DEPARTMENT OF THE AIR FORCE
AIR EDUCATION AND TRAINING COMMAND

DoDM5200.01V3_DAFMAN16-1404V3_SHEPPARDAFBGM2026-01
30 APRIL 2026

MEMORANDUM FOR ALL SHEPPARD AFB PERSONNEL

FROM: 82 TRW/CC
419 G. Avenue, Suite 1
Sheppard AFB TX 76311

SUBJECT: Sheppard AFB Guidance Memorandum (GM) to DoDM5200.01, V3_DAFMAN16-1404, V3, Information Security Program: *Protection of Classified Information*

RELEASABILITY: There are no releasability restrictions on the publication.

By order of the Installation Commander, this Sheppard AFB Guidance Memorandum immediately implements changes to DoDM5200.01, V3_DAFMAN16-1404, V3. Compliance with this memorandum is mandatory. To the extent its directions are inconsistent with other Department of the Air Force publications, the information herein prevails, in accordance with Department of the Air Force Instruction (DAFI) 90-160, *Publications and Forms Management* and Department of the Air Force Manual (DAFMAN) 90-161, *Publishing Processes and Procedures*. This guidance is applicable to all organizations supported by the 82d Training Wing (TRW) Information Protection (IP) office.

The attachment contains guidance pertaining to the Sheppard AFB Information Security Program and supersedes DoDM5200.01V3_DAFMAN16-1404V3_SHEPPARDAFBGM2025-01, 25 February 2025. Ensure that all records created as a result of processes prescribed in this publication are maintained IAW AFI 33-322, *Records Management and Information Governance Program*, and disposed of in accordance with the Air Force Records Schedule (RDS) located in the Air Force Records Management System.

The authorities to waive requirements in this GM are identified with a Tier ("T-0, T-1, T-2, T-3") number following each compliance statement. See DAFMAN 90-161, *Publishing Processes and Procedures*, for a description of the authorities associated with the Tier designators. Submit requests for waivers through the chain of command to the appropriate Tier waiver approval authority, or alternately, to the GM OPR for non-tiered compliance items, as applicable.

This publication requires the collection and/or maintenance of information protected by the Privacy Act of 1974 authorized by DoDI 5400.11, "DoD Privacy and Civil Liberties Program." The applicable System of Records Notices (SORN) DUSDI 02-DoD, Personnel Vetting Records System (which will be renumbered to DoD-0002)) and various training sites (covered by DoD 0005, Defense Training Records) which is available at https://dpcld.defense.gov/Privacy/SORNs/.

This guidance becomes void after one year has elapsed from the date of this memorandum, or upon publishing of a new instruction/manual permanently establishing this guidance, whichever is earlier. Direct questions regarding this memorandum to 82 TRW/IP at DSN 312-736-3514.

PAUL G. FILCEK
Brigadier General, USAF
Commander, 82d Training Wing

Attachment: Guidance Changes

Attachment

Guidance Changes

References

SAFB VA 16-1404-3, *Authorized for Destruction of Classified Information,* 20230515
SAFB VA 16-1404-4, *Not Authorized for Destruction of Classified Information,* 20230515

Terms

Covered Personnel – Permanent party military and civilian personnel who are assigned to a security access requirement (SAR) code 5, 6, or 7 duty position on the unit manpower document. This also applies to the following personnel categories who require a national security background investigation as driven by their assigned duties (1) contractors per the provisions of their contract who require elevated privileges to the unclassified Department of War (DoW) Information Technology (IT) network, however, do not require access to classified material and (2) U.S. military personnel in training and/or TDY at Sheppard AFB (SAFB).

Cleared Personnel – Covered personnel who require access to classified information, as authorized by their commander, to support unit and/or installation mission requirements. This also applies to the following personnel who meet these conditions (1) contractors per the provisions of their contract and (2) U.S. military personnel in training and/or TDY at SAFB.

Uncleared Personnel – Civilian and contractor personnel who do not require a national security eligibility to support unit and/or installation mission requirements; however, do require a Public Key Infrastructure (PKI), Common Access Card (CAC) or Non-classified Internet Protocol Router Network Enterprise Alternate Token System (NEATS) to access the unclassified DoW IT network and/or installation.

