BY ORDER OF THE COMMANDER
SPANGDAHLEM AB (USAFE)

SPANGDAHLEM AIR BASE
INSTRUCTION

16-1401

28 MARCH 2024

Operations Support

INFORMATION PROTECTION

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

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

RELEASABILITY: There are no releasability restrictions on this publication.

OPR: 52 FW/IP

Certified by: 52 FW/CC
(Col Kevin M. Crofton)

Supersedes: AFI16-1404_SPANGDAHLEMABSUP, 7 May 2017

Pages: 38

This publication implements and extends the guidance of Department of the Air Force Policy Directive (DAFDPF) 16-14, *Security Enterprise Governance*; Department of the Air Force Instruction (DAFI) 16-1401, *Information Protection Program*; DAFI 16-1403, *Controlled Unclassified Information*; Department of the Air Force Manual (AFMAN) 16-1404, Volume 1, *Information Security Program: Overview, Classification, and Declassification*; AFMAN 16-1404, Volume 2, *Information Security Program: Marking of Information*; AFMAN 16-1404, Volume 3, *Information Security Program: Protection of Classified Information*; AFMAN 16-1405, *Air Force Personnel Security Program*; and AFMAN 16-1406, Volume 2, *National Industrial Security Program: Industrial Security Procedures for Government Activities*. It establishes policies and procedures for Information Protection within the 52d Fighter Wing (52 FW) and Spangdahlem Air Base (SAB). It applies to all assigned Air Force (AF) civilian, military, and contractors at SAB to include associate organizations per host/tenant support agreements with the 52 FW. This supplement also applies to geographically separated units under the 52 FW. Ensure that all records created as a result of processes prescribed in this publication are maintained in accordance with Air Force Instruction (AFI) 33-322, *Records Management and Information Governance Program,* and disposed of in accordance with 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 DAF Form 847, *Recommendation for Change of Publication;* route DAF Forms 847 through appropriate chain of command. The authorities to waive wing/unit level requirements in this publication are identified

with a Tier ("T-0, T-1, T-2, T-3") number following the compliance statement. See DAFI 90-160, *Publications and Forms Management,* for a description of the authorities associated with the Tier numbers. Submit requests for waivers through the chain of command to the appropriate Tier waiver approval authority, or alternately, to the Publication OPR for non-tiered compliance items.

SUMMARY OF CHANGES

This document has been substantially revised and must be completely reviewed. Roles and responsibilities for various stakeholders have been updated. Detailed procedures for each information protection discipline have been outlined by chapter. Personnel security, industrial security, and controlled unclassified information chapters have been added.

Chapter 1

PROGRAM OVERVIEW

1.1. Overview. This instruction outlines unit information protection program requirements for collateral classified information and controlled unclassified information. It prescribes appointment procedures and responsibilities for commanders and unit Security Assistants for managing and executing the wing IP program. It further addresses procedures and policies of the Information Security (INFOSEC), Personnel Security (PERSEC), Industrial Security (INDUSEC), and Controlled Unclassified Information (CUI) programs.

Chapter 2

ROLES AND RESPONSIBILITIES

2.1. 52 FW/CD:

2.1.1. The Deputy Commander, 52d Fighter Wing (52 FW/CD) is delegated the authority to provide direct oversight for implementing the DAF information protection programs by ensuring security controls, safeguards, and countermeasures are established through application of risk management principles, as appropriate, for the wing and tenant organizations residing on the respective installations when documented in support agreements.

2.1.2. Appoints a Chief, Information Protection (CIP) who resides on the wing special staff and has a clear line of reporting to the 52 FW/CD, for information protection security matters.

2.2. 52 FW Chief of Information Protection:

2.2.1. Executes the information protection program on behalf of the wing commander and provides oversight and direction to group and squadron commanders, directors, activity security managers, assistant security managers, security assistants and the security specialists assigned to the Wing Information Protection Office.

2.2.2. The CIP shall report directly to the 52 FW/CD.

2.2.3. The CIP is delegated the authority to certify and revalidate secure rooms (i.e. open storage areas) as required.

2.3. 52d Civil Engineering Squadron (52 CES). Provides engineering support as needed to evaluate and certify construction standards for secure room/open storage areas.

2.4. 52d Security Forces Squadron (52 SFS):

2.4.1. Serves as the focal point for all Intrusion Detection Systems (IDS) related issues, to include estimates for new installations, changes to existing systems, certifications, and maintenances.

2.4.2. Provides support to evaluate and certify alarm systems for secure rooms/open storage areas.

2.5. 52 MMG/CC. Designates an associate Restricted Data (RD) Management Official in accordance with DoDM 5200.01V3_AFMAN16-1404V3.

2.6. Commanders, Directors, and Staff Agency Chiefs will:

2.6.1. Appoint a primary and alternate Security Assistant (SA) who is a U.S. citizen and has eligibility which allows access to the highest level of material the unit possesses. Submit SA appointment memorandums to 52 FW/IP. Include full name, rank/grade, organization, office symbol, phone number and clearance level using the template provided by 52 FW/IP. When a change occurs, a new appointment letter should be submitted to 52 FW/IP within 10 duty days.

2.6.2. Ensure all (military, civilian and contractor) personnel in/out process through the SA by including the SA as a mandatory item on the organizations in/out processing checklist.

2.6.3. Validate and grant access to classified information for all assigned positions according to the Security Access Requirement (SAR) code on the Unit Manpower Document (UMD).

2.6.4. Appoint, in writing, a Top-Secret Control Officer (TSCO) if the unit handles collateral Top-Secret material.

2.6.4.1. The TSCO shall maintain, for paper and other physical media (e.g., disk drives and removable computer media), a system of accountability (e.g., a registry) for activity top secret information and conducts inventories of Top-Secret information.

2.6.5. Publish a unit specific operating instruction that outlines security procedures for the following:

2.6.5.1. Procedures for conducting end-of-day security checks at the close of each duty or business day.

2.6.5.2. Transportation and transmission of classified information

2.6.5.3. Classified meetings, briefings, and trainings.

2.6.5.4. Processes to ensure personnel with knowledge of combinations to security containers, secure rooms and vaults are maintained and combinations are changed.

2.6.5.5. Identifying, marking, and utilizing equipment used for reproducing classified information and ensuring the systems are accredited properly. The approval must facilitate oversight and control of the reproduction of classified information and the use of the equipment for such reproduction.

2.6.5.6. Protection, removal, or destruction of classified material during emergency situations (e.g., fire, natural disaster, civil disturbance, etc.).

2.6.5.7. Guidance on the use of government or personal portable electronic devices (PEDs) (e.g., cellphones, fitness trackers, MP3 players, smart watches, wireless two-way devices, etc.); medical devices (i.e., hearing aids, breast pumps, etc.); and devices that have photographic or audio recording capabilities in areas where classified information is discussed or processed.

2.6.6. Evaluate security incidents and work with the wing IP office to determine appropriate mitigation measures are taken, to prevent further occurrences. Appoints an Inquiry Official for security incidents originating within the unit.

2.6.7. Designate, in writing, equipment used to reproduce classified material such as copiers, printers, fax machines etc. as well as equipment used to destroy classified material such as shredders, degaussers, etc.

2.6.8. Appoint a Security Container/Secure Room/Vault Custodian for each respective container/secure room/vault in their unit.

2.6.9. Conduct a risk assessment for each GSA-approved security container storing classified information located outside of an open storage area and all open storage areas approved to store top secret information.

2.6.10. Establish a NATO Control Point and appoint a NATO Control Point Officer if the unit creates, stores, or processes NATO information.

2.7. Security Assistant (SA).

2.7.1. Implements and monitors the Information, Personnel, and Industrial Security Programs, at their respective unit level on behalf of the Activity Security Manager (52 FW/IP).

2.7.2. Provides assistance to the commander and advises unit personnel on security matters and recommends improvement measures. The SA is the primary point of contact for 52 FW/IP and all security related questions should be through the SA. This ensures the SA is abreast of any issues pertaining to their respective unit.

2.7.3. Complete initial SA training within 90 days of appointment. SA initial training will include the completion of the Defense Counterintelligence and Security Agency (DCSA) Center for Development of Security Excellence (CDSE) **Air Force Security Manager Program** (GS100.CU) and local 52 FW/IP initial SA training.

2.7.4. Accomplish the following in-processing actions with all newly assigned military, civilian and contractor personnel:

2.7.4.1. Provide or direct assigned personnel to accomplish initial and annual refresher Information Security training, Controlled Unclassified Information training, Derivative Classification training and Personnel Security briefings as appropriate for the persons assigned duties. Establish methods to document and track completion of this training.

2.7.4.2. Establish ownership in the Defense Information System for Security (DISS) or its successor system.

2.7.4.3. Ensure each cleared person in their unit has signed an SF 312, *Non-Disclosure Agreement* and that it is documented in DISS or successor system.

2.7.4.4. Once training is complete, document classified access in DISS or successor system at the level required for the position they occupy on the unit manning documents, or, for contractors, the level specified by the DD Form 254, *Department of Defense Contract Security Classification Specification*. Classified access will match the access required to perform official duties and not necessarily the eligibility level listed in DISS.

