1mm x 5mm. Approved classified shredders are located throughout the unit and are marked with the appropriate visual aid.

3.10.5. Use the appropriate visual aid for unclassified destruction equipment. Post on or near the unclassified equipment.

3.10.6. Refer to AFMAN 17-1301, *Computer Security (COMPUSEC)*, Chapter 6, the governing directive for destruction of classified magnetic medium. A classified CD/DVD destroyer is located in building 1515 Room 101.

3.10.7. The destruction of Secret and Confidential information requires one cleared individual meeting security clearance eligibility requirements. The individual acts as own witness and no receipts are required.

3.11. **Security Incidents.**

3.11.1. Anyone discovering a security incident involving the actual or potential compromise of classified information will take custody of the information and safeguard the classified material until the responsible custodian or assigned security personnel regain proper custody.

3.11.2. Immediately report security incidents to the SM, immediate supervisor, or Commander or Director. Report the following information:

3.11.2.1. The type or level of information involved (i.e., SECRET, CONFIDENTIAL, etc.).

3.11.2.2. All of the persons involved.

3.11.2.3. Where the incident occurred.

3.11.2.4. When the incident was discovered.

3.11.2.5. Actions taken to safeguard the information.

3.11.3. The Commander or Director must report the incident to 375 AMW/IP no later than the end of the first day the incident occurred. This responsibility can be delegated to the SM.

3.11.4. The SM will notify the unit CSL when classified incidents involve unit computer or information systems (i.e., data spillages, classified message incidents [CMIs], etc.). Individuals involved in either a data spillage or CMI must take the following actions:

3.11.4.1. Disconnect affected Information System (IS) or media from the network (i.e., removal of network cable, turn off wireless capability [if applicable], etc.). Do not turn off the IS and do not destroy the affected document. Protect the IS or media accordingly to its highest classification level of data involved.

3.11.4.2. The CSL will follow incident response flow procedures as outlined in AFMAN 17-1301 and AFI 17-203, *Cyber Incident Handling*, Chapter 3.

3.11.5. The Commander or Director will assign an individual other than the SM within two duty days, to conduct a preliminary inquiry into the circumstances surrounding the security incident.

3.11.5.1. The preliminary inquiry official must be a disinterested military or civilian member not associated with the section where the security incident occurred and be at least in equal rank or above of the alleged suspect.

3.11.5.2. The inquiry official will have 10 duty days from the date appointed to conduct the inquiry.

3.11.5.3. The preliminary inquiry official will report to the SM immediately upon appointment for an inquiry briefing.

3.12. **North Atlantic Treaty Organization (NATO) and critical Nuclear Weapons Design Information (CNWDI) Access Requests.**

3.12.1. The Commander is the approval authority for NATO and CNWDI access (if applicable).

3.12.2. Requests for NATO and CNWDI access are forwarded in writing to the SM (e-mail message is sufficient).

3.12.2.1. Include the name, grade, office symbol, work phone number, and justification as to why the individual requires access.

3.12.2.2. In order for contractors to have access to NATO or CNWDI, it must be specified in the Contract DD Form 254 and the company's Facility Security Officer must in-brief the employee and document the access in DISS.

3.12.3. Upon receipt of the request, the SM will prepare an AF Form 2583, *Request for Personnel Security Action*, and forward to the approving authority for signature.

3.12.4. The SM is responsible for conducting the NATO and CNWDI briefs, to include:

3.12.4.1. Use AF Form 2583 for individual acknowledgement and signature for both NATO and CNWDI briefings.

3.12.4.2. Post AF Form 2583 and briefings in appropriate NATO or CNWDI continuity book and update the master NATO and CNWDI lists.

3.13. **CLEAN DESK POLICY.** Supervisors will enforce a clean desk policy throughout their sections to the maximum extent possible. At the end of the duty day, clear the desk surface and surrounding areas of all paper products including routine correspondence, technical data, notes, memos, etc.

3.14. **Physical Security. (** Secure Rooms and Secure Classified Discussion Rooms).

3.14.1. Initial and follow-up physical security survey requests must be routed through the SM to the Host Base IP office. The Chief, Information Protection is the designated approval official to certify collateral classified vaults, secure rooms, and classified discussion rooms on the installation.

3.14.2. The SM will inspect unit collateral certified classified discussion areas annually during the unit's annual security self-assessment to ensure standards are maintained in accordance with DoDM 5200.01, Vol 3_AFMAN 16-1404, Vol 3, Appendix to Enclosure 3, *Physical Security Standards*, document results of the inspection and maintain in the SM handbook.

3.14.3. 635 SCOW is not approved for open storage.

3.14.3.1. Approved collateral classified secure rooms in the unit:

3.14.3.2. Conference Rooms in Building 1521 are approved for SECRET level discussions.

3.14.3.3. Room 212, the Logistics Operations Center (LOC) and WM Room's 101, 102 & 107,109 in Bldg. 1521, as well as the Wing Commander, Wing Deputy Director and Wing Vice Director are authorized for SIPR use. During the times that the SIPR computers will be in use, the rooms will be closed and locked with a signs posted on the doors. Members will need to request access to enter the area.