Classified Processing Area (CPA) – An area used for the open storage and/or processing of classified material and/or where classified information systems (i.e., Secret Internet Protocol Router Network, Defense Integration and Management of Nuclear Data Services, Force Protection, etc.) are in use.

Personnel Security Custodian (PSC) – Personnel provided read-only access to DISS to perform personnel security duties under the guidance and oversight of a unit Security Assistant(s) (SA).

Security Container Custodian (SCC) – Personnel who manage a safe, vault, and/or open storage room (hereafter referred to as a secure room) and classified holdings stored therein under the guidance and oversight of a unit SA.

Security-In-Depth –Security-in-depth is the determination that an installation's and/or facility's security program consists of layers and complementary security controls sufficient to deter, detect, delay, assess, respond, and document unauthorized movement within.

Enclosure 2 – Safeguarding

2. Personal Responsibility for Safeguarding

2.a. **(Added)** Personal observation and control is defined as having sufficient attention and scrutiny over classified material with due physical security, monitoring, supervision, and/or surveillance to deter and detect access by unauthorized persons, while having a commensurate system of control measures that ensure access to classified material is limited to authorized persons. Constant observation and control by an authorized individual (i.e., having constant eyes on the item with nearby physical proximity), is the primary means to meet this intent, especially with classified items capable of being carried (i.e., computer media, documents, etc.). (PAGE 16 INSERT)

2.b. **(Added)** Commanders may also authorize other appropriate risk management options to employ a combination of physical security, monitoring, supervision, and/or surveillance measures for meeting the personal observation and control intent of ensuring protection of classified while accomplishing the mission. Such risk management options should be appropriate to the environment in which access occurs, inherent installation-level security-in-depth features and to the nature and volume of the information. For example, in the case of an Intrusion Detection System failure, minimum 4-hour checks can be implemented for secure rooms; use of an Automated Entry Control System (AECS), which complies with the requirements outlined in Appendix 1 to Enclosure 3, Section 3 of this volume, for management of entry control points. Note: A standard cipher lock CANNOT be used in lieu of an AECS. (PAGE 16 INSERT)

3. Access to Classified Information

3.a. The following conditions account for the Commander's permission for a Security Assistant (SA) to grant individuals possessing a current clearance eligibility, in the following categories, access to classified information. (PAGE 17)

3.a.(1) **(Added)** Permanent party U.S. personnel assigned to a Security Access Requirement (SAR) Code 5, 6 or 7 position via the unit's manpower document (UMD) that have a need to generate, reproduce, view, hear, and/or discuss classified material in the performance of their official duties. A memorandum signed by the Commander must be completed identifying the applicable UMD positions and ancillary duties whereby incumbents are authorized access to classified information to fulfill unit and/or installation mission requirements. **(T-2)** (PAGE 17 INSERT)

3.a.(2) **(Added)** U.S. students who need to generate, reproduce, view, hear, and/or discuss classified material during training. A class roster(s) signed by the SA or Personnel Security Custodian must be posted inside the applicable classroom(s) where classified instruction is taking place. **(T-2)** (PAGE 17 INSERT)

3.a.(3) **(Added)** Contractors who, per their contract, need to generate, reproduce, view, hear, and/or discuss classified material in the performance of their duties. Submittal of a Visit Request with a list of each employee's credential is required to be sent via the Defense Information System for Security (DISS) or successor system by their Facility Security Officer to the sponsoring organization's Security Management Office (SMO). **(T-2)** Contractor personnel shall not be granted access to classified material prior to completion of these actions. **(T-2)** (PAGE 17 INSERT)

3.a.(4) **(Added)** Permanent party U.S. personnel not assigned to a unit who need to generate, reproduce, view, hear, and/or discuss classified material per their official duties (e.g., inspection, training, site visit, etc.). Submittal of a Visit Request by the sending organization's SMO via DISS (or successor system)

with everyone's credential is required. For organizations without DISS access, a Visitor(s) Access Letter signed by the SMO representative on letterhead from the sending organization is acceptable. Unless determined by the Commander in possession of the classified holdings, personnel shall not be granted access to classified material prior to completion of these actions. **(T-2)** (PAGE 17 INSERT)