2.7.4.5. Ensure all assigned personnel are briefed on their responsibilities for maintaining their security clearance eligibility under the CE program and the reporting criteria outlined in Security Executive Agent Directive (SEAD) 4: National Security Adjudicative Guidelines.

2.7.5. Processes all Supplemental Information Requests (SIR), Requests for Action (RFA), Statement of Reasons (SOR) and any other requests from official investigative agencies.

2.7.6. Maintain a list of all classified processing areas, and security containers used for storing classified, classified discussion/meeting/briefing areas, classified reproduction equipment, and classified destruction equipment used and/or assigned in their unit.

2.7.7. Ensure the Emissions Security (EMSEC)/TEMPEST certification and countermeasures are posted within each designated CPA that contain classified computer equipment.

2.7.8. Ensure high security cross-cut shredders, optical destroyers and degaussers authorized for disposal of classified information are on the respective National Security Agency (NSA) Evaluated Products Listing and have the appropriate visual aids posted.

2.8. Security Container, Secure Room, and Vault Custodian.

2.8.1. Conducts visual inspections of containers, vaults, and locks on secure rooms upon initial purchase of a container or initial establishment and at least every 5 years thereafter. Visual inspections will be accomplished using the checklist at Appendix 2 to Enclosure 3, of DoDM5200.01V3_DAFMAN16-1404V3 and documented on the Optional Form (OF) 89, *Maintenance Record for Security Containers/Vault Doors*.

2.8.2. Be appointed in writing by the unit Commander.

2.8.3. Maintains all the required documentation such as SF 700, 701, 702, OF 89, record of combination etc. for their respective security container, vault, or secure room.

2.8.4. Responsible to properly maintain, mark, store and safeguard all documentation and Automated Data Processing (ADP) media under their control, to include courtesy stored material, IAW DoDM 5200.1 and AFI 16-1404.

Chapter 3

INFORMATION SECURITY

3.1. Classified Handling and Safeguarding. Classified information is required to be either under the personal control and observation of an authorized person, stored in a GSA approved security container with a combination lock that meets FF-L-2740, or in a certified vault/secure room. Personal observation and control is defined as having sufficient surveillance and physical control over classified information to detect and prevent access by unauthorized persons. While eyes on observation and physical possession are the ideals, common sense risk management options may be utilized to meet the intent of protecting classified information while accomplishing the mission. For example, a classified workspace with only one entrance, depending on the physical environment, could potentially be protected if a cleared person was in close enough proximity to maintain observation and control over the only entrance. Such risk management decisions should be made by unit commanders or designees for the area and the options used shall be appropriate to the environment in which access occurs and considerate of the nature, volume, and availability of the information.

3.2. Risk Assessment and Security-in-Depth. Risk assessments have been accomplished that measure both the current threat and vulnerabilities for Spangdahlem AB. The information from these assessments and the existence of multiple layers of defense, including perimeter fencing, 24/7 installation entry control and roving Security Forces patrols with the ability to respond to any facility on base within 5-10 minutes, have resulted in the determination that security-in-depth exists for all facilities on Spangdahlem AB and U.S. owned facilities at GSUs.

3.2.1. **Emergency Plans.** All units will develop emergency plans for the protection, removal, or destruction of classified material in case of fire, natural disaster, civil disturbance, terrorist activities, or enemy action. Plans will be posted in all spaces that process or store classified information/material. Plans will be developed utilizing the example plan in **Attachment 2**. One plan can cover the entire units classified holdings if they are not complex. Units that have unique situations such as multiple classified processing areas, open storage areas, and safes are recommended to create plans specific to the rooms/areas. Plans must be exercised annually.

3.3. Visitors and visits that require access to classified information or facilities. Visitors or visits to any 52d FW unit that require access to classified information or facilities will abide by the following procedures:

3.3.1. Visit requests shall be processed and security clearance and access level verified via DISS or successor system for DoD civilian, military, and contractor personnel whose access level and affiliation are reflected in DISS. For US government agencies that do not use DISS, a memorandum from the agency security manager verifying the appropriate clearance eligibility and access will be provided to the hosting unit Security Assistant.

3.4. Storage of Classified for Unexpected or In-transit Personnel.

3.4.1. The 52 FW Command Post will provide temporary classified storage for material up to Secret and NATO Secret for personnel in-transit or arriving unexpectedly. Personnel who require temporary classified storage should request it in advance of arrival if possible.

3.4.2. For temporary classified bulk storage, 726 AMS will provide temporary classified storage for material up to Secret and NATO Secret for personnel in-transit or arriving unexpectedly.

3.5. Portable Electronic Devices (PED). The use of government or personal PED (e.g., cellphones, fitness trackers, MP3 players, smart watches, wireless two-way devices, etc.) and devices that have photographic or audio recording capabilities are prohibited in areas where classified information is discussed or processed. All cleared personnel are responsible for being alerted to detect these items and immediately report violations. Exceptions to this policy will be evaluated on a case-by-case basis by 52 FW/IP.

3.5.1. **Medical Devices.** The use of medical devices (e.g., hearing aids, breast pumps, etc.) in areas where classified information is discussed or processed is subject to the medical device approval process. The National Security Agency (NSA) publishes a list of approved medical devices. Requests for the approval of medical devices in secure areas will be cross-referenced with the NSA Medical Devices List and forwarded to 52 FW/IP for final approval.

3.6. End-of-Day Security Checks.

3.6.1. End-of-day security checks will be completed at the end of every duty or business day in all areas that store, or process classified information (e.g., SIPR rooms, vaults, secure rooms, security containers etc.). These checks will ensure that any area where classified information is used or stored is secured. SF 701, *"Activity Security Checklist"* shall be used to record such checks. An integral part of the security check system shall be the securing of all vaults, secure rooms, and containers used for storing classified material. SF 702, *"Security Container Check Sheet,"* shall be used to record such actions. The SF 701 and 702 shall be retained for a period of three months.

3.6.2. Work centers operating on a 24/7 or continuous operational basis are still required to annotate the SF 701 on the last shift when checklist items are secured and/or continuous operations are suspended.

3.6.3. Units will develop unit specific procedures that outline the procedures for these checks and who is responsible in their respective unit security instructions.

3.7. Classified Reproduction Procedures.

3.7.1. The reproduction of classified information should be kept to a minimum, consistent with mission requirements. Commanders will designate and approve classified reproduction equipment in writing. SAs shall coordinate with the Wing Cybersecurity Office (WCO) prior to seeking approval of a printer or copier authorized to reproduce classified information. Classified reproduction will not be approved/authorized for copiers connected to the unclassified network. Classified reproduction will not be approved/authorized for copiers with an internal hard drive unless they are located within an approved open storage area.

3.7.2. Personnel authorized to reproduce classified material shall:

3.7.2.1. Be knowledgeable of the procedures for classified reproduction and aware of the risks involved with the specific reproduction equipment being used and the appropriate countermeasures they are required to take.

3.7.2.2. Observe all reproduction limitations placed by originators on documents and special controls applicable to special categories of information.

3.7.2.3. Ensure reproduced material is placed under the same accountability and control requirements as applied to the original material.

3.7.2.4. Ensure reproduced material is conspicuously identified as classified at the applicable level and copies of classified material are reviewed after the reproduction process to ensure that the required markings exist.

3.7.2.5. Destroy and protect waste products generated during reproduction.

3.7.2.6. Utilize only approved and accredited systems to reproduce classified material.

3.7.2.7. Ensure foreign government information (FGI) is reproduced and controlled pursuant to guidance and authority granted by the originating government.

3.8. Classified Storage.

3.8.1. All classified material, when not under direct surveillance of an authorized person, will be stored in either a GSA-approved security container, Vault that meets FED-STD 832, or approved Open Storage Area/Secure Room to prevent unauthorized access or compromise.

3.8.2. Whenever handling classified information outside of an approved storage container, vault, or open storage area, it must always be under continuous observation and control. Use the appropriate cover sheet for classified documents when removed from storage.

3.8.3. Classified material will not be removed from officially designated offices or work areas, such as taking it to an individual's quarters for personal convenience unless specifically approved in accordance with the procedures in **para. 3.8.3.1**. Do not release classified to any agency that does not have adequate storage capability.

3.8.3.1. All requests for removing Secret and Confidential material from designated work areas for work or storage at home will be submitted through 52 FW/IP for final approval by HQ-USAFE-AFAF/IP. Any approved request must be maintained by the SA and procedures addressing safekeeping, storage, and arrangements to pick up the classified in case of emergency must be added to unit procedures. Due to the possible unique circumstances in each case of residential storage, tailored location-specific security procedures for each separate instance of residential storage will be developed and the end-user will acknowledge them with their signature.

3.8.4. Each security container, open storage area, and vault will be tracked by the SA. At a minimum, the following information will be tracked: Security Container Serial Number, Location, Primary Custodian, Last Inspection and Location of the SF-700, Part 2 (Combo).

