BY ORDER OF THE COMMANDER
36TH WING

36TH WING INSTRUCTION 16-1400

23 APRIL 2020

Operations Support

WING INFORMATION PROTECTION (IP) PROGRAM

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: 36 WG/IP

Certified by: 36 WG/IP
(Mr. Chris R. Brown)
Pages: 43

This operating instruction establishes responsibilities for managing and executing the wing Information Protection (IP) program as required by AFI 16-1404, DODM5200.02_AFMAN 16-1405 and AFI 16-1406. It further addresses procedures and policies of Information Security, Personnel Security, Industrial Security and some portions of the Physical Security Program in relation to the protection of classified information. It applies to all 36th Wing units, associate units, and contractors assigned to, or visiting a 36th Wing unit. This includes tenant agencies on Andersen Air Force Base that have not specifically notified the Chief, Information Protection (CIP) in writing of non-participation with the exception of AFOSI. The use of a name of any specific manufacturer, commercial product, commodity, or service in this publication does not imply endorsement by the Air Force. Ensure all records created as a result of processes prescribed in this publication are maintained according to AFMAN 33-363, Management of Records, and disposed of in accordance with the Air Force Records Information Management System (AFRIMS) Air Force Records Disposition Schedule (RDS). Refer recommended changes and questions about this publication to the Office of Primary Responsibility (OPR) using the AF Form 847, Recommendation for Change of Publication; route AF Form 847 from the field through the appropriate functional chain of command. This publication may be supplemented at any level, but all direct supplements must be routed to the OPR of this publication for coordination prior to certification and approval.

1. Program Overview:

1.1. Purpose: Information Protection Program.

1.1.1. This OI outlines unit information protection program requirements. It prescribes appointment procedures and responsibilities for commanders and unit Security Assistants for managing and executing the IP program. It further addresses procedures and policies of the Information Security (INFOSEC), Personnel Security (PERSEC), Industrial Security programs and some portions of the Physical Security Program in relation to the protection of classified information.

1.2. The 36 WG/IP SharePoint Site

1.2.1. **https://andersen.eis.pacaf.af.mil/WingStaffAgencies/36WGIP/SitePages/Home.aspx**.

2. DUTIES AND RESPONSIBILITIES.

2.1. The 36th Wing Commander (CC) and Vice Commander (CV).

2.1.1. The 36 WG/CC provides oversight of IP by ensuring security controls, safeguards, and countermeasures are established through application of risk management principles, as appropriate, for the wing. The 36 WG/CV has delegated this responsibility to the 36 WG/CV.

2.2. Commanders/Agency Chiefs.

2.2.1. Establishes a viable IP program within their area of responsibility.

2.2.2. Appoints Security Assistants (SA) and Security Container Custodians (SCC) IAW **para 3**.

2.2.3. Reviews risk assessments conducted by Wing Cybersecurity Office (WCO) and 36 WG/IP for removable and wireless media violations.

2.2.4. Appoints an Inquiry Official (IO) for security incidents originating within their unit.

2.2.5. Reviews security incident reports and makes a determination for final disposition based on IO, Staff Judge Advocate (SJA) and 36 WG/IP recommendations if applicable.

2.2.6. Reviews IP Program Reviews (PR) and Staff Assistance Visit (SAV) reports and provides corrective actions for deficiencies.

2.2.7. Ensures contractors/classified contracts comply with DoD 5220.22-M and AFI 16-1406.

2.2.8. Identifies and approves, the following IP requirements. Approvals may be documented by memorandum with attached lists or spreadsheets.

2.2.8.1. Classified Processing Areas (CPAs) where classified information is processed and/or discussed.

2.2.8.2. Security containers used for storing classified.

2.2.8.3. Classified reproduction and destruction equipment.

2.2.8.4. Access Authorization Letters or Entry Authority Lists (EAL).

2.2.8.5. Derivative classifiers.

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

2.2.10. Implements the Continuous Evaluation (CE) program for all assigned personnel. Makes risk-based decisions for continuance of classified access during CE reviews.

2.3. **Chief, Information Protection.**

2.3.1. Executes IP on behalf of the 36 WG/CV and provides oversight and direction to group and squadron commanders, agency chiefs, SAs, and security specialists assigned to 36 WG/IP. The IP Office serves as the Activity Security Manager as required in DoDM 5200.01, Volume 1.

2.4. **Security Assistant (SA).**

2.4.1. Implements and monitors the Information, Personnel, and Industrial Security Programs, and some portions of the Physical Security Program below the wing level on behalf of the Activity Security Manager (36 WG/IP).

2.4.2. 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 36 WG/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.

2.4.3. Maintains the unit designated continuity book on the 36 WG/IP SharePoint site. ***NOTE****: Do not add PII on the 36 WG/IP SharePoint.*

2.4.4. Primary SA should conduct a self-inspection within 90 days of appointment. This self- inspection is utilized to provide an overview of the unit's IP program. This self-inspection will not count towards the self-inspection requirements in this instruction.

2.4.5. Ensures internal security operating procedures are tailored as necessary, annotated in unit operating instructions, disseminated to unit personnel, and implemented.

2.4.6. Ensures all training required by **paragraph 3.3**. is completed by unit personnel and documented.

2.4.7. Conducts and monitors annual security self-assessments and assists 36 WG/IP with data collection for the annual Enterprise Protection Risk Management (EPRM) assessment.

2.4.8. Ensures all appointed Security Container Custodians are properly trained.

2.4.9. Attends all SA meetings held by 36 WG/IP. The alternate SA will attend in the absence of the primary SA or a suitable unit representative must attend, if both SAs are unavailable. Geographically Separated Units (GSU) are not required to attend and will be provided slides and meeting minutes.

2.4.10. Monitors preliminary inquiries and formal investigations of security incidents for sufficiency and timeliness.

2.4.11. Manages the unit Joint Personnel Adjudication System (JPAS) roster (PSM Net) or successor system and ensures security clearance data is effectively tracked.

2.4.11.1. Ensures all assigned personnel are in-processed in JPAS as owning and grants access (indoctrinates) after verifying requirements in **para 5.1.1**.

2.4.11.2. Ensures personnel are out-processed in JPAS and debriefed as needed IAW **para 5.2**.

2.4.12. Directs unit personnel to complete security clearance investigations, as required.

2.4.12.1. Ensures 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*.

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

2.4.13. Arranges for security-in-depth determinations and risk assessments to be conducted by 36 WG/IP, 36 CS/Cybersecurity, 36 CES and 36 SFS for all proposed CPA's and spaces where classified discussions, meetings and briefings will occur.

2.4.14. Maintains a list of all CPAs and security containers used for storing classified, classified discussion/meeting/briefing areas, classified copiers, and classified destruction equipment used and/or assigned in their unit. Use the unit IP Folder on the 36 WG/IP SharePoint for tracking. The SA will update new and revised commander approval letters and trackers when changes occur.

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

2.4.14.2. Ensures 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.

2.4.15. Ensures plans for the protection, removal, or destruction of classified material in case of fire, natural disaster, civil disturbance, terrorist activities, or enemy action, to minimize the risk of its compromise are readily available. A copy of the plan can be found in *Annex Q, Appendix 2 of the AAFB Integrated Defense Antiterrorism Plan (IDATP).* Ensure a copy of the plan is posted in or near each security container and on the inside of the door to OSAs.

2.4.16. Can appoint Unit Security Representatives (USR) to assist with program management. The SA will determine the training requirements the USR will need to perform the specific duties. USR can be given access to JPAS, or successor system, to accomplish these duties.

