DEPARTMENT OF THE AIR FORCE
AIR EDUCATION AND TRAINING COMMAND

DoDM5200.01V1_DAFMAN16-1404V1_SHEPPARDAFBGM2026-01

28 May 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, V1_DAFMAN16-1404, V1, Information Security Program: *Overview, Classification and Declassification*

RELEASABILITY: There are no releasability restrictions on the publication.

By order of the Installation Commander, this Sheppard AFB Guidance Memorandum immediately implements changes to DoDM 5200.01, V1_DAFMAN 16-1404, V1. 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 DoDM5200.01V1_DAFMAN16-1404V1_SHEPPARDAFBGM2025-01, 27 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 http://dpclo.defense.gov/Privacy/SORNs.aspx.

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 16-1404-1, *Classified Reproduction Rules,* 20230516
SAFB VA 16-1404-2, *No Classified Reproduction,* 20230516
SAFB VA 16-1404-5, *Classified Work in Progress,* 2026XXXX
SAFB VA 16-1404-6, *Your Security Assistant Is,* 20230516

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 who require access to classified information.

Uncleared Personnel – Civilian and contractor personnel who do not require a national security background investigation 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 Security Assistant.

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 – Responsibilities

7.n.(5) Wing (Installation Commander)

7.n.(5)(a). The 82 TRW Deputy Commander (82 TRW/CD) is authorized to ensure security controls, safeguards, and countermeasures are established through application of risk management principles, as appropriate for the 82 TRW and tenant organizations reporting through the 82 TRW Information Protection Office (82 TRW/IP). **(T-2)** (PAGE 25)

7.n.(5)(d). The 363d Training Squadron Commander (363 TRS/CC) is designated as the SAFB Restricted Data (RD) Management Official. The 363 TRS/CC will appoint, in writing, individuals assigned to the 363 TRS as RD Program Managers since most of this type of material is maintained within their organization. **(T-2)** Provide a copy of the appointment letter to 82 TRW/IP and organizations that store and/or handle this type of material. (PAGE 26)

7.n.(5)(e). The establishment or verification of a servicing NATO sub-registry or control point is delegated to the squadron or equivalent level commander or director whose organizations are in possession of this type of material. **(T-2)** (PAGE 26)

7.n.(5)(f). This entry serves as formal documentation that the 82 TRW Commander (82 TRW/CC) has determined that Security-In-Depth exists for units/organizations located on Sheppard Air Force Base (SAFB). As a general policy, supplemental control determinations have been delegated to local commanders and directors. The 82 TRW/CC must be notified through the Chief, Information Protection (CIP) when such supplemental control measures differ from those identified and recommended in para 7.n.(6)(c)4. of this guidance memorandum. **(T-2)** (PAGE 26)

7.n.(5)(g). The CIP will ensure information security program inspections (herein afterwards referred to as security management program inspections) are conducted at least annually for all organizations supported by the 82 TRW/IP. **(T-1)** Security management program inspections are horizontal inspections which consist of the 82 TRW/IP evaluating each supported organizations' information security, personnel security, industrial security, controlled unclassified information, counter-insider threat reporting and operations security programs. Information accumulated from security management program inspections will be used by the 82 TRW/IP to populate the annual Senior Agency Self-Inspection Report to the Information Security Oversight Office (ISOO). **(T-2)** (PAGE 26)

7.n.(5)(g)1. **(Added)** Deficiencies noted during security management program inspections will be placed in the Inspector General Evaluation Management System (IGEMS). **(T-1)** The 82 TRW/IP will utilize the Security Management Program Inspection checklist to convey compliance thresholds for requirements that are evaluated via a sampling strategy. **(T-2)** (PAGE 26 INSERT)

7.n.(5)(g)2. **(Added)** The guidance outlined in 82 TRW Commander's Inspection Program (CCIP) Business Rules will be utilized to manage self-assessment program, waivers, and security management program inspection requirements for organizations supported by the 82 TRW/IP. **(T-2)** Business rule requirements may, however, differ for non-82 TRW organizations supported by the 82 TRW/IP. (PAGE 26 INSERT)

7.n.(5)(g)3. **(Added)** The 82 TRW/IP may conduct a Staff Assistant Visits (SAV) to evaluate security program requirements if requested by a commander or director; however, a written report will not be generated. Additionally, SAVs will not be performed by the 82 TRW/IP within 90 calendar days of a unit's security management program inspection. (PAGE 26 INSERT)

7.n.(5)(h). Open storage (hereafter referred to as secure room) certification and revalidation is delegated to the CIP. **(T-2)** (PAGE 26)