3.8.5. Knowledge of combinations to security containers, vault doors, and secure room doors that contain classified information will be restricted to cleared personnel who are authorized access to the classified material stored therein.

3.8.5.1. Record and seal combinations to security containers on part 2 of SF 700 and store in a separate safe. Mark SF 700, Part 2, with the highest classification level of contents maintained in the container. Mark at top, bottom, front and back. Ensure **Part 2** has the following classification block annotated on the back: Classified by: Name of person filling form, Derived From: 32 CFR 2001.80(d)(3), Declass Date: Upon Change of combination date.

3.8.5.2. Combinations to security containers, vaults doors, and secure room doors will be changed:

3.8.5.2.1. When the container, vault, or secure room door is placed in service.

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

3.8.5.2.3. When compromise of the combination is suspected.

3.8.5.2.4. When the container, vault, or secure room door is taken out of service or is no longer used to store classified information, at which time built-in combination locks shall be reset to the standard combination 50-25-50, and combination padlocks shall be reset to the standard combination 10-20-30.

3.9. Secure Room and Vault Procedures.

3.9.1. All secure rooms/open storage areas and vaults that openly store classified information are required to be certified and approved by the 52 FW/CIP. Units that require secure rooms or vaults will notify 52 FW/IP, in writing of all open storage or vault requirements. This request will be signed by the unit commander and include the justification, building number and room number, and a layout of the facility. Secure rooms and vaults will not be approved for convenience. There must be an operational need where storing classified material in GSA approved security containers is not practical or possible.

3.9.1.1. 52 FW/IP, with assistance from 52 CES, and 52 SFS will assess all proposed and modified secure rooms and vaults to ensure security requirements and construction standards are met per the appropriate regulations. Results of the assessment will be documented in writing and the 52 FW/CIP will give final approval on letter.

3.9.1.2. 52 FW/IP will be notified of any structural modifications to secure rooms or vaults and determine whether recertification is necessary.

3.9.2. All 52 FW secure rooms and vaults will implement the following measures:

3.9.2.1. Access to each room or vault will be facilitated via an Entry Authorization List (EAL) signed by the unit commander and endorsed by the SA for validation of clearances. The EAL shall be updated quarterly or as changes occur. The EAL should be readily available on or near the applicable secure room or vault door. Personnel not on the EAL shall be escorted by authorized personnel and logged via AF IMT 1109.

3.9.2.2. Areas that have dropped/false ceilings or raised floors, will have those spaces inspected and recorded monthly by the space custodian unless those areas are alarmed.

3.9.2.3. Emergency plans detailing the items listed in **Chapter 3., Para 3** limit access.

3.10. Classified Processing Areas (CPA).

3.10.1. A Classified Processing Area (CPA) is any area that is not certified as an Open Storage Area/Secure Room but is used for storing or processing classified information. Examples include SIPRNet rooms/cafes, rooms that house GSA-approved security containers storing classified information, classified briefing rooms, etc.

3.10.2. All CPAs are required to be evaluated by 52 FW/IP to ensure adequate physical security prior to being used. If the space will house an Automated Information System (AIS), communications systems, or cryptographic equipment, the space will require an EMSEC assessment and TEMPEST certification from the WCO.

3.10.2.1. Once WCO approves a CPA, all equipment must stay in the original location as reported in the TEMPEST Certification/EMSEC assessment. A new survey will need to be conducted and approved before any equipment can be moved.

3.10.2.2. The unit commander will approve and designate any unit CPAs after evaluation from 52 FW/IP and WCO (if warranted).

3.10.3. Personnel operating within active CPAs are required to ensure the PED poster (available on the 52 FW/IP SharePoint) is visibly posted on the exterior of entrances to CPAs while classified processing/discussion is in progress.

3.10.4. Personnel controlling entry to active CPAs will ensure unauthorized PEDs are not introduced into the CPA by reminding personnel the devices are prohibited and provide the opportunity to remove devices from the area before discussing and/or processing classified.

3.11. Classified Meeting Procedures.

3.11.1. All classified meetings and conferences, to include seminars, exhibits, symposia, conventions, training classes, workshops, or other gatherings in which classified information is disclosed, will be conducted utilizing the Classified Meeting Checklist found in Appendix 1 to Enclosure 2 of DoDM5200.01V3_DAFMAN16-1404V3 as well as the procedures outlined in Enclosure 2. 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 for implied approval.

3.11.2. A classified meeting shall be formally approved by the appropriate commander, director, or agency chief if it can be deemed unique, complex and/or is a ‘hosted’ type event or meeting, especially when involving multiple organizations with non-unit attendees/visitors.

3.11.3. All classified meetings must occur within the confines of Spangdahlem AB or host-GSU installation, provided the room is under sole control of the U.S. component, in an area/room with sufficient controls to provide protection from unauthorized disclosure i.e. sound attenuation, window covering, etc. Classified meetings that occur at an uncleared, off-installation locations require a comprehensive security plan and an exception to policy request submitted to HQ USAFE-AFAF IP.

3.12. Security Education and Training Awareness.

3.12.1. The SA will be listed on the unit’s in-processing checklist and each assigned individual (military, civilian, and contractor) will immediately process through the SA. The SA shall ensure all personnel receive the following training:

3.12.1.1. DoD Initial Orientation and Awareness Training (myLearning). To be completed upon in-processing into the unit.

3.12.1.2. Security Annual Refresher Awareness Training (myLearning). To be completed annually thereafter the completion date of initial training.

3.12.1.3. Unauthorized Disclosure of Classified Information and Controlled Unclassified Information Training (myLearning). To be completed annually

3.12.1.4. Controlled Unclassified Information (CUI) Training (myLearning). To be completed annually.

3.12.1.5. Insider Threat Awareness Training (myLearning). To be completed annually.

3.12.2. The SA shall ensure the personnel who access classified systems and/or are derivative classifiers complete the following training:

3.12.2.1. Derivative Classification Training (myLearning). To be completed annually.

3.12.2.2. Marking Special Categories of Classified Information (STEPP). To be completed once.

3.12.2.3. North Atlantic Treaty Organization (NATO) Training. To be completed once prior to granting access to NATO information. SA will ensure individuals are granted NATO SECRET access in DISS or successor system prior to granting access to SIPR.

3.12.3. Personnel who escort, hand-carry or serve as a courier for classified material shall receive a courier brief from the SA when transporting classified material beyond the confines of the installation.

3.12.4. The SA will maintain record of and track all the above training for personnel in their unit and are required to maintain a copy of the training certificate.

3.13. Transmission and Transportation of Classified Information.

3.13.1. Persons transmitting or transporting classified information are responsible for ensuring the intended recipients have authorized access, have a need to know, and have the capability to store classified information. Information may only be transmitted in accordance with DoDM5200.01V3_AFMAN16-1404V3.

3.13.2. Protect all US Registered, Certified, and First Class marked “Return Service Requested” mail addressed to DoD organizations and approved cleared contractor facilities on base as classified until determined unclassified. NOTE: Only individuals with US security clearances are authorized to receipt for US Registered Mail.

3.13.2.1. Mailing out-going classified packages.

3.13.2.1.1. Each person mailing (via US postal channels) classified material is responsible for ensuring the material is marked, wrapped, addressed, mailed correctly, proper receipts attached, protected, and secured until its final disposition IAW Enclosure 4 of DoDM5200.01V3_AFMAN16-1404V3.

3.13.2.1.2. Top Secret will NEVER be mailed through any postal channel. Units MUST use an authorized courier service for transportation or an approved secure communications systems approved by the NSA for transmitting messages.

3.13.2.1.3. Secret and Confidential Information. U.S. Postal Service (USPS) registered mail service can be used to send SECRET information. However, before sending USPS registered mail, the MPS must ensure it always remains in U.S. postal channels.

3.13.2.1.4. If the USPS cannot ensure the mail always remains in U.S. postal channels, the Defense Courier Service (DCS) may be used.

3.13.3. Classified Transmission via Phone.

3.13.3.1. All phone transmissions of classified information shall only be via the use of a Secure Terminal Equipment (STE), Secure Voice Over Internet Protocol (SVOIP) or authorized secure communication equipment. Consult with the WCO to verify which systems are appropriate for what classifications.

3.13.4. Transportation of Classified Information.

3.13.4.1. When classified material is to be 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 briefcase or zippered pouch made of canvas or other heavy–duty material and having an integral key-operated lock or combo lock may serve as the outer wrapper when hand-carrying. The outer wrapper will be marked with the unit/office address and phone number. Use serial numbers if units have more than one briefcase or pouch used for transporting classified; DO NOT mark with level of classification on the outer wrapper. Use envelopes or folders marked with the level of classification for the inner wrapper.

3.13.4.2. The transportation, to include hand-carrying, of classified material within the confines of the installation requires the supervisors verbal authorization, at minimum. Courier authorization designation letters are not required unless the courier will be entering and entry control point on the installation and the materials are subject to search.