3.a.(5) **(Added)** Access to classified information for foreign national personnel must be approved respectively by the 80 FTW and 82 TRW Foreign Disclosure Offices. **(T-2)** (PAGE 17 INSERT)

3.a.(6). **(Added)** CUI material governed by International Traffic Arms Regulations which controls the export and import of defense-related articles and services on the United States Munitions List (commonly referred to as Export Controlled Information) and/or governed by a Distribution Statement limiting sharing with non-U.S. personnel, must be approved for release respectively by the 80 FTW and 82 TRW Foreign Disclosure Offices. **(T-0)** (PAGE 17 INSERT)

3.c.(2) The Commander will sign the NATO Security Briefing Certificate to account for an individual's need to know, possession of the requisite clearance eligibility and receipt of the NATO security briefing as a prerequisite of an individual being indoctrinated and granting access to NATO classified level/caveat(s) as recorded in DISS (or successor system) by their SMO. **(T-2)** (PAGE 17)

7. Visits

7.c.(1) **(Added)** Individuals meeting some or none of the security requirements to access the respective security containers/vault/secure room will require an escort official. **(T-2)** All visitors will need to coordinate visits through their SMO with the sponsoring location's point of contact. (PAGE 23 INSERT)

7.c.(2) **(Added)** Escort officials will assume responsibilities for visitors and will: **(T-2)** (PAGE 23 INSERT)

7.c.(2)(a) **(Added)** Ensure visitors are vetted and/or are indoctrinated and granted access, as recorded in DISS (or successor system), to the level/caveat(s) of material under the visited unit's control, as applicable, and valid credentials are used for verification prior to allowing access to classified material under their charge. (PAGE 23 INSERT)

7.c.(2)(b) **(Added)** Document visitors on the AF Form 1109, *Visitor Register Log*, for accountability. The AF Form 1109 must be replaced at the beginning of each month. (PAGE 23 INSERT)

7.c.(2)(c) **(Added)** Provide an escort briefing prior to entering the classified processing area. At a minimum, the following will be briefed. (PAGE 23 INSERT)

7.c.(2)(c)1. **(Added)** Visitors will stay with their escort official and will not handle or touch anything without the express approval from the escort official. (PAGE 23 INSERT)

7.c.(2)(c)2. **(Added)** Surrender unauthorized electronic devices such as cell phones, digital recorders, cameras, smart watches and/or other similar recording, wireless, photography or blue tooth devices to the escort official. (PAGE 23 INSERT)

7.c.(2)(c)3. **(Added)** In the event of an emergency, follow the direction of the escort official. (PAGE 23 INSERT)

9. End of Day Security Checks

9.a. End-of-day security and audit checks must be accomplished every duty day and annotated respectively in the "Checked By" and "Guard Check" columns of the SF 702, even if the container was not opened, after ensuring it is locked. **(T-2)** NOTE: Audit checks are performed to compare the number of times the security container/vault/secure room is opened, via a counter internal to the lock, against the openings transcribed on the SF 702. For security containers housed inside of a secure room, these checks are only required if the room is accessed. (PAGE 23)

9.b. Maintain a copy of each completed SF 701 and SF 702 on file for 90 calendar days. **(T-2)** (PAGE 23)

9.c. **(Added)** The SF 701, *Activity Security Checklist,* must include, at a minimum, the unit-assigned unique identification number or manufacturer serial number for every security container used to store classified material within the area. Personnel must spin the dial of the X-07/8/9/10 locks several times in both directions to ensure positive locking. This also applies to vaults and secure rooms. **(T-2)** (PAGE 23 INSERT)

10. Emergency Plans

10.c.(1) **(Added)** Security Container Custodian(s) (SCC) must ensure personnel with unescorted access to classified holdings stored within their container/vault/secure room are familiar with the location of the emergency action plans and how to use them. **(T-2)** (PAGE 24 INSERT)

16. Classified Meetings and Conferences

16.a.(3)(f) **(Added)** Classified meetings shall be approved by the appropriate commander or director if it is deemed unique, complex, and/or is a "hosted" type of event, especially when involving attendees and/or visitors from organizations outside of Sheppard AFB. **(T-2)** Meetings of this nature require completion of the Classified Meeting/Briefing/Conference checklist located at Appendix 1 to Enclosure 2 by the appointed action officer or SA. **(T-2)** (PAGE 29 INSERT)