7.n.(5)(j) **(Added)** The Standard Operating Procedure (SOP) at Attachment 1 of this guidance memorandum establishes protocols for conducting Random Entry and Exit Inspections for vaults and secure rooms located on Sheppard AFB that contain or store significant amounts of classified material, as determined and directed by the installation commander or subordinate commanders. (PAGE 27 INSERT)

7.n.(6) Wing (Installation) Chief, IP

7.n.(6)(a)1.a. **(Added)** Unit Security Assistants (SA) and Security Container Custodians (SCC), will be formally trained by 82 TRW/IP no later than 120 calendar days after being appointed. **(T-2)** Personnel Security Custodians (PSC) will be provided familiarization training by their unit SA on the System of Record used to manage DoD Personnel Security requirements. **(T-3)** (PAGE 27 INSERT)

7.n.(6)(b)3. This instruction serves and meets the requirement for a unit security plan/instruction by incorporating all minimum requirements. Commanders may accept this instruction in lieu of developing a separate security plan/instruction for their unit. Units may further supplement and enhance requirements through issuance of unit security plan/instruction, which must be coordinated through the 82 TRW/IP prior to being published. (PAGE 27)

7.n.(6)(b)3.a. Sample Emergency Action Plans are available on the 82 TRW/IP SharePoint site for units to tailor to their specific mission requirements. Once complete, these plans must be readily available outside of each applicable security container and posted within each secure room. **(T-2)** Note: Only one set of plans needs to be posted if emergency procedures are applicable to assets stored within multiple security containers located inside a single room. (PAGE 27)

7.n.(6)(b)3.c. The SAFB Command Post is designated as the overnight repository for classified material and is the designated storage facility for transit or emergency storage of classified information/material up to Top Secret. (PAGE 27)

7.n.(6)(b)3.e. Wireless electronic devices (cell phones, personal digital assistants, cordless phones, personal fitness devices, etc.), and cameras create an unacceptable risk and are prohibited in a classified processing area (CPA). *Exception – Emergency Medical Device (EMD) may be used within a designated CPA if approved per the Standard Operating Procedure (SOP) at Attachment 2 of this guidance memorandum.* To alert personnel of prohibited devices prior to entering, CPA officials will ensure the following visual aids are posted at each entry control point. SAFBVA 16-1404-5, *Classified Work in Progress*, and for CPAs with a TEMPEST requirement, SAFBVA 33-6, *Sheppard AFB TEMPEST*. **(T-2)** (PAGE 27)

7.n.(6)(b)3.e.1. **(Added)** The following actions will be taken if an unauthorized wireless electronic device is discovered in a CPA **(T-2)**: (1) Contact the 82d Security Forces Squadron (82 SFS) Base Defense Operations Center (BDOC) at 940-676-2981 or 2982 in addition to notifying the unit Security Assistant and Commander. (2) Maintain positive control of the device. (3) Do not attempt to use, plug in, or log into the device to verify unauthorized use. (4) Instruct the device owner/user to remain in place until a representative from 82 SFS arrives. Do not attempt to forcibly hold an individual; however, be prepared to provide 82 SFS a detailed description and direction/mode of travel for those who flee the scene. (PAGE 28 INSERT)

7.n.(6)(b)3.g. Classified reproduction equipment (copiers, scanners, and/or fax machines) will be designated in writing by the commander or director. **(T-2)** Classified reproduction will not be approved/authorized for equipment that is connected to an unclassified network. **(T-2)** Classified reproduction will not be approved/authorized for equipment with an internal hard drive unless it is within a secure room. **(T-2)** (PAGE 28)

7.n.(6)(b)3.g.1. **(Added)** SCCs will ensure authorized users are informed of classified reproduction procedures. **(T-2)** Procedures are outlined within SAFBVA 16-1404-1, *Classified Reproduction Rules*, which must be posted on and/or above all equipment authorized for this purpose. **(T-2)** Note: Commanders may authorize equipment items on contract for classified reproduction, only if the hard drive is removed and turned over to the unit prior to return of the equipment to the contractor. (PAGE 28 INSERT)

7.n.(6)(b)3.g.2. **(Added)** SAFBVA 16-1404-2, *No Classified Reproduction*, must be posted on and/or above all equipment items not authorized to reproduce classified material which are in a CPA. **(T-2)** (PAGE 28 INSERT)

7.n.(6)(c)3. **(Added)** Secure room certification/construction/modification must be coordinated by units through the 82 TRW/IP as outlined in volume 3, enclosure 3, paras 3.b.(5)(a) – 3.b.(5)(c) of this instruction. **(T-2)** Secure rooms will not be approved solely for convenience. (PAGE 28 INSERT)