3.13.4.3. The transportation, to include hand-carrying, of classified material off-installation requires the approval of the respective unit commander. All personnel transporting classified material off the installation must have a completed courier authorization letter signed by the unit commander or DD Form 2501, Courier Authorization, with them when transporting.

3.13.4.3.1. The SA will brief the responsibilities to each person hand-carrying classified material. The briefing must include emergency procedures and security practices while in possession of the classified material. When transporting classified information over international borders, the courier must have identification and an authorization letter meeting the requirements of DoDM5200.01V3_AFMAN16-1404V3. The authorization letter will be written in English and if possible, in the language of the countries through which the courier is traveling.

3.14. Annual Clean-Out of Classified Information.

3.14.1. The second week of October is designated as the 52 FW classified clean-out period. In addition to focusing on disposing of unneeded classified material, commanders, directors, and staff agency chiefs will ensure all classified holdings are reviewed for required markings, possible downgrading, and declassification. Units will document this action in writing.

3.15. Unit Program Administration.

3.15.1. Program Reviews. The 52d FW IP office is authorized to conduct an annual Information Protection Program Review of all 52 FW units, tenant units and organizations with a Host Tenant support agreement aligning under the 52 FW. The DIP may elect to use a staff

assistance visit (SAV) or Wing Inspection Team (WIT) event in lieu thereof. The CIP may also extend the annual requirement due to operational, scheduling, or other factors as deemed warranted.

3.15.1.1. The 52 FW/IP will provide a report to the commander or director and SA of the unit after each review. The report will indicate whether discrepancies found are of a nature that warrants a follow up review to ensure corrective actions/measures are taken. The decision to conduct a follow-up review rests solely with the Information Protection office. If a follow-up is warranted, it will be conducted approximately 60 days after the report or earlier at the unit's request.

3.15.1.2. Units will ensure that non-compliant items found during a program review from applicable Management Internal Control Toolset (MICT) checklists are entered and tracked as observations per AFI 90-201, *The Air Force Inspection System*.

3.15.2. Program Binders. SAs will maintain an Information Protection program binder. Use of the unit "e-binders" on the 52 FW/IP SharePoint site is encouraged but not mandatory. These binders serve as an environmentally friendly option that allows documentation to be secured through permissions, while remaining available to both the unit program managers as well as the IP staff. Regardless of the type of binder used, the following items should be maintained and/or made available upon request.

3.15.2.1. Appointment letters and training documentation for SAs as required.

3.15.2.2. Unit internal operating instructions and/or written plans, as applicable.

3.15.2.3. List of security containers within the organization, showing manufacturer, class, number of drawers, unique container ID#, lock type and location. The list must also contain all vaults and secure rooms approved by the CIP. Memos listing custodians and names of persons having knowledge of the combinations. Documentation of training covering classified safe operations for all personnel with access to the container.

3.15.2.4. Copies of the unit's IP program reviews, inspection, or review reports. Maintain last two years, to include documentation of corrective actions if not recorded elsewhere.

3.15.2.5. Copies of signed AF Forms 2587, Security Termination Statement. Maintain for 2 years in accordance with the AFRIMS RDS.

3.15.2.6. Copies of AF Forms 2583, Request for Personnel Security Action, for submitted security clearance investigations and interim or final access to special accesses such as Restricted Data (RD), Critical Nuclear Weapon Design Information (CNWDI), or North Atlantic Treaty Organization (NATO). Maintain until access is no longer required.

3.15.2.7. Training documentation, to include initial and refresher training. Maintain records for two years.

3.15.2.8. Copies of any letters approving classified reproduction equipment that are posted with the device.

3.15.2.9. Miscellaneous other documentation to include annual position code review memos, cleanout day memos, secure room certification paperwork, etc.

3.15.2.10. Industrial Security program documentation such as the DD Form 254, Department of Defense Contract Security Classification Specification, Performance of Work Statements and contractor Visit Requests.

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

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

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

3.16.3. 52 FW/IP will advise the Commander on inquiry/investigative requirements. The SA or Commander is responsible for reporting the incident to the 52 FW/IP Office no later than the first duty day following the reporting of the incident. In incidents where classified material is lost or out of proper controls, all notifications will be made in person or over secure communications.

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

3.16.5. The inquiry official appointment letter will be accomplished and signed by the appointing authority. Upon notification of appointment, the inquiry official will make an appointment with the 52 FW/IP office for a briefing on the incident and their responsibilities. The inquiry official will provide a copy of their appointment letter to the 52 FW/IP. The inquiry official will also contact the 52 FW/Staff Judge Advocate (SJA) to receive a briefing (if necessary).

3.16.6. The inquiry official will prepare a written report. The report will at a minimum be marked “Controlled Unclassified Information” and be completed within 30 days of appointment. The report will be routed through the 52 FW/IP to the appointing official. The Chief, Information Protection will provide technical reviews of the report and concur/non-concur on the findings and forward it to the appointing official.

3.16.7. The appointing official reviews the report, concurs or non-concurs with findings, make closing remarks, and identify any corrective actions required. The closed report will be forwarded to the 52 FW/IP.

3.16.8. The appointing official directs a formal investigation when the initial inquiry is insufficient, and it is believed that more information can be obtained through a formal investigation. Refer to 52 FW/IP and 52 FW/SJA for assistance.

Chapter 4

INDUSTRIAL SECURITY

4.1. Overview. Industrial Security is a multi-disciplinary security program focused on the protection of classified information developed by or entrusted to U.S. industry aka "contractors" operating under the National Industrial Security Program (NISP). SAs will notify 52 FW/IP of any contractors that require access to classified information in their unit.

4.2. Contracts that Require Access to Classified Information. All incoming contractors requiring access to classified information will in-process with their respective unit SA for clearance verification/validation and records review prior to performing the terms of contract.

4.2.1. In processing Requirements. SA will verify contractors have a need-to-know for classified information by obtaining the respective contract DD Form 254. The DD 254 must be signed by the proper authority and list the unit location as a performance location and that access to classified information overseas is authorized.

4.2.1.1. The SA will ensure all assigned contractors complete the training outlined in **Chapter 3.**, **Para 11** of this instruction.

4.2.1.2. Verify the contractor has submitted a Visit Request in DISS to the unit SMO listing all personnel working on the contract at the location.

4.2.1.3. Verify the contractor's security clearance eligibility, access level, and NDA via DISS or successor system. If there are any discrepancies, notify 52 FW/IP and withhold access to classified information until resolved.

4.2.1.4. Establish an owning relationship in DISS or successor system with the contractor personnel for the duration of their time in the unit.

4.2.1.5. Notify 52 FW/IP that a Contractor Designation needs to be completed and copy of local Contractor Visitor Group Security Policy provided.

4.2.2. The CIP will designate, in writing, all contractor operations on the installation as either an Intermittent Visitor Group, Integrated Visitor Group, or Independent Visitor Group. A copy of local Contractor Visitor Group Security Policy will be provided to the company Facility Security Officer (FSO).

4.2.2.1. Intermittent Visitors. Contractor operations performing less than 90 days qualify as intermittent visitors. Intermittent visitors will operate under the security requirements of DoD 5220.22-M and the 52 FW and unit information security program.

4.2.2.2. Integrated Visitor Groups. Contractors that are here for longer than 90 calendar days and work embedded in a unit will be characterized as Integrated Visitor Groups. Integrated Visitor Groups will be integrated into the unit Information Security Program and operate under the day-to-day oversight of the unit.

4.2.2.3. Independent Visitor Groups. Contractors that operate independently from day-to-day oversight by Air Force employees and have their own separate assigned spaces will be characterized as Independent Visitor Groups.

4.2.3. The SA must include the contractors in the unit's self-inspection to ensure classified operations are complied with and they are abiding by contract security requirements.

4.2.4. Direct access to unit classified and unclassified information is limited to "need-to-know" contract specific performance requirements, as identified in the DD Form 254.

4.2.5. Integrated visitor groups must report all security incidents including the loss, compromise or suspected compromise of classified information to 52 FW/IP via the SA.

4.2.6. Integrated visitor groups will use 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 National Industrial Security Program Operating Manual (NISPOM) requirements.

4.2.7. The commander will report any adverse issues, within the 13 Adjudicative Guidelines, to 52 FW/IP.

4.2.8. Program Administration. Unit SAs will maintain the following information on each classified contract within their unit:

4.2.8.1. Current signed copy of the DD Form 254, *DoD Contract Security Classification Specification,* and any revisions, to include attachments.

4.2.8.2. Signed copy of the Contractor Visitor Group Designation.

4.2.8.3. SMO Visit in DISS or successor listing all personnel working on the contract.

4.2.8.4. Name of the contract on-site lead and Contracting Officers Representative (COR).

4.2.8.5. Training records for initial and refresher training and training outlined in **Chapter 3**.11.

Chapter 5

PERSONNEL SECURITY

5.1. In-Processing. All military and DoD civilians assigned to a unit must be in-processed in DISS or successor system for complete accountability. This is necessary in acquiring individual ownership and proper security clearance access when a new employee arrives on station. SAs must in-process all unit members with a proper owning or servicing relationship in DISS within 15 days of arrival. Contractors requiring access to classified will be serviced in DISS to monitor clearances.