2.5. **Security Container Custodians.**

2.5.1. Custodians are 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.

2.5.2. Ensures each security container and open storage area is properly managed IAW **para 4.2**.

2.6. **Unit Security Representatives.**

2.6.1. The USR can be any assigned unit member to perform specific duties, as identified by the SA, to enhance unit effectiveness in program management for IP related programs.

3. SECURITY ADMINISTRATION.

3.1. **Appointment of Security Assistants.**

3.1.1. Unit commanders must appoint a primary and alternate SA in writing and provide a copy to 36 WG/IP. The primary must be an E-5/GS-6 or above and alternates must be an E-4/GS-5 or above. See **Attachment 2** for appointment letter template.

3.1.2. SAs will accomplish training identified in **Attachment 3**. Once requirements have been completed, new SAs will forward all certifications to 36 WG/IP and schedule one-on-one training. Complete all training within 90 days of appointment.

3.2. **Appointment of Security Container Custodians.**

3.2.1. Commanders will appoint a primary and alternate SCC to maintain oversight for each security container, open storage area or vault. See **Attachment 4** for appointment letter template.

3.2.2. SCCs will accomplish training identified in **Attachment 5** and upload all training certs to the unit IP folder on 36 WG/IP SharePoint. Complete all training within 90 days of appointment.

3.3. **Information Protection Training.**

3.3.1. The SA will be listed on the unit's in-processing checklist and each assigned individual (military, civilian, and contractor) should immediately process through the SA. The following items will be either conducted or reviewed by the SA.

3.3.1.1. **Initial/Annual Andersen IP Training.** The 36 WG/IP Training Program covers all training requirements outlined in DoD and AF instructions and consists of Initial Indoctrination Training, Annual Refresher, and Continuous Security Education Refresher Training (CSERT). Select personnel will require additional focused training based on job responsibilities (e.g., courier, derivative classifiers, safe custodians, etc.).

3.3.1.2. **Initial/Indoctrination Training.** Newly assigned personnel will receive initial Andersen IP Training. Use the cleared or uncleared brief as appropriate. Training materials are located on the 36 WG/IP SharePoint. Administer the test for cleared personnel. Cleared personnel must pass with a minimum score of 80%. Test is open book. There is no test for uncleared personnel. Document the training for both cleared and uncleared personnel so it is available for review during evaluations and inspections.

3.3.1.3. **Annual Refresher Training.** Complete annual refresher training using the same process as initial Andersen IP training listed above. SAs must document the training completion.

3.3.1.4. **Derivative Classification Training.** SAs are required to maintain a copy of the training certificate, log training completion via database or spreadsheet and track expiration dates for derivative classifiers appointed in writing by the commander. Refresher training is due annually.

3.3.1.5. **North Atlantic Treaty Organization (NATO) Awareness Briefing.** All cleared personnel must receive the NATO Awareness Briefing and acknowledge receipt via signed memorandum upon in-processing. The SA will maintain memorandums. The briefing and acknowledgement template are available at 36 WG/IP SharePoint.

3.3.1.6. **Monthly CSERT Training.** The monthly CSERT plan is available on the 36 WG/IP SharePoint. The site provides topics and training documents for distribution and review on a monthly basis. The documents are designed to be disseminated via e-mail using the voting function to annotate personnel's receipt and review of the message. SAs may conduct briefings at Commander Calls or other training forums to disseminate the information. The goal of the continuous training program is for 100% of assigned personnel to receive the training, regardless of the method used.

3.4. **Program Reviews (PR).**

3.4.1. PRs will be conducted on an annual basis for 36 Wing units that process or store classified material on Andersen AFB and Geographically Separated Units (GSU). This may correspond with the Inspector General (IG) Vertical Inspection. As a minimum, PRs consist of INFOSEC, PERSEC and Industrial Security (if applicable) with a sampling of security containers, secure rooms and classified documents. Checklists are available at 36 WG/IP SharePoint. The Evaluator may cover other areas as required. Tenant unit inspections are unique and will be handled on a case-by-case basis for scope and authority.

3.4.2. A report will be provided to the unit commander, IG and SA detailing the areas evaluated and the findings. Unit commander must review and coordinate on all evaluation reports. Reports will be maintained in the SAs continuity binder.

3.4.3. Units will have 30 calendar days from the date of the report to provide an initial response. The response must indicate if the discrepancy has been corrected or a projected date of completion for items that cannot be sufficiently corrected within 30 days. Follow-up responses will be submitted to 36 WG/IP every 30 days until the deficiency is corrected.

3.5. **Security Self-Inspection.**

3.5.1. Local annual IP Program Reviews will be used to conduct, document and validate the annual wing IP Self-Inspection/Assessment. The SA will assist 36 WG/IP in processing these inspections/assessments. EPRM will be used to fulfill this requirement.

3.5.1.1. The Information Protection EPRM and 36 WG/IP checklist should be used for conducting unit self-inspections. The checklists are available on 36 WG/IP SharePoint.

3.5.2. At minimum, the SA should conduct a self-inspection within 90 days of being assigned to the program.

4. INFORMATION SECURITY PROGRAM.

4.1. **Classification and Marking Classified Materials.**

4.1.1. **Original Classification.** The initial determination that information requires, in the interest of national security, protection against unauthorized disclosure as determined by an Original Classification Authority (OCA). Andersen AFB does not have any OCAs assigned.

4.1.2. **Derivative Classification.** Derivative classification markings is a responsibility of all assigned personnel who incorporate, paraphrase, restate, or generate in new form information that is already classified or those who apply markings according to OCA guidance.

4.1.3. **Marking Information.** The proper marking of a classified document, to include e-mail, is the specific responsibility of the author. Classified markings alert the holder to the presence of classified information, reasons for classification, identity of the person that classified the document in the event of a classification challenge or questions arise, and provide guidance on downgrading and declassification.

4.1.3.1. All personnel will follow the marking standards for classified information, including working papers, as outlined in DoDM 5200.01, Volume 2 and AFI 16-1404 before storing in an approved security container. Additional marking guidance available on 36 WG/IP SharePoint.

4.1.3.1.1. The holder of an improperly marked classified document is responsible for contacting the originator to obtain correct markings and making the appropriate corrections before filing.

4.1.3.1.2. Documents, slideshows and websites that are not properly marked, ambiguous or unclear shall not be used as sources for derivative classification. Derivative classifiers should contact the source to clarify any classification issues.

4.1.3.1.3. Classified publications to include regulations, guides, plans, and other similar documents must be coordinated through 36 WG/IP prior to publication.

4.2. **Storage and Safeguarding of Classified Information.**

4.2.1. **Open Storage Areas (OSA).** An established area that is constructed in accordance with the requirements of DoDM 5200.01, Volume 3 and authorized by the senior agency official for open storage of classified information. OSAs include secure rooms and vaults designated for open storage of classified. The 36 WG/CC or CV approves all OSAs.

4.2.2. **Classified Processing Areas (CPA).** Any area that stores classified information, processes classified information, or houses security containers, classified meetings/briefings must be designated as a CPA. Some CPAs may concurrently be OSAs. SAs will track and Commanders will approve all CPA's. Approval letter and tracking templates are located on the 36 WG/IP SharePoint.

4.2.2.1. Designated CPAs are the only areas on Andersen AFB authorized to process classified information. The SA will ensure all CPAs are tracked and monitored within their unit and inform 36 WG/IP of any significant changes (i.e., structural modifications, office layout redesigns, and addition of secure information systems) that occur. The SA will coordinate with 36 WG/IP and Wing Cybersecurity Office to conduct assessments required for any new or additional CPA. GSU's will request assessments to 36 WG/IP for scheduling during annual program reviews.