7.n.(6)(c)4. **(Added)** Commanders and directors that concur with para 7.n.(5)(f) of this instruction referencing Security-In-Depth, and volume 3, enclosure 3, para 4.a., to this instruction referencing the SAFB historical risk assessment, shall select from the following recommended supplemental security controls: (a) an employee cleared to at least the Secret level shall inspect the secure room and/or vault at least every 4 hours; or (b) an intrusion detection system (IDS) meeting the requirements of Appendix to Enclosure 3 to DoDM 5200.01-V3 with personnel responding to alarms arriving within 30 minutes of the alarm annunciation. **(T-2)** If supplemental control option (b) reference IDS is selected and employed, custodians may establish the minimum 4-hour checks in event of an IDS malfunction per SAFB Base Defense Plan 31-101. (**T-2)** If a commander or director does not concur with the above-referenced Security-In-Depth, Risk Assessment, or recommended supplemental security controls, they must notify the 82 TRW/CC through the CIP. **(T-2)** (PAGE 28 INSERT)

7.n.(6)(e) **(Added)** Ensure meetings are held at least annually with SAs. **(T-2)** Attendance is mandatory by at least one SA per Security Management Office (SMO). **(T-2)** (PAGE 28 INSERT)

7.n.(7) Commanders or Directors

7.n.(7)(a)1. Appoint a primary SA to manage program requirements. **(T-2)** There are no grade restrictions; however, SAs must have a Secret or higher clearance eligibility. **(T-2)** (PAGE 28)

7.n.(7)(a)1.a. **(Added)** The appointment memorandum must include the SA's full name, rank/grade, organization, office symbol and phone number and be submitted to 82 TRW/IP prior to personnel being granted access to resources that will enable execution of the unit security management program. **(T-2)** (PAGE 28 INSERT)

7.n.(7)(a)3. **(Added)** Appoint an alternate SA(s) based on operational needs. (PAGE 29 INSERT)

7.n.(7)(a)4. **(Added)** Appoint as many PSCs and SCCs as necessary for executing security management program requirements under the authority and oversight of the SA(s). A copy of the most current PSC and SCC appointment memorandums must be provided to 82 TRW/IP. There are no grade restrictions; however, PSCs and SCCs must have the minimum Secret clearance eligibility to perform the duties assigned to them under the SA(s). **(T-2)** (PAGE 29 INSERT)

7.n.(7)(a)5. **(Added)** Ensure SAs and SCCs complete initial training provided by 82 TRW/IP no later than 120 calendar days after appointment. **(T-2)** Note: Due to the amount of training required and the scope of duties, commanders are highly encouraged to appoint personnel as a SA or SCC, only if they are available to perform these duties for at least 12 months. (PAGE 29 INSERT)

7.n.(7)(b). Develop a unit security plan/instruction if (a) the unit handles or maintains classified information and (b) unique requirements are not covered by this instruction or within higher headquarters' guidance. **(T-2)** Route the plan/instruction through 82 TRW/IP for coordination. **(T-2)** (PAGE 29)

7.n.(7)(d). Ensure assigned permanent party personnel who are indoctrinated and granted access to a classified level/caveat(s) as recorded in the Defense Information System for Security (DISS) or successor system by their Security Management Office (SMO), complete derivative classification training at least annually as outlined in Volume 3, Enclosure 5 of this instruction. **(T-2)** Access to classified material shall be discontinued on permanent party personnel who are not current with derivative classification training. **(T-2)** (PAGE 29)

7.n.(7)(g). **(Added)** Notify 82 TRW/IP of all secure room modifications to ensure changes do not affect its certification. **(T-2)** (PAGE 29 INSERT)

7.n.(7)(h). **(Added)** Include the SAs in the organization in/out processing checklist. **(T-3)** (PAGE 29 INSERT)

7.n.(7)(i). **(Added)** Ensure SAFBVA 16-1404-5, *Classified Work in Progress*, is posted at the entry control point(s) of CPAs to alert individuals requesting entry. **(T-2)** (PAGE 29 INSERT)

7.n.(7)(j). **(Added)** Ensure personnel security records for members are accurately managed in their unit SMO within DISS or successor system, which includes: (PAGE 29 INSERT)

7.n.(7)(j).1. **(Added)** Maintaining an "Owning" relationship in DISS for all permanent party military and civilian personnel assigned to a SAR code 5, 6 or 7 position via the unit's manpower document. **(T-2)** Those who have a need to generate, reproduce, view, hear, and/or discuss classified material in the performance of their official duties, possess an in-scope clearance eligibility and have completed a SF 312, *Classified Information Non-Disclosure Agreement*, shall be indoctrinated and granted access to the applicable classified level/caveat(s) as recorded in DISS or successor system by their SMO. **(T-2)** Permanent party personnel shall not be granted access to classified material prior to completion of these actions. **(T-2)** (PAGE 29 INSERT)