5.1.1. Commanders validate and grant access for all personnel assigned to positions that require access to classified information. The level of access is determined by the SAR code on the Unit Manning Document (UMD). The SA is authorized to grant access in DISS after verifying the SAR code for the position the member is assigned in the UMD. The SA must also ensure the following criteria is met before access is granted:

5.1.1.1. The individual possesses a completed investigation and eligibility at or above the SAR code requirement. Verify eligibility in DISS or successor system. NOTE: If the member requires a higher-level clearance currently not eligible for, please follow initiation guidance in **paragraph 5.4**.

5.1.1.1.1. If DISS or successor system shows an invalid close date and does not show another investigation processing, the SA will need to verify if member has been enrolled into CE via DISS or successor system. Only CE enrollment dates of 1 October 2018 to present are valid enrollment dates. If there is an invalid date, contact 52 FW/IP for further instructions.

5.1.1.1.2. If DISS or successor system shows any erroneous eligibilities (i.e., No Determination Made, Loss of Jurisdiction, Admin Withdrawal) or the member's profile is highlighted in red (Possible CE processing), coordinate actions with 52 FW/IP.

5.1.1.2. The individual has a need-to-know.

5.1.1.3. The individual signed an SF 312, Classified Information Nondisclosure Agreement (NdA). This can be verified in DISS. If member does not have, complete, and add to DISS. Document the SF 312 NDA and upload a copy into DISS or successor system.

5.1.1.3.1. For military personnel, mail the original SF 312 to the following address: AFPC/DPSIR 550 C Street West JBSA-Randolph TX 78150.

5.1.1.3.2. For federal civilian personnel, send original SF 312 to the Civilian Personnel Office (CPO). For contractors, send original SF 312 to the member's Facility Security Officer (FSO).

5.1.1.4. The individual has completed initial training outlined in **Chapter 3**.11.

5.1.2. Access to any other program falls under the authority of the specific program manager (SAP, SCI, NATO, CNWDI, etc.). If member is erroneously accessed with these types of levels due to a requirement needed at a previous location, go into DISS and remove access.

5.1.3. Specific derogatory issues of unit members that may affect their ability to protect classified information must be addressed on a case-by-case basis under the CE program. Follow guidance in **paragraph 5.6.3.2**.

5.2. Out-Processing Members.

5.2.1. SAs will out-process all members in DISS or successor system. The SA must evaluate assignment documentation to ensure personnel meet the required investigation needed for the new assignment. If personnel must have a new investigation, follow procedures in **paragraph 5.4**. Failure to accomplish security requirements could result in delay of receiving orders and/or cancellation of the assignment.

5.2.1.1. For members separating/retiring from the Air Force, the commander will terminate the member's access by signing the AF Form 2587. This form must be retained for 2 years.

5.2.2. Personnel with SCI must first out process with SSO prior to collateral access debrief. If SSO allows member to transition in status, do not debrief the member, only out process.

5.3. SAR Code Requirements.

5.3.1. Commanders, with the SA, conduct a SAR Code review of their UMD every May to adjust for accuracy of position coding and to eliminate unnecessary access requirements. Reviews will be documented in writing (email or memorandum) and sent to 52 FW/IP.

5.3.1.1. When changes are necessary, SA will complete Authorization Change Request (ACR) form and provide to 52 FW/IP for coordination. Send final form to 52 FSS Manpower Office.

5.3.2. AFMAN 16-1405 allows for the wing commander to approve upgrades based on specific criteria. If the positions needing upgrade REQUIRE access to Joint Worldwide Intelligence Communications System (JWICS) and/or TS Operational Plans (OPLANS), the justification must be indicated in the ACR. Major Command (MAJCOM) approval is not required.

5.3.2.1. For positions that do not fall under the criteria, a 2–3-star MAJCOM general officer or civilian equivalent authority must approve the request.

5.3.3. Every December and June, the manpower office will provide 52 FW/IP a report of all SAR Code changes. This report will include the number of new and upgraded positions, job titles or position numbers, justification; and number of downgrades using one-for-one exchange.

5.4. Personnel Security Investigation (PSI) Types.

5.4.1. TIER 1 (Previously National Agency Check and Inquiries [NACI]). TIER 1's is conducted by the Defense Counterintelligence Security Agency (DCSA) and are required on all contractor and civilian employees assigned to non-sensitive positions. There are no Recertification requirements unless the member has had a 2-year break of federal service.

5.4.1.1. All TIER 1, childcare checks, and any other supporting requirements for this level of investigation (i.e., fingerprinting) are conducted by the CPO.

5.4.2. TIER 3 (Previously Access National Agency Check and Inquiries [ANACI] and National Agency Check, Local Agency Check with Law, and Credit [NACLC]). TIER 3's is conducted by DCSA and are required for military and civilian employees' initial Secret security clearance or assignment to noncritical sensitive positions. Current recertification

requirements are every 5 years. If member is enrolled in the CE Program, there is no PR requirement unless the member has had a loss of DoD affiliation.

5.4.3. TIER 5 (Previously Single Scope Background Investigation [SSBI]). TIER 5's is required for access to Top Secret and assignment to special positions requiring access to critical sensitive or SCI positions. Current PR requirements are every 5 years. If member is enrolled in the CE Program, there is no PR requirement unless the member has had a loss of DoD affiliation.

5.4.3.1. A special agreement check (SAC) is required on the following categories of individuals associated with the subject of a TIER 5 (a) spouse or cohabitant, (b) immediate family members, 18 years old or older, who were born outside the United States. If events occur after completion of the TIER 5, submit a SAC using INV Form 86 to 52 FW/IP for submission to DCSA.

5.4.4. Any member separating or retiring within 12 months of the PR, does not need to accomplish a recertification. The SA will make sure the member has proper documents for discharge or separation.

5.5. PSI Initiations.

5.5.1. When a member requires an initial TIER 3 or 5 investigation, the SA will complete an AF Form 2583, Request for Personnel Security Action, showing the proper investigation type (identified in **paragraph 5.3**.) The SA will sign/date the form and send the form to 52 FW/IP.

5.5.1.1. Any upgrades to a Top Secret will need to have supporting documentation (e.g., assignment orders or UMD Position Number).

5.5.1.2. Members applying for a school or assignment requiring a Top-Secret investigation may only request an actual PSI when instructions specifically state the need.

5.5.1.2.1. When instructions do not require an actual submittal, have member provide a hard copy SF86 with signature/date for the application package. If member is selected for the school or assignment, the SA may proceed to have member complete the actual PSI.

5.5.2. 52 FW/IP will initiate the member's investigation in E-APP after receiving the signed documents. An email will be sent to the member and the SA will provide detailed instructions for completion of the Standard Form 85, Questionnaire for Non-Sensitive Positions, or Standard Form 86, Questionnaire for National Security Positions using the appropriate checklist. Members must access and complete their E-APP within 15 days of the email.

5.5.2.1. The CPO is responsible for all new civilian hires. CPO will initiate the AF Form 2583, E-APP and fingerprints along with required supporting documentation (i.e., OF-306, Declaration for Federal Employment, applicant's resume, childcare paperwork, etc.) as required. 52 FW/IP will conduct the final reviews of TIER 3/5s and submit to DCSA.

5.5.3. Once the member submits their E-APP for review, 52 FW/IP will send any corrections back to the member to complete. Corrections must be completed within 5 business days.

5.5.4. When complete, the investigation will be forwarded to DCSA. All investigations and interviews are conducted by DCSA, and the DoD CAS is the designated authority to grant, suspend, deny, or revoke personnel security eligibility.

5.5.4.1. Electronic fingerprints will be completed on all initial and incomplete previous investigations. NOTE: 52 FW/IP only processes fingerprints for assigned USAF military, civilians and contractors unless covered by a support agreement.

5.5.4.2. Individuals completing an E-APP questionnaire must specify any circumstances that would make them unavailable for a subject interview within 60 calendar days of the date the questionnaire is submitted to DCSA. Detailed information regarding the period in which the individual will be unavailable such as date, location, and duration should be provided to the 52 FW/IP Office prior to submittal of a TIER 3/5.

5.5.4.3. In order for the DoD CAS to make an eligibility determination for an investigation, sometimes additional information is sent to the member as a SIR or a RFA to resolve certain issues. The member usually has 30 days to provide a response to these requests.

5.5.4.3.1. If member cannot provide a response by requested timeframe, they can request an extension through the unit commander. All extension request approvals must be sent to the 52 FW/IP Office for processing and can be in a memorandum or email format.

5.5.5. When DoD CAS does not accept a response to a SIR or RFA, a more stringent unfavorable personnel action can result with a SOR.

5.5.5.1. When the DoD CAS provides a SOR stating intent to deny or revoke a clearance, the member must respond to DoD CAS, through the SA and 52 FW/IP, IAW instructions provided.