3.14.3.4. Conference Rooms on 1st & 2nd floor in bldg. 1521 are authorized for SVTC (secure video teleconference). During the times that the conference rooms are being utilized for SVTC's the hallway will be closed down and members will need to have authorization to enter the area.

3.14.4. Security Container List. The SM will produce a list of collateral security containers (safes, secure rooms) and maintain in the SM handbook.

3.14.5. Classified Equipment List. The SM will account for all classified equipment in the unit (i.e., shredders, copiers, faxes, CD/DVD destroyers).

3.14.6. Classified Meetings. Hold classified meetings only in rooms that afford adequate security against unauthorized access. First option should always be to use an approved secure classified discussion room. When holding classified meetings or discussions in non-approved rooms use DoDM 5200.01, Vol 3_AFMAN 16-1404, Vol 3, Appendix to Enclosure 2, *Classified Meeting/Briefing/Conference Checklist*, to ensure countermeasures are in-place prior to classified discussions occurring.

3.14.6.1. Coordinate security plans with the SM 30 days prior to the meeting/conference.

3.14.6.2. Coordination of plans are not required for meetings/conferences held in secure classified discussion rooms, nor does it apply to routine or ad-hoc discussions between individuals.

3.14.7. Electronic Devices

3.14.7.1. Portable electronic devices such as cellular phones, iPods, MP3 players, kindles and laptops are allowed in the unclassified common areas and unclassified office areas.

3.14.7.1.1. Cell phones should be set on vibrate to moderate the sound ring tones, alarms and other alerts.

3.14.7.1.2. Cell phone conversations are allowed only in break rooms and common areas outside of shared work spaces.

3.14.7.1.3. Do not connect personal or contractor laptops to the network.

3.14.7.2. All electronic devices are "prohibited" in classified processing areas.

3.14.7.2.1. Store electronic devices outside the vault/secure room entry point.

3.14.7.2.2. Waivers/exceptions must be approved by the SM.

3.15. **Photographs** . The taking of photographs in the unit facilities/controlled areas/classified areas are prohibited, unless approved by the SM.

3.16. **Resource Protection.** All personnel are responsible for the care, security and protection of government property within their assigned work areas and specifically, that which is entrusted to their individual custody. This responsibility extends to noting apparent deficiencies and bringing them to the attention of the Commander or Director, supervisor, and/or SM.

3.17. **Visitors Process.**

3.17.1. The SM is responsible for sending unit personnel visit requests to contractor facilities or other visiting locations via DISS where access to classified information is required.

3.17.2. Any U.S. citizen on official business may visit personnel within unit facilities. Permanently assigned unit employees (military, civilian and contractors) may escort visitors.

3.17.3. Incoming Visit Requests.

3.17.3.1. Visit requests are not required for unclassified visits and there is no visitor badge requirement. Sponsors are required to escort visitors for the duration of the visit.

3.17.3.2. Visit requests are required for collateral classified visits. The visitors SM or Company FSO must send visit requests to the unit DISS SMO Code: SF1MFDCP-SCOW-635 (visit requests can be up to one year). Sponsors must coordinate classified visits with the SM to review procedures (e.g., attendee list, security clearance verification, classified room location, visitor badges, etc.). 3.17.3.3. Upon receipt of the visit request, the SM will send the request to the sponsor to validate the visit.

3.17.4. Outgoing Collateral Visit Requests.

3.17.4.1. Complete the appropriate visit request worksheet at the Unit's Security SharePoint site.

3.17.4.2. All out-going collateral classified visits will be processed through the SM for military and civilian personnel only. Contractors must process visit requests through their Company's FSO.

3.17.4.3. Collateral visits must be processed 3-days prior to visit.

4. Industrial Security Program.

4.1. **Industrial Security Oversight.** The SM will coordinate, review and process Product and System Contract and Visitor Group (VG) DD Form 254, *Contract Security Classification Specification*; Statement of Work (SOW)/Performance Work Statements (PWS) to ensure appropriate security requirements are identified; maintain contract folders for all on-site contractors; monitor on-site contract inspections; and issue CACs.

4.1.1. SM will provide guidance/assistance for preparing/processing DD Form 254.

4.1.2. Government Program Managers (PM) will ensure a DD Form 254 is added to all contracts requiring access to classified material IAW DoDM 5220.22, Vol 2_AFMAN 16-1406, Vol 2, *National Industrial Security Program: Industrial Security Procedures for Government Activities*, to include local Information Protection Office DD Form 254 Handbook guidance. Contact the SM for a copy of the handbook.

4.1.3. Prior to allowing contractors to initiate classified work on the contract, PMs must ensure the DD Form 254 has been signed by the contracting officer (CO) and placed on contract.

4.1.3.1. Additionally, anyone providing access to classified information must review the DD Form 254 to ensure the contractor receives only those classified accesses authorized.

4.1.3.2. For subcontractor employees, ensure the DD Form 254 for the subcontractor does not exceed the authorized access granted the prime contractor by the Government.

4.1.3.3. Contractors cannot be granted access to Secure Internet Protocol Router Network (SIPRNet) or other secure networks unless it is specifically identified on the DD Form 254.