7.n.(7)(j).2. **(Added)** Maintaining an "Owning" or "Servicing" relationship in DISS for student personnel who require access to classified material during training. **(T-2)** Those who possess an in-scope clearance eligibility and have completed a SF 312, shall be indoctrinated and granted access to the applicable classified level/caveat(s) as recorded in DISS or successor system by their training unit SMO. **(T-2)** The training unit SMO may also inherit the applicable classified level/caveat(s) denoted on a Visit Request submitted in DISS by the student's home unit SMO. Student personnel shall not be granted access to classified material prior to completion of these actions. **(T-2)** (PAGE 29 INSERT)

7.n.(7)(j).3. **(Added)** Maintaining a "Servicing" relationship in DISS for assigned contractors who, per their contract, require access to classified material. **(T-2)** The SMO sponsoring the classified contract will inherit the applicable classified level/caveat(s) for contract personnel denoted on the Visit Request submitted in DISS by contractor's Facility Security Officer (FSO). **(T-2)** Doing so satisfies the requirements for verifying an individual's clearance eligibility, completing an SF-312, and ensuring they are formally indoctrinated and granted access to the appropriate classified level/caveat(s), as recorded in DISS or its successor system by the FSO. Contractor personnel shall not be granted access to classified material prior to completion of these actions and/or if not driven by the contract. **(T-2)** (PAGE 29 INSERT)

7.n.(7)(j).4. **(Added)** Maintaining an "Owning" relationship in DISS for assigned contractors who, per their contract, do not require access to classified material; however, require a Common Access Card or a Non-classified Internet Protocol Router Network Enterprise Alternate Token System (NEATS) Token. **(T-2)** (PAGE 29 INSERT)

7.n.(7)(k). **(Added)** Ensure SAFBVA 16-1404-6, *Your Security Assistant Is,* is made available to all assigned unit personnel. **(T-3)** (PAGE 29 INSERT)

7.n.(7)(l). **(Added)** Maintain program documentation described in paragraph 7.n.(7)(1).1. through 7.n.(7)(l).11. of this guidance memorandum in a location accessible to all SAs within the organization. **(T-2)** Recommend using the SMO continuity binder on the 82 TRW/IP SharePoint site for this purpose. (PAGE 29 INSERT)

7.n.(7)(l).1. **(Added)** Tab 1, Appointment Memorandums for SA(s), PSC(s), and SCC(s). Note: SCC appointment memorandum must list container type, lock type, location, and unique unit identification, serial, or secure room number. Maintain most current memo(s). (PAGE 29 INSERT)

7.n.(7)(l).2. **(Added)** Tab 2, Training Documentation. Two subfolders: (1) Certificate(s) of Training for SA(s) and (2) Certificate(s) of Training for SCC(s). Maintain until removed from appointment. Note: SMO are not required to maintain Security Education, Training and Awareness (SETA) records for permanent party personnel who have a current transcript – provided to the SMO by their Unit Training Manager – of SETA completed via myLearning, Joint Knowledge Operations (JKO), and/or DAF e-Learning. However, if a transcript is not provided, SETA completion must be maintained by the SMO via the following: (1) Current training certificate(s) of completing the applicable e-Learning module from MyLearning, JKO, DAF e-Learning or the Center for Development of Security Excellence. or (2) Signed documentation from the member acknowledging completion of the required SETA. Maintain most current SETA documentation. (PAGE 29 INSERT)

7.n.(7)(l).3. **(Added)** Tab 3, Security Termination Statements. Maintain current and past 2 calendar years. (PAGE 29 INSERT)

7.n.(7)(l).4. **(Added)** Tab 4, Listing of Approved Classified Reproduction Equipment. Must include type, manufacturer, model number, and location. Maintain until no longer needed. (PAGE 29 INSERT)

7.n.(7)(l).5. **(Added)** Tab 5, Industrial Security Documents for Classified Contracts. Includes at a minimum DD Form 254(s), *DoD Contract Security Classification Specification*; Visitors Group Security Agreement(s); and memorandum identifying facility security officer(s) or on-site visitor group security representative(s) if classified holdings or actions occur for contractor employees sponsored under the unit SMO. Maintain most current documentation. (PAGE 29 INSERT)

7.n.(7)(l).6. **(Added)** Tab 6, Manpower Programming and Execution System (MPES) Position Code Review Memorandum. Maintain most current memorandum. (PAGE 29 INSERT)

7.n.(7)(l).7. **(Added)** Tab 7, Classified Material Cleanout Memorandum(s), Destruction Equipment Memorandum(s) and Security Container/Vault Door Visual Inspection Checklist(s). Maintain the most current memorandum(s) and checklist(s). (PAGE 29 INSERT)