5.5.5.1.1. If member cannot provide a response by requested timeframe, they can request a 30-day extension through the unit commander. All extension request approvals must be sent to the 52 FW/IP Office for processing and can be in a memorandum or email format.

5.5.5.2. If a member receives a final determination of denied or revoked, through a Letter of Denial/Revocation, the member will have an opportunity to appeal. This appeal process is between the member and the Personnel Security Appeal Board (PSAB). The 52 FW/IP Office will not be able to process any documentation on behalf of the member.

5.5.5.2.1. If the DoD CAS maintains the revocation after appeal, the member's commander will not be able to request a new PSI until 12 months after the effective date of revocation or denial or decision of the PSAB, whichever is later. The member must be placed in a non-sensitive position until a new PSI has been adjudicated. No interim clearance access can be granted.

5.5.5.2.2. Requests should be sent to DoD CAS through the 52 FW/IP with the unit commander's recommendation for reinstatement. The commander will include an explanation on how the individual's behavior has improved and the appropriate documentation corresponding to the reason(s) for the initial denial or revocation. The documentation required depends on the reason(s) involved, such as, drug or alcohol abuse evaluations; or current financial statement(s).

5.5.6. Commanders, First Sergeants and SAs may review case details derived from an investigation; however investigative details must not be released to the subject. If the subject

would like a copy of the investigation, they will need to submit a Freedom of Information Act (FOIA) request through the appropriate agency. Contact the 52 FW/IP for further information. When a member has their security clearance suspended, denied, or revoked, 52 FW/IP will provide member information to WCO to meet requirements identified in AFMAN 17-1301 for classified and unclassified system accesses.

5.6. Continuous Evaluation Program.

5.6.1. The CE Program is part of the recertification process for TIER 3/5 investigations. This program will allow members to maintain clearance eligibility by accomplishing continuous requirements instead of completing a recertification over a set period. To get every member enrolled into the CE Program, members will need to accomplish their next recertification, at the normal required time interval.

5.6.2. The SA will run a monthly DISS personnel report. The SA will monitor recertifications coming due within 120 days of the previous close date using the Defense Intelligence Agency's (DNI) temporary recertification timeframes (5 years for Secret and Top Secret) and initiate an investigation IAW **paragraph 5.4**.

5.6.2.1. Once member completes the recertification, 52 FW/IP will use a risk-management process to analyze elements in the SF86. If no risks associated, the investigation will be deferred for CE enrollment. If risks are identified, the investigation will be submitted to DCSA.

5.6.2.1.1. Recertifications submitted to DCSA will eventually be enrolled automatically into the CE Program after investigation has been completed and submitted to DoD CAS by DCSA.

5.6.3. Members enrolled in the CE program are mandated to report any issues, identified under the 13 Adjudicative Guidelines, IAW AFMAN 16-1405 to their chain of command. Unit leadership (i.e., Commanders, First Sergeants, Supervisors) and SAs must forward any members' reports and any other issues, meeting the criteria, to 52 FW/IP. Under the CE program, there are two reporting categories. These are DoD CAS CE Incident Report (CEIR) and Local CE Report.

5.6.3.1. DoD CAS CEIR Alert. This is a downward report from DoD CAS identifying an issue that a member must respond in each timeframe.

5.6.3.1.1. 52 FW/IP will send all DoD CAS CE Reports to the appropriate SA to be processed within 30 days. Unit commanders must determine if the member should retain classified access or not while issue(s) are being reviewed for closure.

5.6.3.2. Local CE Report. This is a report from the local assigned unit to DoD CAS informing of a potential issue involving one of the 13 Adjudicative Guidelines.

5.6.3.2.1. The SA will provide 52 FW/IP any issues falling under the 13 Adjudicative Guidelines, within 72 hours of notification of the issue. Unit commanders must determine if the member should retain classified access or not while issue(s) are being reviewed for closure.

5.6.3.2.1.1. 52 FW/IP will review the daily blotter and any other available resources (i.e., Drug Demand Reduction Center, Legal, etc.) and send out CE notices to the appropriate commander, first sergeant and SA.

5.6.3.3. To properly close an issue on any reportable item, the unit must provide any of the following documentation, if it pertains to that issue for the adjudicator to evaluate.

5.6.3.3.1. Any AFOSI, Security Forces or local reports of investigations and any court proceedings.

5.6.3.3.2. Any unit actions, to include actual reports of administrative, punitive, or disciplinary (i.e., Letters of Counseling/Reprimand, Unfavorable Information Files, Article 15, etc.). Separation, confinement, or permanent change of station orders are needed for members no longer assigned.

5.6.3.3.3. Any medical or mental health summaries which indicate impairment of the individual's judgment or reliability to safeguard classified and summaries of actions by mental health providers.

5.6.3.3.4. Any successful completion of a rehabilitation program, progress in a rehabilitation program, or failure of a rehabilitative program.

5.6.3.4. DoD CAS will provide all final adjudicative decisions for each issue. If DoD CAS decides to act against a member's security clearance (i.e., revoke, deny), due process procedures outlined in DoDM 5200.02 will be followed.

5.6.3.5. If any member shows to have Sensitive Compartmented Information (SCI) access, 52 FW/IP will forward information to the local SSO to process. The SSO will forward any derogatory information they receive to 52 FW/IP as well.

5.7. Out-of-scope Investigation Procedures:

5.7.1. 52 FW/IP will send notifications to the member's SA, unit commander and member 10 days prior to the out-of-scope date if member has not completed PR requirements.

5.7.2. Access to classified information and NIPRNET/SIPRNET systems will be withdrawn for all individuals who fail to complete the required PR prior to their out-of-scope date due to negligence. Withdrawal will occur on the first duty day after the out-of-scope date.

5.7.2.1. The SA, who will notify the commander, and WCO will be notified of the withdrawal.

5.7.2.2. Members who have not complied with investigation submittal, after access and computer system withdrawal, will be recommended for a CE incident under Guideline E (Personal Conduct). All actions will be forwarded to member's unit commander to process.

5.7.2.3. Inbound personnel without a valid investigation may be granted NIPRNET access not to exceed 60 days. This allows for submission of investigation paperwork. At no time will SIPRNET access be given until an open investigation is reflected in DISS.

5.7.3. Waivers to this policy may be submitted by unit commanders to 52 FW/IP prior to withdrawal. Waiver requests must include a statement of reasonable risk and include justification (i.e., member was deployed, member has an approved retirement or separation, member was on convalescent leave). Disapproved waivers may be appealed to 52 FW/CD.

5.8. Interim Security Clearance Procedures:

5.8.1. In some situations, a person assigned to a sensitive position requires access to classified information prior to completion of a required initial investigation. Commanders may grant

interim security clearance for Top Secret and Secret access to classified information after the following process has been completed. NOTE: Interim clearances are not authorized when the member's eligibility is unfavorable or in question. Additionally, interim clearances are not required when associated with a re-investigation of the same scope.

5.8.1.1. Minimum requirements for interim Secret eligibility are:

5.8.1.1.1. Acceptable proof of citizenship and favorable review of Fingerprint results.

5.8.1.1.2. Favorable review of a completed SF86 and processed AF Form 2583.

5.8.1.1.3. The PSI is showing in "Open" status in DISS or successor system.

5.8.1.2. Minimum requirements for interim TS eligibility are:

5.8.1.2.1. Favorable completion of all requirements cited for interim Secret.

5.8.1.2.2. Favorable completion of a National Agency Check (NAC) (Shown in DISS).

5.8.1.2.2.1. If member does not have a previous investigation meeting NAC requirement, 52 FW/IP will add the extra investigation code "6" to the Agency Use Block (AUB) of the member's initial TIER 5.

5.8.2. Unit commander and member signs a memo on interim access and forwards to 52 FW/IP.

5.8.3. The SA will grant interim access in DISS or successor system. Once the PSI has been properly adjudicated, DISS will automatically update from the interim to the proper access.

5.8.4. When Top Secret access is required for urgent operational reasons (i.e., deployment), the Unit Deployment Manager (UDM) will request approval, from the gaining deployed unit commander, if Interim Top-Secret access can be used. If allowed, the SA will follow one-time/short duration access requirements.

5.8.4.1. Access must not exceed 180 days and is limited to specific, identifiable information. Access will be removed immediately when no longer required, at the conclusion of the authorized period of access, upon notification from the granting authority, or after 180 days from when access is granted, whichever comes first.

5.9. Not Used.

5.10. DISS or Successor System Access Requirements for Unit SAs:

5.10.1. Unit SAs are granted access to DISS or successor system for the specific purpose of managing personnel, verifying eligibility, and determining access to classified information of their service members/employees and/or visitors, validating CE enrollment, and reporting foreign travel. Other authorized uses of these systems will be identified by 52 FW/IP.

5.10.1.1. Member must have a security clearance of a TIER 3 or higher.

5.10.1.2. Member must be appointed in writing by unit commander.

5.10.1.3. Members must complete the appropriate DISS training, Protection of Personal Identifiable Information (PII) training and the Cyber Awareness course. Training links are on the 52 FW/IP SharePoint site.