16.a.(3)(g) **(Added)** Standard, recurring and/or day-to-day classified mission meetings need not be continuously or formally approved. The awareness thereof or attendance by senior leadership shall suffice as implied approval. However, a classified meeting shall be more formally approved by the appropriate commander or director if such a meeting is deemed unique, complex, and/or is a "hosted" type event or meeting, especially when involving multiple organizations with non-unit attendees/visitors. **(T-2)** Regardless of meeting type, all members in attendance must be cleared for access by a SMO prior to entry. **(T-2)** (PAGE 29 INSERT)

Enclosure 3 – Storage and Destruction

3. Storage of Classified Information by Level of Classification

3.b.(5)(a) **(Added)** A room will not be certified for the open storage of classified holdings solely for convenience. Commanders must submit a memorandum to the 82 TRW/IP outlining the requirements driving the establishment of a new open storage area/room, hereinafter referred to as a secure room. **(T-2)** Once the 82 TRW/IP determines that a secure room is required, commanders must submit a work order to the 82d Civil Engineering Squadron (82 CES) to assess if the space currently meets secure room construction standards. **(T-2)** Commanders may be required to initiate additional work order(s) to shortalls. (PAGE 45 INSERT)

3.b.(5)(b) **(Added)** Once construction standards have been verified via the documentation provided by the 82 CES and site inspection by the 82 TRW/IP Information Security Program Manager and 82d Security Forces Squadron Physical Security (82 SFS/S5X), the Chief of Information Protection (CIP) will certify the secure room in writing. **(T-2)** A copy of the most recent certification memorandum will be posted on the interior of the main entry door to each secure room. **(T-2)** (PAGE 45 INSERT)

3.b.(5)(b)1. **(Added)** An assessment by a representative from 82 SFS/S5X is also required if installation of an IDS is needed. **(T-2)** (PAGE 45 INSERT)

3.b.(5)(b)2. **(Added)** An assessment by a representative from 82 CS/SCXS is also required if there are TEMPEST considerations to be evaluated. **(T-2)** (PAGE 45 INSERT)

3.b.(5)(c) **(Added)** SA(s) and SCC(s) must coordinate all secure room construction and modifications through 82 TRW/IP to facilitate the recertification process. **(T-2)** 82 SFS/S5X and/or 82 CS/SCXS must also be contacted to verify if their applicable requirements must be recertified. **(T-2)** (PAGE 45 INSERT)

4. Risk Assessment

4.b. The SAFB historical risk assessment indicates a "LOW" to "MODERATE" threat for activities relating to secure rooms, and those classified related operations (e.g., security containers, SIPRNet equipment, etc.,) located outside a secure room. The installation commander, 82 TRW/CC, has authorized Commanders and directors to incorporate the SAFB historic risk assessment when identifying and selecting supplemental controls for protecting related classified operations (e.g., security container, room, area, or vault). If a commander or director deems it prudent or necessary to make a local adjustment to the SAFB historical risk assessment, the 82 TRW/CC shall be notified via the CIP, so associated classified operations posture and/or network support, availability, connectivity, and/or installation-wide implications can be assessed. **(T-2)** Security-in-depth exists for areas within the confines of SAFB. (PAGE 45)

4.b.(1) **(Added)** When conducting the minimum 4-hour guard checks, the entire perimeter of the secure room must be checked; simply checking entry doors will not suffice. **(T-2)** Signs of tampering or forced entry will be immediately reported to the 82 SFS Base Defense Operations Center (BDOC). **(T-2)** (PAGE 45 INSERT)

6. Specialized Storage

6.a.(3)(a) All persons (military, civilian, and contractors) who are performing maintenance or conducting maintenance training on classified parts or components aboard a Ground Instructional Training Aircraft (GITA) must have an active access caveat granted or inherited to the level of the material on the GITA under the unit Security Management Office (SMO) in DISS. **(T-2)** (PAGE 46)

6.a.(3)(a)1. Training squadron commanders are responsible for the protection of classified material and components aboard their GITA(s). (PAGE 46)

6.a.(3)(a)2. Training squadron commanders must consult with the 82 TRW/IP during GITA acquisition planning to determine the appropriate safeguarding standards for classified material and components aboard. **(T-2)** (PAGE 46)