7.n.(7)(l).8. **(Added)** Tab 8, Security Incident and Unauthorized Disclosure of CUI Inquiry and/or Investigation Reports. Maintain current and past 2 calendar years. (PAGE 29 INSERT)

7.n.(7)(l).9. **(Added)** Tab 9, Secure Room Certification Memorandum(s). Maintain most current memorandum(s). (PAGE 29 INSERT)

7.n.(7)(l).10. **(Added)** Tab 10, Unit operating instructions, written plans and/or standard operating procedures. Maintain most current documentation. (PAGE 29 INSERT)

7.n.(7)(l).11. **(Added)** Tab 11, Classified Access Authorization Documentation. Four subfolders. (1) AF Form 2583 and Temporary Access (a.k.a. Interim Clearance) Memorandum signed by the commander. Maintain until a final clearance eligibility is granted or temporary access is no longer needed. (2) Commander's Memorandum of Positions and Ancillary Duties Authorized Access to Classified Information. Maintain the most current memorandum. (3) NATO Security Briefing Certificate. Maintain until access to NATO classified information is no longer needed. (4) Critical Nuclear Weapons Design Information (CNWDI) briefing memorandum. Maintain until access to CNWDI is no longer needed. (PAGE 29 INSERT)

7.n.(7)(l).12. **(Added)** Tab 12, Miscellaneous. Note: Do not maintain documentation governed by the privacy act that is not required for program management. (PAGE 29 INSERT)

7.n.(7)(m). **(Added)** If a unit possesses classified holding(s), ensure the following program requirements are executed by SCC(s) under the oversight of SA(s). SCC(s) shall: **(T-2)** (PAGE 29 INSERT)

7.n.(7)(m).1. **(Added)** Ensure all personnel granted unescorted access to a security container/vault/secure room used to store or process classified material receive training on access control and safeguarding procedures. This includes briefing personnel authorized to remove classified material from a security container/vault/secure room of their safeguarding responsibilities. (PAGE 29 INSERT)

7.n.(7)(m).2. **(Added)** Update and route SCC appointment and container access memorandum(s) through their SA(s) to their commander for signature. The appointment memorandum must be submitted to 82 TRW/IP. (PAGE 29 INSERT)

7.n.(7)(m).3. **(Added)** Control and manage the combination to their security container/vault/secure room. Also ensure at a minimum a primary and alternate SCC is listed on the Standard Form (SF) 700, *Security Container Information*. (PAGE 29 INSERT)

7.n.(7)(m).4. **(Added)** Ensure classified material under their control is properly destroyed when required. (PAGE 29 INSERT)

7.n.(7)(m).5. **(Added)** Oversee annual cleanout requirements of material under their charge, which includes (1) reviewing classified holdings stored within their security container(s)/vault(s)/secure room(s) for retainability, required markings, possible destruction, and/or possible declassification; (2) checking the functionality of equipment used to destroy classified and its currency on the NSA Evaluated Products List; and (3) performing an operational visual inspection on security container(s)/vault(s)/secure room(s). They will also forward the applicable documentation to their SA(s) accounting for the completion and results of the cleanout. (PAGE 29 INSERT)

7.n.(7)(m).6. **(Added)** Ensure an Optional Form (OF) 89, *Maintenance Record for Security Containers/Vault Doors*, or successor form is maintained inside the locking drawer of each security container and on the inside of the entrance door of each vault/secure room under their charge. They will also ensure all maintenance performed on a security container/vault/secure room is recorded on the OF 89. (PAGE 29 INSERT)

7.n.(7)(m).7. **(Added)** Maintain a current list of individuals authorized by the commander for unescorted access and/or knowledge of combination(s) to their security container/vault/secure room. (PAGE 29 INSERT)

7.n.(7)(m).8. **(Added)** Maintain an inventory list of all classified holdings stored within each security container/vault/secure room. Inventory listing must be placed within the immediate proximity inside or outside the associated security container/vault/secure room. (PAGE 29 INSERT)

7.n.(7)(m).9. **(Added)** Ensure classified holdings on the inventory list, that are removed from a security container/vault/secure room, are checked out via hand receipt, charge-out form, etc. until returned. (PAGE 29 INSERT)

7.n.(7)(m).10. **(Added)** Post an Emergency Action Plan in a visible location within the immediate proximity outside of their container(s) and/or inside of each vault/secure room. Note: Only one plan needs to be posted if emergency procedures are applicable to assets stored within multiple security containers which are located inside a single vault/secure room. (PAGE 29 INSERT)