4.2.2.2. The WCO is responsible for conducting EMSEC assessments and TEMPEST Certifications on all CPAs housing Automated Information Systems (AIS), communications systems, or cryptographic equipment.

4.2.2.2.1. 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.

4.2.2.3. **Security-in-depth and Risk Assessments.** 36 WG/IP is responsible for conducting security-in-depth and risk assessments for all CPAs. Security-in-depth assessments ensure a CPA's security program consists of layered and complementary security controls sufficient to deter and detect unauthorized entry and movement within the area. Results of assessments are logged on a consolidated CPA risk acceptance memo submitted to the unit commander.

4.2.2.3.1. Once the area meets all requirements, the CPA will be added to the unit CPA approval letter and tracking spreadsheet. If the CPA is or will be a certified OSA, secure room or vault, additional surveys are required by 36 CES (structures) and 36 SFS (alarms). Additionally, notify 36 WG/IP for any removal of an established CPA. GSU's will utilize local CE and SFS equivalent agencies for surveys.

4.2.2.4. **Portable Electronic Devices (PED).** The use of government or personal cellular and or radio frequency (RF), infrared (IR) wireless devices, and other devices such as cell phones and tablets, and devices that have photographic or audio recording capabilities are prohibited in all CPA's unless specifically approved by the appropriate approval authority. All cleared personnel are responsible for being alert to detect these items and immediately report violations.

4.2.2.4.1. Personnel operating within active CPAs are required to ensure the PED Poster (available at 36 WG/IP SharePoint) is visibly posted on the exterior of entrances to CPAs while classified processing/discussion is in progress.

4.2.2.4.2. 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.

4.2.2.4.3. Prohibited electronic devices discovered within an active CPA will be immediately powered off and removed from the CPA. Refer to **paragraph 4.5** of this instruction for details.

4.2.2.5. **Electronic Flight Bags (EFB).** These devices are primarily used for electronic Flight Information Publications (eFLIP), in-flight publications, and aircrew/operations productivity tools on the ground or in-flight.

4.2.2.5.1. **Approved use.**

4.2.2.5.1.1. EFBs are approved for use in the Tropicana and Wing Operations Center (WOC). Ensure the requirements in the following paragraphs are met.

4.2.2.5.1.2. For CPAs other than the Tropicana and WOC, a letter, signed by the owning unit/enclave commander or above, designating authorized areas for EFB use

4.2.2.5.1.3. Flying squadrons deployed or TDY to Andersen AFB are authorized to use their EFBs in the Tropicana and WOC. Deployed EFB POC will coordinate with the 36 Wing EFB Manager for local requirements before bringing any EFBs into the Tropicana or WOC.

4.2.2.5.2. **Prerequisites.** The following is required prior to EFB use in PACAF-controlled collateral classified processing areas:

4.2.2.5.2.1. Unit developed specific security classified processing area guidance on how each unit will implement the EFB checklist.

4.2.2.5.2.2. AF Form 4170 submitted to AF-CTTA with EFB use addressed within the package (can be used as the Risk Assessment).

4.2.2.5.2.3. Risk assessment for each area if the AF Form 4170 if not used to document the RA.

4.2.2.5.3. **EFB use in CPAs.** The following is required for EFB use in PACAF-controlled collateral classified processing areas:

4.2.2.5.3.1. Approved AF Form 4170. The approved AF Form 4170 will list the minimum separation distances for properly configured EFBs must maintain from classified processing equipment.

4.2.2.5.3.2. Appropriate MAJCOM Configuration Profile loaded.

4.2.2.5.3.3. Units will comply with the entire MAJCOM security checklist before bringing EFB devices into a CPA and upon exiting the facility.

4.2.2.5.3.4. Logging of all EFB's entering and exiting approved CPA's on the EFB CPA Log each time the device is brought into and leaves the CPA.

4.2.2.5.3.5. EFBs entering into the CPA facility require a "Checklist Complete" tag and must be under the control of an authorized user. Devices must never be left unattended while in the CPA.

4.2.2.5.3.6. EFBs may be stored in a designated area outside of the CPA. The first two steps of the checklist must be complete when leaving the EFBs unattended, but no tag is required.

4.2.3. **Safeguarding and Storage.** All classified material, when not under direct surveillance of an authorized person, will be stored in a GSA approved security container or OSA to prevent unauthorized access or compromise.

4.2.3.1. Follow procedures in **paragraph 5.1.2**. of this OI for authorizing access to classified information. Use DoDM 5200.01 and AFI 16-1404 for additional information on protecting classified information outside of a storage container.

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

4.2.3.2.1. 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. Do not release classified to any agency that does not have adequate storage capability.

4.2.3.2.2. All requests for removing Secret and Confidential material from designated work areas for work at home will be submitted through 36 WG/IP. HQ PACAF/IP has final approval authority. 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.

4.2.3.3. Each security container will be tracked by the SA. For ease of tracking, security containers can be added to the CPA tracking spreadsheet and authorization letter. A separate letter and tracker is not required. At a minimum, the following information will be on the tracker: Security Container Serial Number, Location, Primary Custodian, Last Inspection and Location of the SF-700, Part 2 (Combo).

4.2.3.4. Each security container and OSA will have a minimum of one SCC appointed. Serviceability, operational visual inspections, and contents of the security container or OSA are the responsibility of the custodian.

4.2.3.5. Each security container and OSA will have an inventory of all classified documents, equipment, and material in the security container, secure room or OSA. The inventory listing will be unclassified and maintained within the security container, or OSA. The inventory will be used for accountability in case of emergencies or if the container/room was left open unattended to account for missing classified items.

4.2.3.6. Security container custodians responsible for the security container, or OSA will be listed first on the Standard Form 700, *Security Container Information*.

4.2.3.7. Each security container, open storage area, and vault will have an access authorization letter or Entry Authorization List (EAL). The letter or list will be signed by the commander and endorsed by the SA for validation of clearances. They shall be updated quarterly or as changes occur. ***NOTE****: The EAL is only used if the area is designated as a Restricted/Controlled Area under the Physical Security Program.*

4.2.3.7.1. The EAL/Access Authorization should be readily available on or near the applicable container, secure room or OSA. ***NOTE****: The unit commander is responsible for the classified in the unit and does not need to be on the access letter.*

4.2.3.7.2. When personnel, not listed on the EAL/Access Authorization, require access to the container or OSA, a credential and clearance access verification must occur through JPAS (or successor system) or verified by memorandum endorsed by a SA or a JPAS Visit Request. In addition to clearance verification, need-to-know must also be verified.

4.2.3.7.3. "Vouching" for another individual's clearance access level is not an approved method to utilize for providing access to classified information. All clearances and accesses must be verified prior to entry in JPAS or successor system.

4.2.3.7.4. Log visitors not on an EAL/Access Authorization Letter on the AF FM 1109, *Visitor Register Log*, and maintain forms for 90 days. ***NOTE:*** *Logging visitors is not required when personnel are accessing a sanitized/inactive CPA housing a locked security container.*

4.2.3.8. Restrict combinations for classified to appropriately cleared personnel who are authorized access to the classified material stored therein.

4.2.3.8.1. 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: Change of combination date.*

4.2.3.9. **Operational Visual Inspection (OVI).** An OVI will be accomplished on all security containers or OSAs utilizing the checklist in AFI 16-1404, Attachment 6 (available on 36 WG/IP SharePoint). An OVI is required to be conducted upon receipt and every 5 years. After checklist completion, custodians are required to record the OVI on the OF-89. Custodians will keep a hard copy of the form in the control drawer of the container or posted on the interior of the OSA door.