4.1.4. To extend the contract or exercise an option period, the CO will issue an Amendment of Solicitation/Modification of Contract (SF 30) extending the contract. Provide copies of the SF 30 to the SM and all offices that are identified in block 18 (Required Distribution) on the DD Form 254.

4.2. **Processing DD Form 254.**

4.2.1. Prior to a contract solicitation or award, a draft DD Form 254 will be prepared by the organization responsible for submitting the request for proposal or awarding the contract. A separate DD Form 254 will be prepared for each contract solicitation and contract award when applicable. Delivery Order level DD Form 254's will be created as required by DoDM 5220.22, Vol 2, AFMAN 16-1406, Vol 2.

4.2.2. Organization PMs and COs will review the draft DD Form 254 to determine the appropriate access to classified information needed to satisfy the specific contract requirements.

4.2.2.1. The security requirements in blocks 10a through 11m of the DD Form 254 will be marked according to the access required for the contract.

4.2.2.2. When access to SAP information is required, ensure the DD Form 254 is coordinated through the Special Access Program Security Office prior to submitting for formal review/coordination.

4.2.3. The draft DD Form 254 will be submitted via electronic means to the SM to ensure DoD security requirements are satisfied, the DD Form 254 is complete, and all applicable documentation is included. The PWS, or equivalent, will accompany the draft DD Form 254 for solicitations and new awards.

4.2.4. After review, the SM will forward the draft DD Form 254 via electronic means to the appropriate IP office in sufficient time to secure coordination. The SM and PM will facilitate any changes needed in the DD Form 254 once it has been sent to 375 AMW/IP. Unit personnel will coordinate with the SM only. The SM will work any issues or concerns with 375 AMW/IP.

4.2.5. Completed and coordinated DD Form 254 will be added to the appropriate contracts IAW DoDM 5220.22, Vol 2_AFMAN 16-1406, Vol 2, in an expeditious manner. COs will sign the DD Form 254 in Block 17h (signature block) and forward a signed copy to the SM.

4.3. **Prime Contractors.** Are responsible for ensuring their on-base subcontractors are knowledgeable of and comply with the applicable security requirements (NISPOM, installation, etc.) as identified in contracts and/or contracting documents. Prime contractors complete DD Form 254s on subcontractors.

4.4. **Integrated Visitor Groups (VG).** DoD contractors who are performing contracted services requiring access to classified information and occupy office space in the unit for more than 90 days are designated as an integrated VG. In this circumstance, PMs will notify the SM and local IP Office 30 days prior to the contractor beginning work. Additionally, if a contract is extended or ends, the same notifications are required.

4.4.1. Integrated VGs will operate in accordance with DoD 5220.22-M, *NISPOM*; DoDM 5220.22, Vol 2_AFMAN 16-1406, Vol 2; DoDM 5200.02_AFMAN 16-1405, Air Force P*ersonnel Security Program*, and supplemental guidance thereto. They handle, generate, process, and store classified information per Air Force guidance. The exception being, their "access" is limited to "need-to-know" contract specific classified performance information.

4.4.2. VG personnel will in-process prior to being granted access to unclassified or classified on-site. As part of in-processing, PMs/CO Representative (COR)/Government point of contact will notify the SM prior to contractor work beginning (i.e., work or classified information access; a contract with a DD Form 254).

4.4.3. During in-processing, the SM will ensure all VG personnel meet the prerequisites to access classified information (i.e., valid security clearance meeting the requirements of the contract, signed a SF 312 and have the "need-to-know") and service the employee in DISS.

4.4.4. The SM must ensure the contractor only accesses classified, sensitive and Controlled unclassified Information (CUI) information and equipment that are specified on DD Form 254.

4.4.5. VG personnel must in-process with the SM for clearance verification/validation and records review prior to performing the terms of the contract.

4.4.6. VG personnel will use and must have access to existing AF security program related plans (Operations Security, Program Protection, AIS, etc.), procedures, operating instructions, and educational/training materials that meet the intent of and satisfy NISPOM requirements.

4.4.7. The SM will ensure VG personnel are integrated in the unit's initial and annual security training curriculum (Information, Personnel, and Industrial Security Programs) and ensure the training is documented.

4.4.8. VG personnel requiring access into restricted/controlled areas to accomplish their duties must complete the unit's restricted area/restricted area badge training and ensure the training is documented.

4.4.9. The SM must ensure VG personnel are included in the unit's annual security self-assessment to ensure classified operations are compliant and VG personnel are abiding by contract security requirements.

4.4.10. DoD contractors located on or visiting AF installations in support of a contract requiring access to classified information must comply with DoDM 5220.22, Vol 2_AFMAN 16-1406, Vol 2, visit requirements.

4.4.10.1. The SM is the unit's authorizing/approval authority for incoming/outgoing visit requests through DISS for VGs and unit personnel. The visit request for all contractor visits to the organization will be forwarded from the VGs home Facility Security Office (FSO) to the SM.

4.4.10.2. The SM is responsible for verifying the contractors' security clearance and maintaining current visit requests on file.