7.n.(7)(m).11. **(Added)** Prohibit the use of electronic devices in CPAs such as cell phones, cameras, tablets, portable wearable fitness devices and other devices that have photographic, video or audio recording capabilities. This includes unapproved EMDs. (PAGE 29 INSERT)

7.n.(7)(m).12. **(Added)** Ensure newly acquired equipment under their charge that is intended to be utilized for classified destruction is evaluated for functionality and currency on the NSA Evaluated Products List. (PAGE 29 INSERT)

7.n.(7)(m).13. **(Added)** Ensure items stored inside a security container/vault/secure room with classified material or within a high use CPA are marked to reflect its classification and/or unclassified status. High use CPAs at a minimum are those areas where classified operating system(s) are connected to the network, vault(s)/secure room(s), as well as routinely utilized operating locations with an abundance of classified co-located with unclassified material. (PAGE 29 INSERT)

7.n.(7)(n). **(Added)** Commanders, their Deputies, and First Sergeants must complete training provided by 82 TRW/IP on reporting incidents that meet one or more Security Executive Agency Directive 3 (SEAD-3) and/or DoW Insider Threat Program enterprise threshold reporting criteria. This training must be accomplished within 60 days of in-processing. **(T-2)**

Enclosure 3 – DoD Information Security Program Overview

12. Access to Classified Information

12.a.(4). **(Added)** Access and indoctrination to the applicable classified level/caveat(s) is recorded in DISS or successor system by the SMO in possession of the classified material. **(T-2)** Note: A SMO with classified holdings may also accept the access level/caveat(s) granted by another SMO for personnel visiting their unit. (PAGE 42 INSERT)

12.b.(1). SA(s) will upload the completed SF 312, *Classified Information Nondisclosure Agreement*, to DISS. **(T-2)** (PAGE 42)

12.c. The Information Security Indoctrination also encompasses NATO security awareness and classified marking training. Indoctrination training will be accounted for in DISS upon recording an individual's access level/caveat(s) under their unit SMO. **(T-2)** (PAGE 43)

12.c.(1). **(Added)** SAs will utilize the NATO Briefing Certificate on the 82 TRW/IP SharePoint site to account for an individual's need to know, possession of the requisite security clearance and receipt of the NATO security briefing prior to granting access to classified NATO material. **(T-2)** (PAGE 43 INSERT)

12.e. **(Added)** SAs will utilize the CNWDI Briefing Memorandum on the 82 TRW/IP SharePoint site to account for an individual's receipt of the CNWDI security briefing prior to granting access to CNWDI material. **(T-2)** (PAGE 43 INSERT)

Attachment 1

SHEPPARD AFB
Random Entry and Exit Inspections

Purpose	This Standard Operating Procedure outlines procedures for Random Entry/Exit Inspection (REEI) for vaults and open storage areas/rooms (hereinafter referred to as secure facilities) on Sheppard AFB (SAFB) that process or store significant amounts of classified material, as directed by the installation or subordinate commander. REEIs are conducted in direct compliance with DoDM5200.01, Vol 1, DAFMAN16-1404, Vol 1, DAFGM2024-01 and SAFB Plan 31-145, Vol 1. They are designed to deter the unauthorized removal of classified material from and the introduction of prohibited items into secure facilities. REEIs are not intended to harass personnel but to ensure security protocols are being followed. REEIs at SAFB are integrated into the Antiterrorism Program as a Random Antiterrorism Measure.
Responsibilities	a. The IPO will • Provide oversight and guidance on REEI implementation. • Train affected unit Security Assistants (SA) on approved REEI procedures. • Evaluate compliance with REEI requirements by affected units during annual security management program inspections. b. Unit SA(s) with cognizant oversight of secure facilities will • Train inspection designee(s) on approved REEI procedures. • Ensure signs are posted at secure facility entrances advising personnel of the potential for inspection of all items in their possession, to include but not limited to backpacks, purses, portable electronic devices, pockets, etc. • Notify unit Antiterrorism Representative(s) when REEIs are completed. • Maintain a log of completed REEIs for at least two complete calendar years IAW AF Records Information Management System Table 33-46, Rule 31.00. • Review REEI logs for trends and repeat violators. • Incorporate compliance with REEI requirements in self-assessment program.
REEI Procedures	a. Secure facilities with multiple entrances/exits will be brought to a single entry/exit control point (ECP). b. There will be at least three inspectors (of a male and female mix, if possible). Two to inspect those entering the ECP and a third to observe members awaiting inspection for suspicious behavior(s). c. Care will be taken not to damage personal property. d. Obtain Common Access Card from everyone being inspected and read the following statement: *"My name is_____from the [Unit] and we are conducting a Random Entry/Exit Inspection by order of the Installation or [Unit] Commander. You have been selected to be inspected. The intent of this inspection is to ensure the safety and security of government personnel, property, and sensitive or classified information. I am required to inspect your hand-carried items, electronics and the contents of your pockets. Failure to comply with this inspection may result in possible administrative or Uniform Code of Military Justice (UCMJ) action and/or revocation/suspension of access, until an access determination can be made by the responsible commander."* e. Each inspector at ECP will inspect a member, instructing them to remove all