4.2.3.9.1. OVI discrepancies will be reported to 36 WG/IP and a determination will be made if GSA certified locksmith maintenance or assessment is required. If determined a locksmith is needed, the unit/agency will initiate a work request to a local GSA certified locksmith or 36 CES Customer Service for secure room/vault doors considered real property.

4.2.3.10. **Locksmith.** A GSA Certified Locksmith will be immediately notified of security container lockouts and repairs affecting the function of securing classified information. An uncleared locksmith will not be allowed access to classified materials while performing maintenance on security containers and must be under constant surveillance by the container custodian or other authorized and cleared unit representative. Whenever possible, remove all classified from the security container before a locksmith performs repair or maintenance.

4.2.3.11. **Optional Form 89, Maintenance Record for Security Containers/Vault Doors (OF 89).** Locksmiths who conducted maintenance/repairs will be logged on the OF 89 which replaces the Air Force Technical Order (AFTO) Form 36, *Maintenance Record for Security Type Equipment*. Maintain all records of security container and OSA door maintenance, repairs, and inspections (OVI) while the container is in use. The AFTO Form 36 can be destroyed if there is no record of maintenance or repairs on the security container.

4.2.4. **Opening and Closing of security containers and OSAs.** Authorized personnel will use the SF 702, *Security Container Check Sheet*, to record each opening, closing, and checking of security containers and OSAs. Completed SF 702s are required to be filed for 90 days.

4.2.4.1. Use a new SF 702 at the beginning of the month for each security container. When containers are infrequently opened, a single SF 702 may be used to annotate multiple months as long as the delineation is clearly marked on the form.

4.2.4.2. **End-of-Day Security Checks.** Each CPA will establish procedures to perform end-of-day checks using the SF 701, *Activity Security Checklist*. Completed SF 701s are required to be filed for 90 days. As a minimum, section leaders will ensure the last person departing the office or area (CPA) for the day conducts the end-of-day checks. Only cleared personnel are authorized to conduct these checks. Ensure newly assigned personnel are familiar with procedures.

4.2.4.2.1. 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.

4.2.4.2.2. On weekends, down-days or holidays, the SF 701 does not need to be annotated unless the room is accessed. For Secure Internet Protocol Router Network (SIPRNET) assets, if the room or building was opened but a container or OSA was not opened, the person closing the office and/or building will check the container or OSA to ensure it is still locked and annotate the check on the SF 701 and annotate the “checked by” block on the SF 702.

4.2.4.3. When performing end-of-day security checks:

4.2.4.3.1. Conduct a check of the security container(s)/OSA(s) by spinning the dial on the lock to ensure the lock is engaged and attempt to open the container or door. ***NOTE:*** *Checked by column annotation of SF 702 is required for containers/OSAs containing Defense Information Security Agency (DISA) computer assets when the room/bldg is occupied, even if the container/OSA is not accessed. (Security Technical Implementation Guide (STIG) Requirement).*

4.2.4.3.2. Check computer(s) and printer(s) authorized to process classified information as well as Tactical Local Area Network Encryptor(s) (TACLANE), ensuring all classified removable hard-drive(s), switches, Cryptographic Ignition Key(s) (CIK) etc., are removed and properly secured.

4.2.5. **Specific OSA Requirements.** The 36 WG/CV certifies OSAs and bulk storage areas of classified information, in writing. ***NOTE****: This does not include the authority to certify Sensitive Compartmented Information Facilities (SCIF) or Special Access Program Facilities (SAPF).*

4.2.5.1. Organizations will notify 36 WG/IP, in writing of all OSA and bulk storage area requirements. This request will be signed by the unit commander and include the OSA or bulk storage area justification, building number and room number, and a layout of the facility. OSAs will **NOT** be approved for convenience. There must be an operational need where storing classified in GSA approved security containers is not practical or possible.

4.2.5.1.1. 36 WG/IP, with assistance from 36 CES, 36 SFS and WCO will conduct an assessment of all proposed and modified OSAs to ensure security requirements and construction standards are met IAW DoDM 5200.1, Volume 3. Results of the assessment will be documented in writing and the 36 WG/CV will give final approval on letter. 36 WG/IP maintains the original approved package and the requesting organization displays the certificate on the back of the OSA door.

4.2.5.2. Organizations must notify 36 WG/IP in writing when an OSA is no longer needed.

4.2.5.3. Intrusion Detection Systems (IDS) are required for all OSAs. 36 SFS/S5 is the POC for all IDS related issues, to include IDS new installs, certifications and maintenance. During IDS outages/malfunctions, the minimum requirement for supplemental controls are 4-hour checks conducted by owning unit. If 4-hour checks cannot be conducted, owner/user must relocate classified materials to another approved security container/OSA or provide continuous surveillance until the IDS is operational. USN Security is the POC for all IDS related issues for Diego Garcia.

4.2.5.4. The use of 4-hour checks is not authorized for convenience when the IDS is operational or when physical security requirements are not met such as high security lock failures. Users must provide continuous surveillance of the unprotected area until the condition is repaired or relocate classified materials to another approved security container/OSA.

4.2.5.5. Any new construction or modification of OSAs must be coordinated with 36 WG/IP.

4.2.6. **Top Secret Information.**

4.2.6.1. **Top Secret Control Accounts (TSCA).** The unit commander may formally establish a TSCA by letter if the unit handles large inventories of hardcopy collateral TS. Maintain this letter with the account, and provide a copy to 36 WG/IP who will provide training for all Top Secret Control Officers (TSCO) NLT 45 days after appointment. Recurring TSCO training will be conducted by request from the TSCO. TSCO are responsible for training all personnel within their unit that work directly with Top Secret materials. All training will be documented with the type of training and date conducted.

4.2.6.2. **Top Secret Inventories.**

4.2.6.2.1. The unit commander will designate officials to conduct annual inventories for all Top Secret material in the account.

4.2.6.2.2. Conduct annual inventories every January and when there are TSCO changes. The inventory official must be someone other than the appointed TSCOs, meeting the proper security clearance requirements.

4.2.6.3. Refer to DoDM 5200.1, Volume 3 for further guidance on storage and protection of Top Secret materials.

4.2.7. **Unique Situations.**

4.2.7.1. In the event an aircraft carrying classified material lands unplanned at Andersen AFB, 36 WG/IP can be contacted for storage guidance. The 36 WG/CP is designated as a transient AIRCREW storage location for classified up to collateral Top Secret. If the aircraft is transporting Top Secret or Sensitive Compartmented Information (SCI), 36 WG/SSO must also be contacted.

4.2.7.2. Andersen AFB flight-line consists of restricted and controlled areas. Any processing, deployment or shipment of classified is authorized provided the material is under constant surveillance by the owner/user or authorized custodian/courier. GSA approved security containers that contain classified configured for cargo shipment must also be under constant surveillance. Owner/user maintains full responsibility until the classified is loaded on the aircraft or custody is transferred via DD Form 1907, *Signature and Tally Record*.

4.3. **Destruction and Reproduction.**

4.3.1. **Destruction.** Commanders will ensure classified information is destroyed by authorized means and appropriately cleared personnel in accordance with the methods and procedures prescribed in DoDM 5200.01, Volume 3 and this OI. SA's will develop a Shredder Designation Memo/Listing for this purpose that lists the approved destruction devices and NSA approval verification of each device. This memo/listing will be signed by the commander.