4.4.10.3. PMs receiving information directly from contractors will send the requests to the SM before any contractors are allowed access to classified information.

4.4.10.4. The SM will provide a copy of the DISS visit request to 375 AMW/IP and post it in the Industrial Security six-part folders.

4.4.11. VG personnel must report adverse information and suspicious contacts to 375 AMW/IP through the SM. Adverse information or suspicious contact reports will be maintained in the VGs file for two years.

4.4.12. VG personnel must report the loss, compromise or suspected compromise of classified information to the 375 AMW/IP through the SM.

4.5. **Industrial Security Six-Part Folders.** The 375 AMW/IP, SM, and VG Security Focal Point (SFP) are required to establish Industrial Security six-part folders and maintain the following documentation in the SM Handbook. The SM must ensure 375 AMW/IP receives the required documentation.

4.5.1. A signed copy of the current Prime DD Form 254 and all Subcontract DD Form 254s.

4.5.2. Performance Work Statement (PWS) or Statement of Work (SOW).

4.5.3. A signed copy of the VGSA and documentation of the VGSA provided to all subcontractors *(VGSAs are no longer required, but some contracts may still possess a VGSA until a new contract is revised or awarded. If this is the case, then maintain the VGSA).*

4.5.4. Training documentation (Initial and Annual Security Training).

4.5.5. Documentation of the last Information Protection Security Review (IPSR).

4.5.6. Documentation of last Annual Security Self-Assessment.

4.5.7. Key Management Personnel.

4.5.8. Current List of VG Employees (DISS Visit Request can substitute for employee list).

4.6. **Intermittent Visitor Group (VG).** DoD contractors who are performing contracted services requiring access to classified information and **do not** permanently occupy office space in the unit (usually 90 days or less) are classified as an intermittent VG.

4.6.1. DD Form 254 and DISS visit request must be on file prior to classified work being performed by visiting intermittent VG personnel.

4.6.2. DD Form 254 and DISS visit request of visiting intermittent VG personnel must be provided to 375 AMW/IP at least two weeks prior to arrival of the VG personnel.

4.7. **CAC Process Management.** The following processes are in effect for all unit personnel. Purpose is to ensure documentation of eligibility of applicants and accountability of CAC issuance and retrieval.

4.7.1. CAC Issuance.

4.7.1.1. Trusted Agent (TA) verifies the need with government CO, COR and PM.

4.7.1.2. TA verifies eligibility via DISS. Individual must have a current and valid Tier 1 investigation (formerly known as NACI); or higher-level security clearance; or Favorable FBI Fingerprint check and initiated Tier 1 investigation or DoD determined equivalent investigation. Note: If returned unfavorable, cancel/collect CAC immediately.

4.7.1.3. TA completes Trusted Associate Sponsorship System (TASS) entry.

4.7.1.4. TA notifies applicant to proceed to nearest RAPIDS Facility for CAC issuance.

4.7.2. CAC Retrieval.

4.7.2.1. CAC turn-in is part of out-processing. The CAC is turned into the TA or SM Office and out-processing form annotated.

4.7.2.2. TA revokes the CAC in TASS.

4.7.2.3. SM or TA turns the CAC into local FSS Military Personnel Section (MPS) and MPS signs turn-in letter to acknowledge receipt.

4.7.2.4. SM or TA files the turn-in letter and CAC receipt in official files.

4.7.3. Lost, Stolen, or Confiscated CAC.

4.7.3.1. Individuals will report lost CACs to their supervisor immediately.

4.7.3.2. The supervisor will complete the lost, stolen, confiscated DoD CAC Memorandum. The supervisor and individual will sign the memo and send to the SM.

4.7.3.3. The SM will sign-off on the letter and instruct the individual to go to the MPS for CAC issue.

4.8. **Identification.** Contractors shall identify themselves as such via the following means: office/cubicles marked as contractor work area, display of badge while on the installation, e-mail address, telephone conversations, and during meetings.

4.9. **Individual Contractor Terminations.** In the event a Contractor terminates employment (i.e., disciplinary issues, fired, medical, death, etc.), the SM must notify the below offices to ensure all out-processing actions occur:

4.9.1. PM of the affected contract to ensure the individual's CAC and facility access badge is retrieved and turned into the SM. Further, remove personal items from cubicle/desk area.

4.9.2. CSL for disabling of computer systems (SIPRNet and NIPRNet) and removing the individual from records.

4.9.3. Unit Training Manager to remove individual training files.

4.9.4. In/out-processing Manager to remove individual records.

4.10. **Contract Closure/Termination.**

4.10.1. The SM will immediately notify 375 AMW/IP in writing upon completion or termination of contracted services.

4.10.2. PMs will ensure individuals out-process with the SM when the requirement to work on base is no longer valid. This consists of giving the contractor the appropriate reminders to protect data. The SM will accomplish debriefs as applicable, retrieve identification/credential badges (organization ID and CAC), and remove the individual from appropriate databases.