6.a.(3)(c) When not under the personal control and observation of an authorized U.S. government person with a proper clearance eligibility and access, GITAs with classified parts and components will be parked within a temporary or permanent controlled area. **(T-2)** Additionally, GITAs with Secret parts or

components must also be within an alarmed area that is monitored by the 82 SFS BDOC. The 82 TRW/IP will be consulted for additional security measures for GITAs with Top Secret parts and components. **(T-2)** (PAGE 46)

6.a.(3)(c)3. GITAs are not a protection level, transient nor an operational resource, thus negating the need to seal the aircraft egress doors with tamper-proof seals as a safeguarding requirement. (PAGE 46)

10. Security Container Information

10.a. The names of the primary and alternate SCC(s) must be listed on the SF 700, *Security Container Information*, to identify personnel responsible for serviceability, preventive maintenance, and contents stored within. **(T-2)** The envelope containing SF 700, Part 1 must also be marked "CUI" at the top and bottom of the front and back of each side. **(T-2)** Tape or place the envelope in a sleeve that is located and adhered to the interior front side of the security container control drawer or on the back of the secure room/vault door so it is readily identifiable by anyone that may find the container/vault/secure room open and unattended. **(T-2)** (PAGE 50)

10.b. Use of SF 700, Part 2 is optional, per a commander's discretion, but is highly recommended. If used, Part 2 must be sealed in an opaque envelop conspicuously marked "Container Combination" with classification level of the combination at the top and bottom of the front and back of each side. **(T-2)** Part 2 will be secured in a separate security container/vault/secure room. **(T-2)** (PAGE 50)

10.c.(1) **(Added)** SCCs will conduct a visual inspection on newly acquired security containers utilizing the security container and vault door visual inspection checklist located in Appendix 2 to Enclosure 3 of this volume and annually thereafter in October. **(T-2)** The most current complete visual inspection checklist shall be maintained. **(T-2)** (PAGE 50 INSERT)

10.c.(2) **(Added)** The AFTO Form 36, *Maintenance Record for Security Type Equipment*, is only required to be maintained with the OF 89 if there is documented maintenance and/or repairs to a security container and secure room/vault door listed within. (PAGE 50 INSERT)

11. Combinations to Containers, Vaults, and Secure Rooms

11.a. Combinations to containers housing classified NATO, RD, or CNWDI material may only be stored in containers cleared for storing this information. Ensure the SF 700, Part II is properly marked (i.e., NATO SECRET, SECRET//RD, SECRET//RD-N, etc.). (PAGE 50)

13. Inspection of Storage Containers Prior to Removal, Repair, Etc.

13.a. **(Added)** If a security container is no longer required, the SCC(s) must pull out all drawers and closely examine interior for classified material, set combination to default setting of (50-25-50), remove exterior security container markings (i.e., SFS-01), and contact 82 TRW/IP for disposition instructions. **(T-3)** Place a note on container stating, "Not in use – combination set to default". Do not remove the OF 89. **(T-3)** (PAGE 52 INSERT)

17. Destruction of Classified Information

17.b. Commanders/Directors will ensure annual cleanout days are conducted in the month of October. **(T-2)** During this month, SCCs will execute the actions outlined in 10.c.(1), 17.b.(1), 17.e. of this enclosure for security containers/vaults/secure rooms within their area of responsibility. **(T-2)** Once complete, SCC will submit the classified material cleanout memorandum, destruction equipment

memorandum and visual inspection checklist(s) to the SA(s) to place in the SMO program binder. **(T-2)** (PAGE 52)

17.b.(1) **(Added)** SCCs will review all classified holdings stored inside security containers/vaults/secure rooms within their area of responsibility for retainability, required markings, possible downgrading, destruction, and declassification. **(T-2)** (PAGE 52 INSERT)

17.e. **(Added)** SCCs will check the functionality and currency of equipment utilized to destroy and/or sanitize classified material on the NSA Evaluated Products List prior to being purchased by their organization and annually in thereafter in October. **(T-2)** SAFBVA 16-1404-3, *Authorized for Destruction of Classified Information*, must be posted on these devices. **(T-2)** (PAGE 53 INSERT)