	outer garments (e.g. coats, jackets, hats, service blouses), open all hand-carried items and empty all pockets. f. Inspect all hand-carried briefcases, handbags, luggage, packages, lunch bags, athletic bags, etc. for prohibited items. • Have owner open hand-carried items being inspected. • Inspect all compartments that could store contraband or government property. • If needed, have individual(s) remove large material from hand-carried items to conduct visual observation. • A complete emptying of hand-carried item(s) is not required. g. Inspect binders/notebooks/planners and loose papers by having owner flip through pages . h. Inspect all pockets, which should be turned inside-out, if possible, by individual(s) being inspected. i. Have individual(s) with Electronic Medical Device(s) provide approval documentation. ***IMPORTANT NOTE: At no time will an inspector physically touch individual(s), except in the case of self-defense.***
REEI Findings or Adverse Procedures	a. For personnel entering a secure facility: if an individual refuses inspection of their hand-carried items, electronics and/or pockets after the reading of the initial inspection notification as detailed above, the REEI inspector will advise the member of the following: *"Your refusal to this mandatory inspection requires me to confiscate your CAC, deny you entry, temporarily hold you and notify law enforcement to assist in this inspection. I am also required to notify the unit security assistant(s) and commander. Please remain here while I report the incident and await the arrival of law enforcement personnel."* The inspector will contact Security Forces at 940-676-2981 or 2982 in addition to notifying the unit security assistant and Commander while maintaining positive visual control over the individual. Inspector(s) will not attempt to forcibly hold an individual, however, must be prepared to provide Security Forces a detailed description and direction/mode of travel of those who flee the scene. In all cases, inspectors will document finding(s) on the REEI Worksheet. b. For personnel departing a secure facility: if an individual refuses inspection of their hand carried items, electronics and pockets after reading of the initial inspection notification as detailed above, the REEI inspector will advise the member of the following: *"Your refusal to this mandatory inspection requires me to confiscate your CAC, temporarily hold you, and notify law enforcement to assist in this inspection. I am also required to notify the unit security assistant and commander. Please remain here while I report the incident and await the arrival of law enforcement personnel."* The inspector will contact Security Forces at 940-676-2981 or 2982 in addition to notifying the unit security assistant and Commander while maintaining positive visual control over the individual. Inspector(s) will not attempt to forcibly hold an individual, however, must be prepared to provide Security Forces a detailed description and direction/mode of travel of those who flee the scene. In all cases, inspectors will document finding(s) on the REEI Worksheet. c. Discovery of prohibited items *(e.g. includes but is not limited to recording*

	devices, photographic devices or wireless devices) upon entering or exiting a secure facility: If the REEI inspector finds prohibited items during an entry inspection, those items may be returned to allow the individual(s) being inspected to properly store them outside the secure facility after documenting the finding on the REEI Worksheet. If the REEI inspector discovers prohibited items during an exit inspection, they will positively control the item and instruct the individual(s) to remain in place under the direct observation of an inspector. The REEI inspector will also contact the Security Forces at 940-676-2981 or 2982 in addition to notifying the unit security assistant and Commander. Inspectors will not attempt to forcibly hold an individual, however, must be prepared to provide Security Forces a detailed description and direction/mode of travel for those who flee the scene. In all cases, inspectors will document finding(s) on the REEI Worksheet. d. Discovery of classified material upon entering or exiting a secure facility: If the REEI inspector finds classified material during an entry or exit inspection, have the individual being inspected provide a valid Courier Authorization Letter or Courier Card (DD Form 2501). If the individual(s) being inspected does not have a valid courier credential(s), the REEI inspector will maintain positive control of the material and instruct the individual(s) to remain in place under the direct observation of a REEI inspector. The inspector will also contact the unit security assistant and/or Commander to check if the individual(s) is authorized to hand carry the classified material in lieu of being issued courier credential(s). If individual(s) hand carrying of classified material is deemed unauthorized, the inspector will contact Security Forces at 940-676-2981 or 2982. Inspectors will not attempt to forcibly hold an individual, however, must be prepared to provide Security Forces a detailed description and direction/mode of travel for those who flee the scene. In all cases, inspectors will document finding(s) on the REEI Worksheet. e. Discovery of Contraband *(e.g. includes but not limited to illegal drugs, weapons, ammunition, or stolen property)* upon entering or exiting a security facility: If the REEI inspector discovers contraband, they will not touch it, will direct the individual(s) not to touch it and to remain in place under the direct observation of a REEI inspector. The inspector will also contact Security Forces at 940-676-2981 or 2982 in addition to notifying the unit security assistant and Commander. Inspectors will not attempt to forcibly hold an individual, however, must be prepared to provide Security Forces a detailed description and direction/mode of travel for those who flee the scene. In all cases, inspectors will document finding(s) on the REEI Worksheet.