4.3.1.1. The annual clean-out day occurs on the third Wednesday of January. The number of items of each classification destroyed will be documented in a memorandum and uploaded to the unit's folder on the 36 WG/IP SharePoint site.

4.3.1.1.1. During the annual clean-out day, each piece of classified material will be reviewed and a determination to retain or destroy will be made. Check with the 36 WG Historian before destroying information which may be of historical value. Units and staff agencies are encouraged to continuously audit classified holdings throughout the year and destroy as necessary.

4.3.1.1.2. Shredder purchases will be routed through the SA to ensure they meet the proper requirements for classified destruction and will be added to the Shredder Designation Memo/Listing upon receipt.

4.3.1.1.3. Visual aids will be posted by, or on designated shredders which will indicate whether the equipment is authorized for the destruction of classified or controlled unclassified material.

4.3.1.1.4. Removable computer media such as floppy disks or classified hard drives must be sanitized using appropriate computer software prior to destruction. This software must meet the criteria of AFSSI 5020, Remanence Security, Chapters 4 through 8. For authorized software, contact your Unit Cybersecurity Liaison (CSL). Should physical destruction of computer media be appropriate, refer to DoDM 5200.01 and AFI 16-1404.

4.3.1.2. All Controlled Unclassified Information (CUI) must be shredded IAW NIST SP 800-88 *Table A-1: Hard Copy Storage Sanitization* to prevent authorized disclosure of personal, sensitive and critical information. Shredders must meet the high security standard (1mm x 5mm) (0.04 in. x 0.2 in.) in size (or smaller).

4.3.1.3. Material produced by approved NSA destruction devices (shredders, optical destroyers etc.) will be inspected for proper sanitization before disposal (long strings, clumps etc.). Material that does not meet the required sanitization size for classified, will not be disposed of until it is properly inspected and sanitized.

4.3.1.4. Destruction devices require periodic cleaning to maintain standards. Devices authorized for destruction of classified will be inspected periodically and cleaned if necessary. Ensure devices are unplugged before cleaning the shredder blades. Recommend using a toothbrush or wire brush without touching the blades. Devices that do not maintain the required standards after cleaning will be removed from use.

4.3.1.5. Plans for the protection, removal, or destruction of classified material must be readily available. A copy of the plan can be found in *Annex Q, Appendix 2 of the AAFB Integrated Defense Antiterrorism Plan (IDATP).* Ensure a copy of the Classified Emergency Destruction plan is posted in or near each security container and on the inner door of OSAs.

4.3.2. **Classified Reproduction Procedures.**

4.3.2.1. **Copiers.** Classified reproduction will only be conducted on approved copiers.

4.3.2.1.1. SAs must coordinate with the WCO and 36 WG/IP prior to seeking approval of a copier to reproduce classified information.

4.3.2.1.2. Unit commanders will approve any copiers that reproduce classified information.

4.3.2.1.3. Copiers with information storage devices (i.e. hard drives) must be located in an open storage area to be considered for approval to reproduce classified information. At no time will a copier that is connected to the Non-Secure Internet Protocol Router Network (NIPRNET) be used for classified reproduction. Contract copiers approved for classified reproduction removed from service must have their hard drives removed and properly disposed of by WCO.

4.3.2.1.4. SAs are responsible for security control and development of copying procedures for each approved copier within their unit.

4.3.2.1.5. All copiers will have the required visual aids showing whether or not copiers are authorized for reproduction of classified.

4.3.2.1.6. Inspect reproduction equipment as part of the End-of-Day Checks to ensure no classified material remains in, on, or near it.

4.3.2.2. **Printers.** Users will be familiar with proper clearing procedures. Classified Printer Clearing Procedures Visual Aid will be posted by each classified printer unless they are in an OSA.

4.4. **Classified Transmission and Transportation.**

4.4.1. 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 DoDM 5200.01, Volume 3 and this OI.

4.4.2. 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.*

4.4.2.1. Mailing out-going classified packages.

4.4.2.1.1. 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.

4.4.2.1.2. 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.

4.4.2.1.3. 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 remains in U.S. postal channels at all times.

4.4.2.1.3.1. If the USPS cannot ensure the mail remains in U.S. postal channels at all times, the Defense Courier Service (DCS) may be used. The closest DCS office is located at Yokota AB, Japan. Please see the DCS Customer Service Guide posted on the 36 WG/IP SharePoint.

4.4.3. **Using the Phone/FAX for Classified Transmission.**

4.4.3.1. **For Verbal Discussions:**

4.4.3.1.1. Use a Secure Terminal Equipment (STE), Secure Voice Over Internet Protocol (SVOIP) or other authorized secure communication equipment.

4.4.3.1.1.1. Follow the encryption procedures for that equipment.

4.4.3.1.1.2. While using equipment, ensure unauthorized personnel are not within hearing range of your voice.

4.4.3.1.1.3. Ensure the person on the other end of the line has the proper security clearance eligibility to receive the message.

4.4.4. **Transmission through Classified Meetings/Briefings.** The Classified Conference and Meeting Checklist in AFI 16-1404, Attachment 4 must be followed when hosting a classified briefing in a room other than one previously cleared for such meetings; i.e., designated CPA. If there becomes a need to utilize a room for these purposes on a regular basis call 36 WG/IP to properly approve the requested room as a CPA.

4.4.4.1. Do not post signs, or cover sheets stating the level of classification on doors or entrances to classified meetings/briefings.

4.4.5. **Transporting (Hand-Carrying) classified information on base.**

4.4.5.1. When classified material is hand-carried on base, 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. 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.

4.4.5.2. Supervisor's verbal authorization is required prior to an individual hand-carrying classified information to activities on the installation. Courier authorization designation letters are not required, unless the courier will be entering an entry control point on the installation, where the materials are subject to search (i.e., controlled areas, restricted areas, facility entry points during increased Force Protection Conditions, etc.).

4.4.5.2.1. Use a local courier authorization designation letter (for on-base use only) or the DD Form 2501, Courier Authorization Card signed by the unit commander, which is valid for one year or when authorizing officials and couriers change (e.g., assignments, change positions, etc.). The letter/Card exempts classified materials being hand-carried from examination. Authorization Designation Letter format is available at 36 WG/IP SharePoint.

4.4.5.3. When emergency situations occur during local operational readiness exercises, real world contingencies, or increased Force Protection Conditions (e.g., relocation of wing, group, or unit control centers, etc.), individuals do not need to be in possession of a local courier authorization designation letter when transporting or relocating classified information.

4.4.5.4. Personnel carrying classified material between buildings on the installation will not deviate from their route between departure and arrival points. Stops for unofficial business such as conversations, snacks, and mail box check, etc., are prohibited.

4.4.6. **Transporting (Hand-Carrying) classified information off base.**

4.4.6.1. The SA must be notified prior to any off-base hand-carry of classified materials.

4.4.6.2. The unit commander will approve the hand-carry of classified information off the installation. Only the commander can authorize the hand carrying of classified materials aboard commercial airline flights. ***NOTE:*** *SIPRNET is the primary and most secure means of transmitting classified information.*

4.4.6.3. 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. The DD 2501 is preferred when transporting through military or commercial air off island.

4.4.6.3.1. 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. The SA will prepare courier designation letter and exemption notice that facilitates passage of material through the Federal Aviation Administration passenger screening points. Courier letter and exemption notice format is available at 36 WG/IP SharePoint.

4.4.6.3.1.1. Advance coordination should be made with airline and departure terminal officials and, when possible, with intermediate transfer terminals when your mode of travel is by air.