5.10.1.4. Member must have a completed DD Form 2962, signed by their commander as the nominating official, for the system needed.

5.10.2. Once all requirements have been met, SA must forward information to 52 FW/IP.

5.10.3. Unauthorized Actions. The following DO NOT do list is not all inclusive, but users must ensure all actions are for official purposes. Any unauthorized activity is monitored by DMDC and could permanently remove your access, in addition open a security incident.

5.10.3.1. Querying DISS or successor system for your OWN record or any other record not for official purposes (i.e., celebrities, President, etc.).

5.10.3.2. Providing printouts of DISS or successor system data without proper authorization.

5.10.3.2.1. The SA may use the Security Clearance Verification Letter to provide for a member if security clearance information is needed. The letter is located on the 52 FW/IP SharePoint.

5.10.3.3. Sharing access, leaving DISS unattended or allowing unauthorized personnel access.

Chapter 6

CONTROLLED UNCLASSIFIED INFORMATION

6.1. Overview. All 52 FW personnel will properly safeguard and protection CUI from unauthorized access, disclosure, or observation. The DoD CUI Program maintains the DoD CUI Registry (**https://www.dodcui.mil**), which is comprehensive source of marking requirements, visual aids, infographics, and training resources. All personnel that handle CUI as high encouraged to utilize the DoD CUI Registry to aid in properly marking CUI.

6.2. Release and Disclosure:

6.2.1. The release or disclosure to foreign governments, international organizations, coalitions, or allied personnel of CUI not controlled as NOFORN will be in accordance with a law, regulation, or government-wide policy. Access to such CUI during official foreign national visits and assignments to DoD Components and cleared contractor facilities, when applied by contract, will be in accordance with DoDD 5230.20.

6.2.2. CUI that is not controlled as NOFORN may be released or disclosed to non-U.S. citizens employed by the DoD if:

6.2.2.1. Access to such information is within the scope of their assigned duties.

6.2.2.2. Access to such information would help accomplish a lawful and authorized DoD mission or purpose and would not be detrimental to the interests of the DoD or the U.S. Government.

6.2.2.3. There are no contract restrictions prohibiting access to such information.

6.2.2.4. Access to such information is in accordance with DoDI 8500.01 and 5200.02 and export control regulations, as applicable.

6.3. NOFORN and REL TO Markings:

6.3.1. NOFORN. All personnel will ensure the correct application of ‘not releasable to foreign nationals” NOFORN markings to CUI documents. The dissemination NOFORN is an intelligence control marking used to identify intelligence information an originator has determined meets the criteria of Intelligence Community Directive 710 and Intelligence Community Policy Guidance 403.1, which provides guidance for further dissemination control markings. It must be applied to controlled unclassified intelligence information that is properly characterized as CUI with appropriate CUI markings. CUI identified with this marking will not be provided, in any form, to foreign governments (including coalition partners), international organizations, foreign nationals, or other non-U.S. persons without the originator’s approval in accordance with E.O.s 13526 and 13556. If originator approval is required for further dissemination, the originator will mark the requirement on the information in accordance with Section 4.1(i)(1) of E.O. 1352.

6.3.1.1. The control marking NOFORN or NF will be applied to Naval Nuclear Propulsion Information (NNPI), Unclassified Controlled Nuclear Information (UCNI), National Disclosure Policy (NDP-1), and cover and cover support information. When warranted, it can be applied to unclassified information properly categorized as CUI having a licensing or export control requirement. Before marking a document or material as NOFORN or NF,

it will be reviewed by the Foreign Disclosure Officer to ensure there are no agreements in place to prohibit its use and sharing.

6.3.2. REL TO. All personnel will ensure the correct application of "releasable to" REL TO markings to CUI documents. The application of "Releasable to" ("REL TO") can only be applied, when warranted and consistent with relevant law, regulation, or government-wide policy or DoD policy, to information properly categorized as CUI with an export control or licensing requirement with a foreign disclosure agreement in place.

6.4. Not Used.

6.5. Not Used.

6.6. Not Used.

6.6.1. **Not Used.**

6.6.2. **Not Used.**

6.6.3. **Not Used.**

6.6.4. Procedures for CUI Incidents

6.6.4.1. Incidents involving CUI such as CUI misuse, unauthorized disclose (UD), improper CUI designation and marking, violation of CUI policy, and incidents potentially placing CUI at risk of UD shall be reported promptly to the SA, commander, and 52 FW/IP.

6.6.4.2. The SA will document the incident via an MFR and the Commander will endorse it. The MFR will contain a summary of what occurred and what management/corrective actions were taken in response. SAs will provide a copy of the signed MFR to 52 FW/IP.

6.6.4.3. Commanders will determine whether any appropriate management action and/or disciplinary actions are warranted based on the severity. For UD of CUI, a security inquiry is required if disciplinary actions will be taken against the individual(s).

6.6.4.3.1. Unauthorized Disclosure Reporting Procedures.

6.6.4.3.1.1. Personnel who discover a suspected UD, compromise, potential compromise, and/or loss of CUI must take custody of the material (if possible) and notify their supervisor and unit SA. The unit SA will notify 52 FW/IP and the unit commander.

6.6.4.3.1.2. The SA will notify the original CUI information owner.

6.6.4.3.1.3. The information owner will determine if an inquiry is necessary and proceed accordingly. The security manager/assistant needs to stay abreast of all findings to ensure appropriate mitigations are applied.

6.6.4.4. At minimum, the SA will document the incident as outlined in **paragraph 6.6.4.2**.

6.7. Procedures for handling of CUI. All 52 FW personnel have a personal responsibility to protect CUI. It is the responsibility of the user to properly safeguard CUI in their possession. Personnel must always keep CUI under their control or protect it with at least one physical barrier to reasonably ensure the CUI is protected from unauthorized access, disclosure, or observation. Viewing CUI documents in public settings is prohibited.

6.7.1. Handling during working hours. During working hours, steps will be taken to minimize the risk of access by unauthorized personnel, such as not reading, discussing, or leaving CUI information unattended where unauthorized personnel are present. Physical CUI documents will be protected by at least one physical barrier, the Standard Form 901 coversheet, on top of the documents. Users of electronic devices that display CUI such as monitors will use common sense measures to prevent unauthorized personnel from viewing the material. This can include turning off the computer monitor, or using a computer monitor screen cover to prevent unauthorized personnel from viewing the CUI information.

6.7.2. Handling when not under continuous monitoring or physical control. When CUI is not under continuous monitoring or physical control such as after hours, CUI will be stored in locked desks, file cabinets, bookcases, locked rooms, or similar secured areas.

6.7.3. Destruction of CUI. CUI material must be destroyed in utilizing one of the following below methods. The NSA Evaluated Products Lists (EPL) meets the below criteria for destruction of CUI. Units are encouraged to utilize the NSA EPL when purchasing shredders or disintegrators:

6.7.3.1. A cross-cut shredder that produces 1 mm x 5mm (0.04 in. x 0.2 in.) particles or smaller.

6.7.3.2. A pulverizer/disintegrator equipped with a 3/32 in. (2.4 mm) security screen.

6.7.4. Transmission and Proper Packaging for Mailing.

6.7.4.1. Electronic CUI information will be processed and transmitted utilizing the appropriate government information systems accredited for CUI. The use of non-government unapproved domains such as group chats, text messages, websites etc. is prohibited for processing or transmitting CUI information.

6.7.4.2. CUI information and material may be transmitted via first class mail, parcel post, or bulk shipments.

6.7.4.2.1. When mailing CUI, users will ensure the contents are protected by at least on barrier to prevent being able to see the contents.

6.7.5. Marking. All CUI material will be properly marked IAW with DoDI5200.48_DAFI16-1403 to alert personnel of CUI information. The SF 902, CUI Label, will be used for marking media and peripheral equipment.

6.8. Training Requirements. All 52 FW military, civilian, and contractor personnel will complete CUI training annually utilizing the CUI training on the myLearning platform.

6.9. Decontrolling Procedures for Originators. Originators of CUI information will decontrol the information when the CUI no longer requires safeguarding procedures. Decontrolling procedures can be found in Section 4 of DoDI5200.48_DAFI16-1403.

6.10. Removal from the workplace. Removal of CUI information or material from the workplace requires the approval of the unit commander/director.

6.10.1. Personnel removing CUI from the workplace must make sure the documents are properly marked and protected with at least one physical barrier (e.g., place the document in a folder, opaque envelope, or briefcase) to avoid unauthorized disclosure or observation while in transit.

6.10.2. Viewing CUI documents in public settings, or while using public transportation is prohibited.

6.10.3. CUI that is not under continuous monitoring or physical control shall be stored in a locked desk, file cabinet, or similar means, where only authorized personnel have access.