17.f. **(Added)** SAFBVA 16-1404-4, *Not Authorized for Destruction of Classified Information*, must be posted on all equipment, not authorized for destroying classified material that is located within a classified processing area. (PAGE 53 INSERT)

Appendix 1 to Enclosure 3 – Physical Security Standards

3. Access Controls

3.a. For secure room(s)/vault(s), the XO-7/8/9/10 combination lock can remain in the open mode only when the room/vault is manned by a cleared individual, the entry door is under continuous observation, or an authorized automated entry control system is used. Use of a standard cipher lock is only authorized as a convenience during duty hours when a secure room/vault is manned, or the entry doors are under visual control. Manned means personnel within the area can readily detect unauthorized entry into the secure room/vault. The Intrusion Detection System (IDS) will always be activated during non-duty hours. During duty hours, the IDS can remain inactivated, XO-7/8/9/10 unlocked, if AECS, which complies with the requirements outlined in Appendix 1 to Enclosure 3, Section 3 of this volume, is used. If AECS is not used, the IDS can remain inactive for short times (no more than 4 hours) when unmanned as long as the XO-7/8/9/10 combination lock is engaged. (PAGE 60)

Enclosure 4 – Transmission and Transportation

13. Escort, Courier, or Hand-Carry Authorization

13.c. **(Added)** Hand-carrying classified within the confines of Sheppard AFB, or the Explosive Ordnance Disposal annex requires, as a minimum, approval from an immediate supervisor. **(T-3)** (PAGE 77 INSERT)

13.d. **(Added)** A DD Form 2501, *Classified Courier Authorization Card*, or a Courier Authorization memorandum signed by the unit Commander or director, is required to hand-carry classified material off-base within the continental United States (CONUS) or aboard an U.S. military transport outside the CONUS (OCONUS). **(T-2)** Off base is defined as outside the fence line of Sheppard AFB or the Explosive Ordnance Disposal annex. (PAGE 77 INSERT)

13.e. **(Added)** Wing Commander approval must be obtained, in writing, to hand-carry classified material aboard a commercial transport outside of the CONUS. **(T-2)** (PAGE 77 INSERT)

Enclosure 5 – Security Education and Training

3. Covered Personnel shall complete the DoD Initial Orientation and Awareness training within 60 calendar days of assignment. (T-2) Completion of this training must be accounted for as follows: (1) Training certificate of completing the DoD Initial Orientation and Awareness e-Learning module from the Center for Development of Security Excellence (CDSE); (2) Transcript reflecting completion of the DoD Initial Orientation and Awareness e-Learning module via myLearning; (3) Transcript reflecting completion of the DoD Annual Security Awareness e-learning module via the Joint Knowledge Operations (JKO) Learning Management System (LMS); or (4) Documentation signed by the member acknowledging completion of either the Initial Orientation Awareness or Annual Security Refresher training requirement. (T-2) *Note: Completion of this training is not required by personnel who are TDY or attending a formal training course at SAFB.* (PAGE 85)

3.c. As a prerequisite to being granted access to classified information, Cleared Personnel shall complete Information Security Indoctrination training, which also encompasses NATO Security Awareness and Classified Marking training, prior to being granted access to a classified level/caveat(s) as recorded in DISS (or successor system) by their assigned SMO. (T-2) This training will be presented by their SMO via the material provided by the 82 TRW/IP. (T-3) Completion of this training must be recorded in DISS (or successor system). (T-2) *Note: This pertains to personnel who are TDY or attending a formal training course at SAFB, only if they require access to classified information while assigned to a SMO at SAFB.* (PAGE 86)

3.c.(3) Cleared Personnel shall complete Derivative Classification training prior to being granted access to a classified level/caveat(s) as recorded in DISS (or successor system) by their assigned SMO. (T-2) Completion of this annual training requirement must be accounted for as follows: (1) Unit ancillary training report pulled from myLearning, DAF e-Learning, and/or JKO LMS e-Learning transcripts; (2) Certificate of training of completing the Derivative Classification e-Learning module via JKO LMS or CDSE; or (3) Documentation signed by the member acknowledging completion of this training requirement. (T-2) *Note: Completion of this training is not required by personnel who are TDY or attending a formal training course at SAFB.* (PAGE 86)