4.4.6.3.2. All personnel going temporary duty (TDY) that are required to carry classified material must have the following statement included in block 16, remarks section of DD Form 1610, Request and Authorization for TDY Travel of DoD Personnel, “Travelers are authorized to carry classified material”. SAs will coordinate on TDY orders for those individuals requesting authorization to transport classified off the installation.

4.4.6.3.3. When hand carrying classified information over international borders, the courier must have identification and an authorization letter meeting the requirements of DoDM 5200.1, Volume 3. The authorization letter will be written in English and if possible, in the language of the countries through which the courier is traveling.

4.4.6.4. Classified material hand carried by a courier must be inventoried; the courier's SA shall retain a copy of the inventory and the courier shall carry a copy. Do not open, display or otherwise use in public places.

4.4.7. **In-Transit AIRCREW Overnight Classified Repositories on Andersen AFB.**

4.4.7.1. 36 WG/CP, Bldg 23028, 36 WG/CP, DSN 366-2981 (Top Secret/Secret/Confidential).

4.4.7.2. 36 OSS/Intel Flight, Bldg 25002, DSN 366-2341 (Top Secret/SCI).

4.4.7.3. If personnel are TDY on an official visit, they may use the above storage locations or they may store their classified with the agency being visited, provided the agency is capable of storing classified material to the appropriate level. In the event an individual arrives with SCI, contact 36 WG/SSO personnel immediately. At no time will SCI material be stored in a non-SCI approved facility.

4.5. **Security Incidents.**

4.5.1. Anyone discovering a security incident will immediately take control of the situation or material, report and safeguard it until the responsible custodian or other official regains proper custody.

4.5.1.1. Immediately report and secure unsecured/unattended classified material by maintaining personal control, cover the material to avoid potential compromise and make contact with the SA, safe custodian, supervisor, unit commander or 36 WG/IP at DSN 366-5108 or 5815.

4.5.1.1.1. Take the following immediate action when a security incident with an Automated Information System (AIS) is suspected: Disconnect network access to component, lock computer system down under current user and **DO NOT** shut down or unplug the computer power. All AIS systems will be protected as classified until sanitized.

4.5.1.1.2. Any time the 36 CS receives notification of a suspected security incident involving AIS, they will immediately notify 36 WG/IP of the incident prior to sanitizing any AIS hardware or software to safeguard against the loss of potential evidence.

4.5.1.2. All personnel must be alert and report discovery of unauthorized electronic/wireless device(s) within a CPA. Reports can occur at any level within the chain-of-command, but should be funneled to the SA and subsequently the 36 WG/IP Office.

4.5.1.2.1. 36 WG/IP in consultation with the unit commander and WCO determines whether a security incident inquiry should be initiated and the disposition of the device. Government devices may be confiscated to determine if it's contaminated with classified information. If it is suspected a personal device is contaminated with classified information, request the individual surrender it. If the individual refuses to surrender the device, the commander will consult with 36 WG/JA on how to resolve the issue.

4.5.1.2.1.1. An AF Form 52, *Evidence Tag*, will be provided to the owner, for accountability purposes if a government or personal device is confiscated. Personnel will be informed on the process for retrieving the device.

4.5.1.3. After duty hours, when the personnel in **paragraph 4.5.1.1**. cannot be contacted, notify the 36 WG/CP at DSN: 366-2981, who will in-turn contact 36 WG/IP and/or 36 CS personnel.

4.5.2. **Appointing Authority (AA) Responsibilities.** Upon notification from 36 WG/IP, the responsible commanders will appoint an Inquiry/Investigative official (IO), to ascertain the circumstances surrounding the security incident, within two duty days from the discovery of the incident, and will inform 36 WG/IP of the appointment in writing. 36 WG/IP will send the template when the notification is made via e-mail. The template is also available on the 36 WG/IP SharePoint. 36 WG/IP will provide the AA and IO the assigned incident number.

4.5.2.1. IOs will be in the grade of E-7 or above when incidents do not warrant a higher grade. IOs will not be less in rank or grade than the person(s) involved with the incident, will not be the assigned primary or alternate SA, will not be persons assigned to 36 WG/IP and should not be persons in the direct chain of command. The inquiry official must be a disinterested member not associated with the activity (section/element, etc.) where the security incident occurred. Additionally, IOs must be cleared to the highest level of information involved.

4.5.2.2. All IOs will contact 36 WG/IP within two duty days of appointment to schedule a briefing prior to initiating the inquiry.

4.5.2.3. IOs must complete the preliminary inquiry and forward results to 36 WG/IP, within 10 duty days of receiving the IP brief. Requests for extensions must be in writing from the unit commander and forwarded to the CIP. Extensions may be included in the closure memorandum.

4.5.2.3.1. IOs contact the SA to verify, through JPAS, all personnel related/involved in the inquiry have the appropriate security clearance eligibility. The IO then determines and reports facts, makes conclusions of whether or not classified information was actually, potentially, or suspected of loss or compromise, characterize the incident as a security infraction or violation and recommend actions to prevent future incidents. IOs should not recommend punitive action against individuals.

4.5.2.3.2. Complete preliminary IO reports utilizing the format provided by 36 WG/IP and available at 36 WG/IP SharePoint.

4.5.2.4. The IO coordinates draft report with 36 WG/IP for a technical review, before finalizing report.

4.5.2.5. 36 WG/IP submits the IO report and the IP Technical Review to the AA to approve, endorse, and close the inquiry. Closure actions must be completed no later than 30 days after initial notification of the incident.

4.5.2.5.1. AAs will complete the AA Closure Memorandum when closing an incident. The closure memo will outline if an actual, potential or suspected loss or compromise occurred or did not occur and whether or not further investigation is needed; any corrective actions implemented to prevent further similar occurrences; any administrative, disciplinary or punitive action taken against individual(s) responsible for the violation if warranted. The template will be provided to the IO for processing.

4.5.2.5.2. In instances where a commander seeks administrative or punitive action against culpable individual(s) as a result of the incident, forward the IO report and 36 WG/IP Technical Review to 36 WG/JA for legal review prior to closing the incident.

4.5.2.6. Once the AAs closure memo is completed and forwarded to 36 WG/IP, the incident will be closed and all associated paperwork will be electronically filed within the 36 WG/IP Office.

5. PERSONNEL SECURITY PROGRAM.

5.1. **In-Processing.** All military and DoD civilians assigned to a unit must be in-processed in JPAS 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 JPAS within 15 days of arrival. Contractors requiring access to classified will be serviced in JPAS 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 UMD. The SA is authorized to grant access in JPAS 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 JPAS. ***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 JPAS 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 the Defense Information System for Security (DISS). Only CE enrollment dates of 1 October 2018 to present are valid enrollment dates. If there is an invalid date, contact 36 WG/IP for further instructions.

5.1.1.1.2. If JPAS 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 36 WG/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 JPAS. If member does not have, complete and add to JPAS.

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/indoctrination IP training.** Training materials can be accessed on the 36 WG/IP SharePoint site. The SA will ensure to document this training.

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 JPAS 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 JPAS. 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 36 WG/IP.

5.3.1.1. When changes are necessary, SA will complete Authorization Change Request (ACR) form and provide to 36 WG/IP for coordination. Send final form to 36 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 36 WG/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 are 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 Periodic Reinvestigation (PR) 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 are conducted by DCSA and are required for military and civilian employees' initial Secret security clearance or assignment to noncritical sensitive 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. **TIER 5 (Previously Single Scope Background Investigation [SSBI]).** TIER 5's are 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 36 WG/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 reinvestigation. 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 36 WG/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. 36 WG/IP will initiate the member's investigation in e-QIP 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-QIP 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-QIP and fingerprints along with required supporting documentation (i.e., OF-306, *Declaration for Federal Employment*, applicant's resume, childcare paperwork, etc.) as required. 36 WG/IP will conduct the final reviews of TIER 3/5s and submit to DCSA.