5. AFPET Specific Items.

5.1. Office Security Training Plan. The AFPET will follow the 11th Wing Security Training.

5.2. Classification Challenges. Personnel who doubt the classification level of a document, either over or under the classification, have the right to challenge the originator. Prior to submitting challenges, a qualified technical expert will review the material in question. The 11 WG/IP if the focal point for challenges and will assist individuals with the challenge process upon request. All challenges will be routed through 11 WG/IP.

5.3. Lock Control: AFPET USM will function as the lock custodian. The combinations for cipher locks and combination locks, including XO-9 and XO-10 types, will be changed immediately when a container is placed in use, whenever a person knowing the combination no longer qualifies for access, the combination is compromised (e.g. members departing due to PCS), or the container is taken out of use.

5.4. End-of-Day Security Checks.

5.4.1. End-of-day security checks will be performed on all AFPET areas that process, store, or generate classified information, and conducted by the methods identified in DoD 5200.1: AFI 16-1404; and applicable supplements.

5.4.2. For AFPET Rm 1231, a sheet enumerating the opening and closing procedures will be posted on the back of the door.

5.4.3. End-of Day Security Checks Designated Personnel. The last Current Operations person on duty in Rm 1231 will conduct the end-of-day security checks to ensure classified material is stored appropriately.

5.4.4. Emergency Procedures: Controlled area security procedures must not hamper fire, medical, or Security Forces responding to an emergency. Uniformed emergency personnel will be granted immediate access to the controlled area when responding to a known emergency. It is not necessary to log all of the responding emergency personnel. When the emergency is resolved, the highest-ranking emergency respondent will be identified and their visit posted on the AF Form 1109, Visitor Access Register.

5.4.5. Bomb Threats: In the event a bomb threat is received by phone, the person receiving the threat will immediately refer to the Bomb Threat Aid, AF Form 440 (Nov 98), and get as much information as possible while attempting to keep the caller on the phone. Notify co-workers to contact Security Force by calling 703-767-4010 and report the threat. Secure the controlled area (cipher lock only); evacuate the building and rendezvous IAW the AFPET/DLA HQC Evacuation Plan. Ensure all personnel are accounted for. The facility manager or designated individuals will ensure Security Forces emergency responders have access to the controlled area. Personnel will return to the facility when cleared by the on scene commander.

5.5. Destruction of Classified Material.

5.5.1. Clean-out day. The 11 WG/CC will designate the annual "Clean-out Day" to ensure personnel are not retaining classified material longer than necessary. Documents, working papers, AIS media, etc., are reviewed for retainability, required markings, possible downgrading and declassification.

5.5.2. Destruction Equipment Operating Procedures. Shredder Operating Procedures will be posted near the destruction equipment. Obtain this visual aid from the 11 WG/IP Security Manager.

5.6. Security Termination

5.6.1. The Security Manager will report the fact to the 11th WG/IP

5.6.2. Furnish a copy of the AF Form 2587 to 11 WG/IP. Disposition of the original form will be IAW AFMAN 37-139.

5.6.3. Supervisors will inform AFPET/CC and Security Manager if any person in their branch is absent from work without an adequate explanation as to his/her whereabouts and the reason(s) for their absence.

6. 635th Supply Chain Operations Group Specific Items.

6.1. **Handling, Transfer, and Transmission of Classified.** Procedures for removing classified material from the confines of Bldg. 1515 are as follows.

6.1.1. Ensure documents are marked with the correct classification.

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

6.1.3. Place material in an unmarked envelope front and back.

6.1.4. Retain envelope or folder in your possession at all times until placed back in safe or destroyed.

6.2. **Emergency Protection Plan.**

6.2.1. The 635 SCOG Emergency Protection Plan outlines procedures for the removal and protection of classified material pertaining in 635 SCOG, Safe Number RSS2, Building 1515, Room 213. This plan will be maintained by the Security Manager and Safe Custodian(s) and located in Building 1515, Room 213. This plan will be reviewed every 2 years or in the event of any significant changes. The Emergency Protection Plan is for planning purposes only, until activated by the Group Commander or Unit Security Manager. Once an Emergency Protection Plan is established and/or changed, the procedures will be briefed to all office staff and a copy placed in close proximity of the security container.

7. 735th Supply Chain Operations Group Specific Items.

7.1. **Reproducing Classified.**

7.1.1. Documents and other material containing classified information shall be produced only when necessary for accomplishment of the 735 SCOG mission. The following personnel and positions may exercise reproduction authority: 735 SCOG Deputy Director; 735 SCOG/CCX Chief, Commander's Action Group; and 440 SCOS/GWA, Chief Assessments.

7.2. Prior to reproducing, follow the procedures that are displayed near the approved copier machine. Ensure LAFBVA 31-8, This Equipment is Authorized for Reproduction of Classified Material, is posted by reproduction machines authorized to reproduce classified material. Post LAFBVA 31-6, Not Authorized for Classified Material, by reproduction machines not authorized to reproduce classified material. Currently, 735 SCOG does not possess any classified copiers.

7.2.1. **Disposal and Destruction.**

7.2.1.1. Destruction should be accomplished periodically to preclude the accumulation of excess material. At a minimum, classified documents no longer required will be destroyed quarterly or more frequency if accumulation is excessive. The 735 SCOG will perform an annual clean out week the first week of April each year.