6.10.4. Prior to removing hardcopy CUI from the workplace, personnel will complete the required CUI training.

KEVIN M. CROFTON, Col
Commander

Attachment 1

GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

References

AFI 16-1404, *Information Protection Program*, 3 February 2023

DoDM 5200.01V1_AFMAN16-1404V1, *Information Security Program: Overview, Classification and Declassification*, 6 April 2022

DoDM 5200.01V2_AFMAN16-1404V2, *Information Security Program: Marking of Classified Information*, 7 January 2021

DoDM 5200.01V3_DAFMAN16-1404V3, *Information Security Program: Protection of Classified Information*, 12 April 2022

DoDM 5200.02_AFMAN16-1405, *Air Force Personnel Security Program*, 1 August 2018

DoDM 5220.22V2_AFMAN16-1406V2, *National Industrial Security Program: Industrial Security Procedures for Government Activities*, 25 Mar 2022

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

Prescribed Forms amd Adopted Forms

AF Form 310*, Document Receipt and Destruction Certificate*

AF Form 1109*, Visitor Register Log*

AF Form 2583*, Request for Personnel Security Action*

AF Form 2587*, Security Termination Statement*

DAF Form 847, *Recommendation for Change of Publication*

DD Form 254*, DoD Contract Security Classification Specification*

DD Form 2501*, Courier Authorization Card*

DD Form 2962*, Personnel Security System Access Request (PSSAR) Defense Manpower Data Center (DMDC)*

INV Form 86C*, Special Agreement Checks*

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

OF-306*, Declaration for Federal Employment*

OFI 86C*, Child Care Special Agreement Check (SAC)*

SF 85*, Questionnaire for Non-Sensitive Positions*

SF 86*, Questionnaire for National Security Positions*

SF 311*, Annual Agency Security Classification Management Program Data Report*

SF 312*, Classified Information Nondisclosure Agreement (NdA)*

SF 700*, Security Container Information*

SF 701, *Activity Security Checklist*

SF 702, *Security Container Check sheet*

SF 703, *Top Secret Cover Sheet*

SF 704, *Secret Cover Sheet*

SF 705, *Confidential Cover Sheet*

SF 901, *CUI Cover Sheet*

SF 902, *CUI Media Label*

SF 903, *CUI Media Label: USB size*

Abbreviations and Acronyms

OPR—Office of Primary Responsibility

ADP—Automated Data Processing

AF—Air Force

AFRIMS—Air Force Records Information Management System

AMS—Air Mobility Squadron

ANACI—Access National Agency Check and Inquiries

CC—Commander

CD—Deputy Commander

CDSE—Center for Development of Security Excellence

CE—Continuous Evaluation

CEIR—Continuous Evaluation Incident Report

CES—Civil Engineering Squadron

CFR—Code of Federal Regulations

CIP—Chief of Information Protection

CNWDI—Critical Nuclear Weapons Design Information

CPA—Classified Processing Area

CPO—Civilian Personnel Office

CUI—Controlled Unclassified Information

DCS—Defense Courier Service

DCSA—Defense Counterintelligence and Security Agency

DISS—Defense Information System for Security

DoD CAS—Department of Defense Consolidated Adjudications Services

DoDM—Department of Defense Manual

EAL—Entry Authority List

EAP—Emergency Action Plan

EMSEC—Emanations Security

E-APP—Electronic Questionnaires for Investigations Processing

FGI—Foreign Government Information

FOIA—Freedom of Information Act

FSO—Facility Security Officer

FW—Fighter Wing

GSA—General Services Administration

IDS—Intrusion Detection System

IMT—Information Management Tool

INDUSEC—Industrial Security

INFOSEC—Information Security

IP—Information Protection

JVS—Joint Verification Service

JWICS—Joint Worldwide Intelligence Communications System

MAJCOM—Major Command

MFR—Memorandum for Record

MICT—Management Internal Control Tool

NACI—National Agency Check and Inquiries

NACLC—National Agency Check, Local Agency Check with Law and Credit

NATO—North Atlantic Treaty Organization

NDA—Non-Disclosure Agreement

NDP—National Disclosure Policy

NIPRNet—Non-Classified Internet Protocol Router Network

NISP—National Industrial Security Program

NNPI—Naval Nuclear Propulsion Information

NOFORN—Not Releasable to Foreign Nationals

NSA—National Security Agency

OF—Optional Form

OPLANS—Operational Plans

PED—Personal Electronic Device

PERSEC—Personnel Security

PII—Personally Identifiable Information

POC—Point of contact

PR—Periodic Recertification

RD—Restricted Data

RDS—Records Disposition Schedule

REL TO—Releasable To

RFA—Request for Action

SA—Security Assistant

SAB—Spangdahlem Air Base

SAC—Special Agreement Check

SAP—Special Access Program

SAR—Security access requirement

SAV—Staff Assistance Visit

SCI—Sensitive Compartmentalized Information

SEAD—Security Execute Agent Directive

SETA—Security Education Training and Awareness

SF—Standard Form

SIPRNet—Secret Internet Protocol Router Network

SIR—Supplemental Information Requests

SJA—Staff Judge Advocate

SMO—Security Management Office

SOR—Statement of Reasons

SSBI—Single Scope Background Investigation

SSO—Special Security Officer

STE—Secure Terminal Equipment

STEPP—Security Training, education, and Professionalization Portal

SVOIP—Secure Voice Over Internet Protocol

TEMPEST—Electronics Material Protected from Emanating Spurious Transmissions

TSCO—Top Secret Control Officer

UCNI—Unclassified Controlled Nuclear Information

UMD—Unit Manning Document

US—United States

USPS—United States Postal Service

WCO—Wing Cybersecurity Officer

WIT—Wing Inspection Team

Attachment 2

EXAMPLE UNIT EMERGENCY PLAN TEMPLATE.

A2.1. Purpose. To establish procedures for the protection, removal and/or destruction of classified material located in building _____, room _____, on [installation]. These procedures will be executed in case of emergency, such as fire, natural disaster, civil disturbance, terrorist activities, or enemy attack.

A2.2. Background:

A2.2.1. Each activity authorized to process or store classified information must develop an emergency plan for protection of classified material. Note: for emergency plan requirements pertaining to special access program (SAP), sensitive compartmented information (SCI) and/or communications security (COMSEC), contact your local program security officer, special security officer or COMSEC custodian.

A2.2.2. Although the importance of protecting collateral material cannot be discounted, it must be accomplished in such a way as to minimize the risk of loss of life or injury to employees.

A2.3. Actions:

A2.3.1. If there is no imminent danger to employees:

A2.3.1.1. Thoroughly check workspaces for unsecured collateral material prior to departure.

A2.3.1.2. Secure collateral material in authorized containers before evacuation. Authorized containers are in [insert any unit specific locations/containers].

A2.3.1.2.1. If authorized storage is not immediately available, attempt to carry collateral material from the area, seeking assistance from other cleared personnel, as needed.

A2.3.1.2.2. Should circumstances require that some collateral material be left unattended, immediately report this fact to the 52 FW/IP.

A2.3.1.2.3. The holder will notify the senior government official, or incident commander at the central evacuation point that they are holding classified material or that classified materials has been left unsecured in the work area. The holder will provide the location, type of classified (i.e., media, documents, etc.) and the approximate amount. Protect the classified material until the emergency is terminated or take action to secure it in an approved security container. Individual is responsible for returning the classified information to the proper security container unless otherwise directed by the commander or the security manager. Under no circumstances will the classified material be transported to the holder's private living quarters.

A2.3.1.3. Upon cancellation of the emergency and when given the authorization to do so, employees will return to the work area and inventory any unsecured collateral material, reporting the results of this action to the security office. As appropriate, employees will also check security containers, secure rooms, and vaults for evidence of forced entry.

A2.3.2. If there is imminent danger to employees:

A2.3.2.1. Evacuate immediately, leaving collateral material in place. Under no circumstances should employees endanger themselves attempting to secure or remove classified information from workspaces.

A2.3.2.2. When possible, report the existence of unattended collateral material to the area supervisor who will then, as conditions allow, either arrange for monitoring of the area perimeter or contact the security office to report the situation.

A2.3.3. Should destruction of collateral material be warranted (e.g., enemy/terrorist attack):

A2.3.3.1. When possible, collateral material should be destroyed using equipment previously authorized for classified destruction (e.g., approved shredders and degaussers). Authorized destruction device is in [insert unit specific location of shredder/pulverizer/degausser etc]

A2.3.3.2. When such equipment is not available, or circumstances otherwise dictate, collateral material may be destroyed by any means that will ensure positive destruction of the material (e.g., burned).

A2.3.3.3. As possible, document the destruction of all accountable collateral material by noting, at a minimum, the accountability number (e.g., barcode or serial number).

A2.3.3.4. Report the overall destruction totals to 52 FW/IP or Command Post.

A2.3.4. Should circumstances preclude the protection or destruction of all collateral material, then appropriate prioritization should occur based on the classification level of the material. Consequently, the protection/destruction of top-secret material must take precedence over secret material, and so on.

A2.4. Responsibilities. Personnel working in areas that process classified information will ensure these procedures are posted to allow for easy access by personnel responsible for safeguarding collateral material.

Figure A2.1. Collateral Material Verification.

Office Point of Contact: _____Phone: _____

Unit Security Point of Contact: _____Phone: _____