Attachment 2

Electronic Medical Device (EMD) Request Process

Disclaimer	This Standardized Operating Procedure (SOP) applies to all units on Sheppard AFB. It is not applicable to geographically separate units who must adhere to the guidance provided by their host installation.
Background	DAF personnel may need to utilize Personable Wearable Devices (PWD), which EMDs are a subset of, within a classified processing area (CPA) with TEMPEST requirements (hereinafter referred to as a CPA) to treat medical issues or disabilities. In accordance with DAFMAN 17-1301, *Computer Security*, devices of this nature may only be authorized in secure spaces by a cognizant authority after consulting with the Certified TEMPEST Technical Authority (CTTA). The following guidance was provided by CTTA regarding EMD(s) in CPA(s): • There is no reciprocity authorizing their introduction and use from one CPA to the next. • They must be identified on the approved TEMPEST package for a given CPA. • Only those identified as "Permitted" on the current National Security Agency (NSA) Office of Security & Counterintelligence (S&CI) Portable Electronic Devices (PED) listing will be considered by CTTA for approval.
Purpose	This SOP outlines local protocols for processing requests to introduce EMD(s) within CPA(s) with TEMPEST requirements on Sheppard AFB. Other PWD types are strictly prohibited in CPAs of this nature on Sheppard AFB.
Procedures	1. The Requester will provide their unit Security Assistant (SA) a copy of the EMD specifications from the manufacturer and complete Blocks 1 & 2 of the DAF Form 110, *DAF EMD Request Form and Approval Card*. 2. The SA will verify if the device is identified as "Permitted" on the current NSA S&CI PED listing. a. If the device is not permitted, the SA will disapprove the request and notify the Requester, in writing, cc'ing the 82 TRW/IP (IPO) at 82trw.ip@us.af.mil. The SA will also forward the Requestor's DAF Form 110 to the IPO. **--END OF PROCESS--** b. If the device is permitted, the SA will • Ensure the EMD is added to the CPA TEMPEST package. • Obtain the EMD's manufacturer's specifications from the Requestor. • Provide EMD training to the Requestor. • Have the Requestor digitally sign the DAF Form 110, Block 3, User Agreement. • Forward the updated TEMPEST package, manufacturer's specifications, and DAF Form 110 to the Information System Security Manager (ISSM) at 82cs.ia@us.af.mil. ***NOTE: SAs are not the approval authority. They are just providing expectation management to the Requester.*** 3. The ISSM will revalidate if the EMD is identified as "Permitted" on the NSA S&CI PED listing. a. If EMD is not permitted, the ISSM will disapprove request & notify the Requestor, in-writing, cc'ing the SA and IPO. The ISSM will also forward DAF Form 110 to the IPO. **--END OF PROCESS--**

	b. If the EMD is "Permitted", the ISSM will submit the updated TEMPEST package to CTTA for a decision. • If CTTA disapproves, the ISSM will notify the Requestor, in writing, cc'ing the SA and IPO. The ISSM will also forward DAF Form 110 to the IPO. **--END OF PROCESS--** • If the CTTA approves, the ISSM will sign DAF Form 110, Block 4 and forward to the IPO. 4. The IPO will: a. If disapproved, input DAF Form 110 information and request number to the SAFB EMD tracker and maintain for a year. b. If approved, update the SAFB EMD tracker, sign the DAF Form 110, Request Form and Approval Card and return to the SA. 5. Upon receipt of the DAF Form 110 from the IPO, the SA will issue the EMD Approval Card to the Requester and maintain the Request Form until the EMD is removed from TEMPEST package. **--END OF PROCESS--**
Other Considerations	• Requester(s) must have their EMD Approval Card on their person while in the CPA. • IPO will review updates to the NSA S&CI listing for changes in "Permitted" status. o If previously approved EMD(s) are no longer "Permitted", IPO will provide SA(s) affected member(s) name(s) & device(s), cc'ing the ISSM. o SA(s) will, in turn, notify members, in writing, cc'ing the IPO and ISSM. The SA will also collect and forward member(s) EMD request form & approval card to the IPO.