7.2.2. Two cleared personnel will witness and record the destruction of TOP SECRET material and the destruction is recorded on an applicable destruction certificate, e.g., AF Form 143. One cleared person may destroy SECRET/CONFIDENTIAL material (documentation is not necessary for collateral classified material.)

7.2.3. 735 SCOG has two shredders authorized for destroying classified material. One is located in Bldg. 330, Rm. 14, 735 SCOG Unit Deployment Manager (UDM) Office and the other is located in Bldg. 1017, Suite 15, 735 SCOG Commander's Action Group Secure Internet Protocol Router (SIPR) Rm.All shredders authorized to destroy classified material must be purchased from NSA/CSS evaluated products list for high security crosscut paper shredders that is maintained and offered through GSA. Information on approved destruction devices can be obtained from the Information Protection Office share point.

Before purchasing a shredder (to be used for destroying classified material) personnel must coordinate the purchase through the security manager. NOTE: 735 SCOG Commander's Action Group Government Purchase Card (GPC) holder(s) will be aware of this requirement.

7.3. **Handling, Transfer, and Transmission of Classified.**

7.3.1. Ensure documents are marked with the correct classification.

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

7.3.3. Place material in an unmarked envelope front and back.

7.3.4. Retain envelope or folder in your possession at all times until placed back in safe or destroyed.

7.3.5. Voice Over Secure Internet Protocol (VOSIP.) VOSIP or some other authorized secure voice communications system will be used when discussing classified information on the phone. 735 SCOG has two VOSIPs, one located in Bldg. 330, UDM's office, and the second one is located in Bldg. 1017, Commander's Action Group SIPR Rm.

7.3.5.1. When using the equipment, ensure that other people are not within hearing range of your voice and the other person on the receiving end has proper clearance and a need-to-know.

7.3.5.1.1. Once the Tactical Local Area Network Encryptor (TACLANE) is running, VOSIP will become active and ready to use for secure phone calls. VOSIP is used like a regular phone.

8. 635th Material Maintance Group Specific Items.

8.1. **Information Security.**

8.1.1. Storage. Within the unit, classified information or material will be stored only in General Service Administration (GSA)-approved security containers or an accredited secure room (open storage). If the security container does not have a GSA label, a GSA-trained locksmith must re-certify the container to meet GSA standards. Security containers (safes) are located in buildings 901, MMS Readiness, building 933, room 19 and building 953, room 111. The unit’s do not have a secure room (open storage) is located anywhere in MMG.

8.2. Receiving of Classified Material. Any office requesting classified material be sent to the unit must ensure they use the official address for the unit. The Official address is: 1273 Bear Path Rd, Holloman AFB, NM 88330.

8.3. Weekends and Off-duty hours**.** In the event that classified material is found unsecured and a SM or safe custodian is not available, the individual should secure it on their person and deliver the material to the 49th Wing Command Post. The individual should immediately notify the SM on the first duty day.

8.4. Overnight Repository for Classified Material. The Wing Command Post is the repository for temporary overnight storage of classified material up to Top Secret (collateral level). Personnel arriving unexpectedly or while in transit and in possession of classified information will coordinate with the Wing Command Post Controller prior to storing any classified information in the Command Post. The SM shall coordinate, in advance, with Wing IPO (572-1020/0890) and Wing Command Post (572-4900), prior to storing any classified material in the Command Post. The SMs are responsible for disseminating this information to all personnel during initial and refresher unit information security training.

CHAD R. ELLSWORTH, Colonel, USAF
Commander

Attachment 1

GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

References

Executive Order 13526, *Classified National Security Information*

DoDI 5200.48, *Controlled Unclassified Information (CUI)*

DoCN 5200.01, Vol 1_AFMAN 16-1404, Vol 1, *Information Security Program*

DoDM 5200.01, Vol 2_ AFMAN 16-1404, Vol 2, *Information Security Program:*

AFPD 16-14, *Security Enterprise Governance*

AFI 16-1401, *Information Protection*

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

MIL-HNBK-1013/1A, *Military Handbook, Design Guidelines for the Physical Security of Facilities*

ICD 705-1, *Physical Security Standards for Sensitive Compartmented Facilities (SCIFs)*

DoDM 5200.02_AFMAN 16-1405, *Air Force Personnel Security Program*

DODI 5200.46, *DoD Investigative and Adjudicative Guidance for Issuing the CAC*

Executive Order 12829, *National Industrial Security Program*

Federal *Acquisition Regulation* (FAR)

DoDM 5220.22, Vol 2_AFMAN 16-1406, Vol 2, *National Industrial Security Program:*

Industrial Security *Procedures for Government Activities*

DoD 5220.22-M, *National Industrial Security Program Operating Manual* (NISPOM)