5.5.3. Once the member submits their e-QIP for review, 36 WG/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 DoDCAF 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****: 36 WG/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-QIP 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 36 WG/IP Office prior to submittal of a TIER 3/5.

5.5.4.3. In order for the DoDCAF 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 36 WG/IP Office for processing and can be in a memorandum or email format.

5.5.5. When DoDCAF 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 DoDCAF provides a SOR stating intent to deny or revoke a clearance, the member must respond to DoDCAF, through the SA and 36 WG/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 36 WG/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 36 WG/IP Office will not be able to process any documentation on behalf of the member.

5.5.5.2.1. If the DoDCAF 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 DoDCAF through the 36 WG/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 36 WG/IP for further information. When a member has their security clearance suspended, denied, or revoked, 36 WG/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 Periodic Reinvestigation (PR) process for TIER 3/5 investigations. This program will allow members to maintain clearance eligibility by accomplishing continuous requirements instead of completing a PR over a set period of time. In order to get every member enrolled into the CE Program, members will need to accomplish their next PR, at the normal required time interval.

5.6.2. The SA will run a monthly JPAS personnel report. The SA will monitor reinvestigations coming due within 120 days of the previous close date using the Defense Intelligence Agency's (DNI) temporary PR timeframes (10 years for Secret and 6 years for Top Secret) and initiate an investigation IAW **paragraph 5.4**.

5.6.2.1. Once member completes the PR, 36 WG/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. PRs submitted to DCSA will eventually be enrolled automatically into the CE Program after investigation has been completed and submitted to DoDCAF 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 36 WG/IP. Under the CE program, there are two reporting categories. These are DoDCAF CE Incident Report (CEIR) and Local CE Report.

5.6.3.1. **DoDCAF CEIR Alert.** This is a downward report from DoDCAF identifying an issue that a member must respond in a given timeframe.

5.6.3.1.1. 36 WG/IP will send all DoDCAF 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 DoDCAF informing of a potential issue involving one of the 13 Adjudicative Guidelines.

5.6.3.2.1. The SA will provide 36 WG/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. 36 WG/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. In order 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. DoDCAF will provide all final adjudicative decisions for each issue. If DoDCAF decides to take action 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, 36 WG/IP will forward information to the local SSO to process. The SSO will forward any derogatory information they receive to 36 WG/IP as well.

5.7. **Out-of-scope Investigation Procedures.**

5.7.1. 36 WG/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 JPAS.

5.7.3. Waivers to this policy may be submitted by unit commanders to 36 WG/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 36 WG/CV.

5.8. **Foreign Travel Reporting.** All DoD personnel (Military and Civilian) must report any travel outside of CONUS to the SA prior to going.

5.8.1. The member will first review the Foreign Clearance Guide (FCG) to gather critical information such as general entry requirements, mandatory pre-travel training and documentation, and whether the travel location(s) is in a DoD restricted area.

5.8.1.1. FCG Link: **https://www.fcg.pentagon.mil/fcg.cfm**

5.8.2. Once member has all necessary FCG info, they will notify the SA and complete an AFOSI Det 602 security clearance verification memorandum (Attachment 6), if an in-person briefing is required. SA will email any memorandums to AFOSI Det 602 (**afosi.det602.ops@us.af.mil**).

5.8.2.1. SA will have member complete the Individual Antiterrorism Plan (IATP), Aircraft and Personnel Automated Clearance System (APACS, if required by FCG), and the AFOSI Travel Prebrief located on AF Portal (*Also see Unit Security Manager Guidance for Foreign Travel*).

5.8.2.1.1. IATP Link: **https://iatp.pacom.mil/**

5.8.2.1.2. APACS Link: **https://apacs.milcloud.mil/**

5.8.2.1.3. AFOSI Travel Prebrief Link: **https://www.my.af.mil/gcss-af/USAF/ep/browse.do?programId=tE3494DD050FC730801511C25EA04023F&channelPageId=sA4057E1F3C9BF4E2013CBB496E650A37**

5.8.2.2. Member must ensure a copy of the AFOSI Travel Pre-brief is provided to the SA to determine if a DISS entry is required. ***NOTE****: Official travel does not require a DISS entry.*

5.8.3. Upon return, member will brief SA within 5 duty days, and provide any official or unofficial contacts while in the travel location(s). Member should try to have a contact's first/last name, country of citizenship, and address for any foreign contact.

5.8.3.1. **Official Contacts.** The member's organizational leadership will inform member on when official contacts constitute reporting.

5.8.3.2. **Unofficial Contacts.** Any unofficial contact with a known or suspected foreign intelligence entity and any continuing association with a known foreign national that involves bonds of affection, personal obligation, or intimate contact; or any contact involving the exchange of personal information. ***NOTE****:* If a member makes an unofficial contact while on official travel, they must ensure to report the contact to the SA within 5 days of return. SA will enter information into DISS and add contact info under "Official Trip for Non-DoD Purposes".

5.8.3.2.1. The reporting of limited or casual public contact with foreign nationals is not required (i.e. hotel staff, public conversation with no exchange of personal info, etc.).

5.8.4. SA will have member complete the AFOSI Travel Debrief on the AF Portal.

5.8.4.1. AFOSI Travel Debrief Link: **https://www.my.af.mil/gcss-af/USAF/ep/browse.do?programId=t0ECF2BB8513FA7C701516DCF6DF90288&channelPageId=s330D98A14F55D478014F750C8A3F00FC**

5.8.5. For those cleared members with a DISS entry, the SA will enter the debrief date in DISS which will save the travel information and submit the record as final.

5.8.6. Member will attend an AFOSI in-person pre-brief and debrief, if requested by AFOSI.

5.9. **Interim Security Clearance Procedures.**

5.9.1. 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.*

5.9.1.1. **Minimum requirements for interim Secret eligibility are:**

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

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

5.9.1.1.3. The PSI is showing in "Open" status in JPAS or successor.

5.9.1.2. **Minimum requirements for interim TS eligibility are:**

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

5.9.1.2.2. Favorable completion of a National Agency Check (NAC) (Shown in JPAS).

5.9.1.2.2.1. If member does not have a previous investigation meeting NAC requirement, 36 WG/IP will add the extra investigation code "6" to the Agency Use Block (AUB) of the member's initial TIER 5.

5.9.2. Unit commander and member signs a memo on interim access and forwards to 36 WG/IP.

5.9.3. The SA will grant interim access in JPAS. Once the PSI has been properly adjudicated, JPAS will automatically update from the interim to the proper access.

5.9.4. 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.

5.9.4.1. 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.

5.10. **JPAS/DISS Access Requirements for Unit SAs and USRs.**

5.10.1. Unit SAs and USRs are granted access to JPAS/DISS 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 36 WG/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 JPAS training, Protection of Personal Identifiable Information (PII) training and the Cyber Awareness course. Training links are on the 36 WG/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 (JPAS, DISS or both).

5.10.2. Once all requirements have been met, SA must forward information to 36 WG/IP.

5.10.3. **Unauthorized JPAS/DISS 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 JPAS/DISS for your OWN record or any other record not for official purposes (i.e. celebrities, President, etc.).