3.c.(8) As a prerequisite to granting access to classified NATO material, the NATO Briefing Certificate available for download from the 82 TRW/IP SharePoint site shall be completed and signed by individuals requiring access to this material as well as their SA and Commander. (T-2) (PAGE 88)

3.c.(9) As a prerequisite to granting access to Critical Nuclear Weapons Design Information (CNWDI), the CNWDI briefing memorandum available for download from the 82 TRW/IP SharePoint site shall be completed and signed by individuals requiring access to this material. (T-2) (PAGE 88)

7. Annual Refresher Training

7.a. Covered Personnel shall complete DoD Annual Security Awareness Refresher training, which also encompasses Continuous Evaluation reporting requirements. (T-2) Completion of this annual training requirement must be accounted for as follows: (1) Unit ancillary training report pulled from myLearning, DAF e-Learning, and/or JKO LMS e-Learning transcripts; (2) Certificate of training of completing the DoD Annual Security Awareness e-Learning module via JKO LMS or CDSE; or (3) Documentation signed by the member acknowledging completion of this training requirement. *Note: Completion of this training is not required by personnel who are TDY or attending a formal training course at SAFB.* (PAGE 92)

7.c. Enclosure 5, paragraph 3.c.(3), outlines Derivative Classification training requirements for Cleared Personnel. Personnel who are not current with this training cannot generate classified material and will lose their access to a classified information system. (T-2) (PAGE 92)

9. Termination Briefing

9.f. (Added) An AF Form 2587, *Security Termination Statement*, must be completed under the following conditions. (PAGE 94 INSERT)

9.f.(1) (Added) Upon terminating a member's access to a classified NATO caveat, Restricted Data (RD) and/or Critical Nuclear Weapons Design Information (CNWDI). (PAGE 94 INSERT)

9.f.(2) (Added) When an individual(s) who requires a clearance eligibility for their assigned duties separates or retires. (PAGE 94 INSERT)

9.f.(3) (Added) Access to classified material is being suspended by a commander or director. (PAGE 94 INSERT)

9.g. (Added) Completing an AF Form 2587 is not required for a Permanent Change of Station or Assignment. However, debriefing/removing a person's access to a classified level/caveat(s) granted by their losing SMO in DISS or successor system is required. (PAGE 94 INSERT)

Enclosure 6 – Security Incidents Involving Classified Information

6. Security Inquiries and Investigations

6.d.(1)(a)1. **(Added)** If the commander or director is involved in the incident, appointment of the inquiry official (IO) will be elevated to the next level of command. An inquiry official must be available for at least 90 calendar days after being appointed. A copy of the appointment memorandum must be provided to 82 TRW/IP. (PAGE 103 INSERT)

6.d.(1)(b)1. **(Added)** In lieu of a formal inquiry for a reportable security incident, commanders or directors may, after consulting with the CIP, submit a memorandum promptly identifying a Practice Dangerous to Security (PDS) to 82 TRW/IP within 10 duty days. A PDS may be considered for those incidents where the time and cost of conducting a formal inquiry are not warranted, and with concurrence of the CIP. The PDS memorandum shall clearly identify the key elements of who, what, when, where, and/or how-type questions; any recommendations and/or actions to prevent future occurrences; and any warranted disciplinary or punitive action. The CIP will ensure a brief technical review is completed, and

either formally concur on closing the matter as a PDS or direct other necessary actions, including declaring the need to accomplish a formal inquiry. (PAGE 103 INSERT)

6.d.(3)(b) The appointing authority will notify 82 TRW/IP, in-writing, of approved extensions. (PAGE 104)

6.d.(3)(c) **(Added)** The appointing authority will close preliminary inquiries within 10 duty days of receipt from the IO. The appointing authority will provide a copy of the final report to the 82 TRW/IP and their SA to file in Tab 8 of the SMO program binder. (PAGE 104 INSERT)

Enclosure 7 – IT Issues for the Security Manager

5. Data Spills

5.c.(1) Negligent Discharge of Classified Information (NDCI) incidents, or classified data spills, must be reported to the Sheppard Communications Focal Point (82 CS/SCOS) and the 82 TRW/IP. (PAGE 119)