DoD 5200.08-R, *Physical Security Program*

DoDI 5200.08, *Security of DOD Installations and Resources*

AFI 31-101, *Integrated Defense*

Adopted Forms

AF Form 847, *Recommendation for Change of Publication*

DD Form 2501, *Courier Authorization*

SF 312, *Classified Information Non-Disclosure Agreement*

(**NDA**) SF 700, *Security Container Information*

SF 701, *Activity Security Checklist*

SF 702, *Security Container Checklist*

Optional Form 89, *Maintenance Record for Security Type Equipment*

Acronyms and Abbreviations

AFCAF—Air Force Central Adjudication Facility

AFOSI—Air Force Office of Special Investigation

ANACI—Access National Agency Check and Written Inquiries

CMI—Classified Message Incidents

COMSEC—Communications Security

ISPM—Installation Security Program Manager

JCAVS—Joint Clearance and Access Verification System

NDA—Non-Disclosure Agreement

SAC—Single Agency Check

SAR—Security Access Requirement

SCI—Sensitive Compartmented Information

SMO—Security Manager Office

Attachment 2

EMERGENCY PROTECTION, REMOVAL AND DESTRUCTION OF CLASSIFIED MATERIAL

A2.1. Threat.

A2.1.1. Natural Disasters. (Severe rainstorms and flooding, tornadoes, fire etc). Civil disturbance, terrorism, and enemy action. Air Force Bases are susceptible to civil disturbances from outlying communities. Terrorism is a threat that could be experienced at any military installation at any time. The threat of terrorist action increases with the level of the local Force Protection Condition (FPCON). The Defense Condition (DEFCON) increases with the increased threat of enemy action.

A2.1.2. Limiting Factors. There is no central destruction facility on the installation capable for destroying classified material within the time criteria specified by this plan. As a result, units must effectively plan and acquire enough routine and emergency destruction equipment to execute this plan.

A2.2. Execution.

A2.2.1. PHASE I, Emergency Protection. Phase I will be implemented in the event of fire, natural disaster, bomb threat, civil disturbance, or in the case of an increased terrorist threat.

A2.2.2. Fire, Natural Disaster, or Bomb Threat.

A2.2.3. Secure material in approved security containers, if time and safety permit. When personal safety is in jeopardy, evacuate the area and post individuals to control entry and emergency access. Owner/user is responsible for the protection of their classified and facilities; Security Forces are not used for this function.

A2.2.4. Time permitting, the custodian will remove the material from the security container and take custody of it during building evacuation. Material will be transported to 635 SCOG, Building 1515, room 119 and secured in the classified storage container.

A2.2.5. If the classified material cannot be removed from the facility or the security container cannot be locked, notify the Fire Chief immediately. If feasible, a guard should remain with any unsecured classified material until the emergency is over.

A2.2.6. Allow only responding emergency crews to enter the facility (Fire Department, Medical Services, Security Forces, etc.). Classified custodians may enter the facility to account for the unsecured classified materials after the area is declared safe.

A2.2.7. Admit all firefighters or other emergency response personnel required to combat the situation. To the maximum extent possible, ensure that only emergency personnel are allowed into areas where classified material is present. If the intensity of the fire is such that the area must be abandoned, to the best of your ability, maintain surveillance of the general area to prevent unauthorized persons from entering. Obtain a list of names of all personnel allowed entry for possible debrief.

A2.2.8. Civil Disturbance or Increased Terrorist Threat.

A2.2.9. If a civil defense alert signal (3-5 minute steady-tone siren) is sounded or flooding occurs, all classified material must be removed from the immediate work area and secured in the appropriate security container as long as time permits.

A2.2.10. Prepare for the initiation of Phase II. Phase II is implemented when the possibility of conflict increases.

A2.3. PHASE II, Precautionary Destruction.

A2.3.1. Segregate all classified into "mission essential" and "non-mission essential" categories.

A2.3.2. Retain mission essential classified material. Destroy non-mission essential classified material using routine classified destruction methods. Classified shredders are located in Room 101 and 212. Memo for record are required for all classified destruction.

A2.3.3. Prepare for PHASE III.

A2.4. PHASE III, Emergency Destruction.

A2.4.1. PHASE III actions will be initiated upon the determination an imminent threat exists of the installation being overrun. The effect of premature destruction is considered inconsequential when measured against the compromise of classified information.

A2.4.2. Each unit will predesignate a location for the emergency destruction of classified material and procure or manufacture sufficient equipment to accomplish the destruction process. If time does not permit you to use predesignated material, immediate destruction will be accomplished in any available means. Destruction equipment are located in Room 101 and room 212.

A2.4.3. Secret and Confidential material holders must destroy the materials within two hours.

A2.4.4. No destruction records are required under emergency destruction procedures.

A2.5. Notification.

A2.5.1. The installation Command Post will implement this plan by order of the installation commander or higher authority.

A2.5.2. The installation Emergency Operations Center (EOC) will be formed upon implementation to track progress and ensure all units are notified.

A2.5.3. Any senior individual present in an area containing classified material that determines there is a sufficient threat, may implement any portion of this plan.

A2.6. Preparation Instructions.

A2.6.1. Assign classified material one of the following priorities.

A2.6.2. Priority One: Secret.

A2.6.3. Priority Three: Confidential.

A2.6.4. Post emergency action checklists will be located in the security container-locking drawer or in secure room continuity books.

A2.7. Taskings.

A2.7.1. SM ensure notification is made upon implementation of this plan.

A2.7.2. Custodians ensure individuals with access to the secure material are familiar with emergency destruction procedures.

Attachment 3

END OF DAY SECURITY CHECKS

A3.1. POLICY: It is policy that unit personnel having access to classified information or equipment will take precautionary measures to preclude the possible compromise of sensitive information, protect physical resources, and conserve energy. IAW the reference directives, an end-of-day security check of all areas will be accomplished to ensure safes, vaults, secure rooms or office/work areas are locked at the end of each day. End-of-day checks will normally be performed no earlier than 1600. When personnel are released early, checks will coincide with the earlier release time. In instances where the majority of the organization works late, the check is accomplished at the completion of the workday. If individuals work on a non-duty day, the entire office area check is performed at the end of the non-duty period.

A3.2. RESPONSIBILITIES:

A3.2.1. Section Chiefs (areas where classified information is processed):

A3.2.1.1. Assign in writing a roster of properly cleared personnel to perform end-of-day checks. Scheduled checkers will find a replacement should they be unable to perform the duty. Checkers must have at least a Secret clearance.

A3.2.1.2. Provide each checker with a Security Check Kit. The kit should contain, as a minimum, the current month's SF 701, *Activity Security Checklist*, a copy of this attachment and a copy of the end-of-day checker roster. The SF 701 will include, as a minimum, all security containers (identify each safe by a serial number), office lights, windows, doors, electrical equipment/appliances, STE telephones, faxes, printers, shredders, computers and security alarm systems.

A3.2.1.3. In areas not approved for open storage of classified, personnel are required to clear desk tops, tables, file cabinet tops, etc., for classified documents. Secure any unopened USPS registered mail. Store all classified documents, CDs, diskettes and removable hard drives in a GSA-approved safe. In areas approved for open storage of classified, as a minimum, ensure classified documents have the appropriate coversheet attached to the front of the document when not in a safe.

A3.2.2. End-of-Day Checker will:

A3.2.2.1. Check all listed items on the SF 701 and place a check mark in all areas checked and found to be in compliance.

A3.2.2.2. Physically verify safes are locked. If found to be secure, the checker will initial and annotate the time on the SF 702, *Security Container Checklist*, in the "checked by" column. If the SF 702 indicates that the safe/vault was not opened that day, then the checker will annotate "Not Opened" through the "opened by" and "closed by" blocks and annotate their initials and time in the "checked by" column.

A3.2.2.3. When individuals are working after hours with security container(s) open, acknowledge the open container by placing an "*" in the appropriate block on the SF 701. Annotate the container number(s) and date on the reverse of the SF 701.

A3.2.2.4. If individuals are still working at the time of the end-of-day check, ensure they assume responsibility for lights, equipment/appliances and vault/secure room door alarms.

A3.2.2.5. Upon completion of the check, initial and annotate the time completed on the SF 701 in the appropriate blocks.

A3.2.2.6. In the event unattended classified material/documents are found in areas not authorized for open storage, protect the material and notify the supervisor or SM of the incident. If no one is present, the checker will secure the material in a GSA-approved safe, leave a note for the supervisor and report it to the SM at the beginning of the next business day. The material must be properly protected.

A3.2.2.7. In the event a security container is found open or unlocked, notify one of the individuals listed on the SF 700 posted inside the locking drawer. Do not leave the safe open or unattended. Remain with the safe until the person notified responds or secure the safe and depart, depending on instructions received from the safe custodian. The SF 701 will be annotated "found opened" to show the incident. If no contact was made with the custodian, secure the container and notify the safe custodian, supervisor, and SM at the beginning of the next business day.

A3.2.2.8. Contractors are not permitted to perform end-of-day security checks unless specifically stated in their Security Agreement or Contract Statement of Work.

A3.2.3. SM will:

A3.2.3.1. Include end-of-day check procedures in initial and annual training.

A3.2.3.2. Report all security incidents brought to his/her attention.

A3.2.3.3. Assist personnel, as required, in order to comply with this Instruction.

A3.2.4. Individuals will:

A3.2.4.1. Assume responsibility, if working after hours, for those items in their area on the SF 701 that were not checked by the end-of-day checker.

A3.2.4.2. Be responsible for finding a replacement if unable to perform the check on a specific day or for the period scheduled. Notify supervisor of schedule change to ensure coverage.

A3.2.4.3. If using a security container after hours, or if a need arises to open a security container after it has been checked, perform the end-of-day check for that container, initial, and annotate the time checked in the appropriate block. In this instance, the same individual who annotated the container open and closed, also annotates the "checked by" block.

A3.2.4.4. If notified of an opened/unattended container, check the container for evidence of tampering or malfunction of the locking device. The safe custodian will review the contents of the safe to ascertain if documents are missing. If there is no evidence of tampering/malfunction and no documents are missing, lock the safe, have the checker annotate the SF 702 and change the combination at the beginning of the next duty day.

A3.2.4.5. Perform all of the duties of end-of-day checker when working weekends and holidays.

A3.3. Disposition of Records: The SF 701 and 702 will be maintained IAW Records Disposition requirements.