5.10.3.2. Providing printouts of JPAS/DISS 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 36 WG/IP SharePoint.

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

5.11. **JPAS Visit Request Procedures.**

5.11.1. The SA is responsible for sending unit personnel visit requests to contractor facilities or locations where security clearance eligibility is required. This will be accomplished by entering a visit request, through JPAS/DISS, to the appropriate Security Management Office (SMO).

5.11.1.1. Personnel who intermittently visit the same facility throughout the year may request the duration of their visit for up to one year.

5.11.2. For units with classified contracts, a visit request will be completed with the sponsoring unit and a copy sent to 36 WG/IP.

5.12. **JPAS Monthly Reports.**

5.12.1. Monthly, the SA will run a personnel report in JPAS/DISS. The SA will verify all unit personnel have proper accesses, eligibility, signed NDA and are properly owned/serviced.

6. INDUSTRIAL SECURITY PROGRAM.

6.1. **Unit Classified Contracts.** The SA will notify 36 WG/IP when defense contractors are assigned to work within their unit that need classified access. Please refer to AFI 16-1406 and this section for guidance.

6.1.1. The SA will ensure each assigned classified contract has the following documentation.

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

6.1.1.2. Signed copy of the Visitor Group Security Agreement (VGSA). The CIP has been delegated the signatory authority for all VGSAs for Andersen AFB.

6.1.1.3. Copy of Contractor's Visit Access Request (VAR) in JPAS. The VAR must be updated annually or when expired.

6.1.1.4. Copy of contract Performance Work Statement and/or Scope of Work.

6.2. **Integrating Classified Contractors.** DoD contractors performing classified contract work and occupying office space at Andersen AFB are designated as visitor groups. The SA will incorporate all authorized classified defense contractors into the unit's IP program.

6.2.1. All integrated contractor personnel must in-process with the SA for clearance verification/validation and records review prior to performing the terms of the contract. Once validated, and access has been granted by the commander, the SA will in-process the contractor as servicing in JPAS and indoctrinate to the level of access required by the contract/position.

6.2.1.1. The SA will ensure contractors are integrated in the unit's initial and annual IP refresher training and make sure the training is documented.

6.2.1.2. 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. See **paragraph 3.5**. for self-inspection procedures.

6.2.1.3. 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.

6.2.1.3.1. Integrated visitor groups must report all security incidents including the loss, compromise or suspected compromise of classified information to 36 WG/IP via the SA.

6.2.1.4. All PSIs for contractors will be handled by the company's Facility Security Officer (FSO). If there are any issues with a contractor's clearance or PSI, contact the FSO to correct.

6.2.2. 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.

6.2.3. The commander will report any adverse issues, within the 13 Adjudicative Guidelines, to the contractor's FSO to have information relayed to DCSA, Personnel Security Management Office for Industry (PSMO-I), DoDCAF and 36 WG/IP. If confirmed the adverse information was relayed by the FSO, no further action is required. If no action is being taken by the FSO, contact 36 WG/IP for further guidance.

6.2.4. The SA will notify 36 WG/IP when contractual services and/or performance has been completed or terminated.

GENTRY W. BOSWELL,
Brigadier General, USAF
Commander

Attachment 1

GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

References

DoDM 5200.01, *DoD Information Security Program, Volumes 1 - 3*

DoDM 5200.02, *Procedures for the DoD Personnel Security Program*

DoD 5220.22-R, *Industrial Security Regulation*

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

AFI 16-1404, *Air Force Information Security Program*

AFMAN 16-1405, *Air Force Personnel Security Program*

AFI 16-1406, *Air Force Industrial Security Program*

Adopted Forms

AF Form 52, *Evidence Tag*

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*

DD Form 254, *DoD Contract Security Classification Specification*

DD Form 1610, *Request and Authorization for TDY Travel of DoD Personnel*

DD Form 1907, *Signature and Tally Record*

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*

Prescribed Forms

None

Abbreviations and Acronyms

AA—Appointing Authority

ACR—Authorization Change Request

ADP—Automated Data Processing

AF—Air Force

AFB—Air Force Base

AFI—Air Force Instruction

AFMAN—Air Force Manual

AFOSI—Air Force Office of Special Investigations

AFRIMS—Air Force Records Information Management System

AFSSI—Air Force Systems Security Instruction

AFTO—Air Force Technical Order

AIS—Automated Information System

ANACI—Access National Agency Check and Inquiries

APACS—Aircraft and Personnel Automated Clearance System

AUB—Agency Use Block

CE—Continuous Evaluation

CEIR—Continuous Evaluation Incident Report

CES—Civil Engineering Squadron

CFR—Code of Federal Regulations

CIK—Crytographic Ignition Key

CIP—Chief, Information Protection

CONUS—Continental United States

CP—Command Post

CPA—Classified Processing Area

CPO—Civilian Personnel Office

CS—Communications Squadron

CSERT—Continuous Security Education Refresher Training

CSL—Cybersecurity Liaison

CUI—Controlled Unclassified Information

DCS—Defense Courier Service

DCSA—Defense Counterintelligence Security Agency

DISA—Defense Information System Agency

DISS—Defense Information System for Security

DNI—Director of National Intelligence

DoD—Department of Defense

DoDCAF—Defense Central Adjudication Facility

DoDM—Department of Defense Manual

EAL—Entry Authority List

EFB—Electronic Flight Bag

EMSEC—Emissions Security

EO—Executive Order

EPRM—Enterprise Protection Risk Management

e-QIP—Electronic Questionnaire for Investigation Processing System

FCG—Foreign Clearance Guide

FOIA—Freedom of Information Act

FSO—Facility Security Officer

GSA—Government Services Administration

GSU—Geographically Separated Unit

IATP—Individual Antiterrorism Plan

IDATP—Integrated Defense Antiterrorism Plan

IDS—Intrusion Detection System

IG—Inspector General

INFOSEC—Information Security

IO—Inquiry Official

IP—Information Protection

IR—Infrared

JPAS—Joint Personnel Adjudication System

JWICS—Joint Worldwide Intelligence Communications System

MOA—Memorandum of Agreement

MOU—Memorandum of Understanding

NAC—National Agency Check

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

NIPRNET—Non-Secure Internet Protocol Router Network

NISPOM—National Industrial Security Program Operating Manual

NSA—National Security Agency

OCA—Original Classification Authority

OF—Optional Form

OPLANS—Operational Plans

OPM—Office of Personnel Management

OSA—Open Storage Area

OVI—Operational Visual Inspection

PDT—Position Designation Tool

PED—Portable Electronic Device

PERSEC—Personnel Security

PII—Personal Identifiable Information

PR—Program Review

PR—Periodic Re-investigation

PSAB—Personnel Security Appeal Board

PSI—Personnel Security Investigation

PSMO-I—Personnel Security Management Office for Industry

RF—Radio Frequency

RFA—Request for Action

SA—Security Assistant

SAC—Special Agreement Check

SAF/AA—Secretary of the Air Force Administrative Assistant

SAP—Special Access Program

SAPF—Special Access Program Facilities

SAR—Security Access Requirement

SAV—Staff Assistance Visit

SCC—Security Container Custodian

SCI—Sensitive Compartmented Information

SCIF—Sensitive Compartmented Information Facility

SEAD—Security Executive Agent Directive

SECAF—Secretary of the Air Force

SF—Standard Form

SFS—Security Forces Squadron

SIPRNET—Secure Internet Protocol Router Network

SIR—Supplemental Information Request

SJA—Staff Judge Advocate

SMO—Security Management Office

SOR—Statement of Reasons

SSBI—Single Scope Background Investigation

SSN—Social Security Number

SSO—Special Security Office

STE—Secure Terminal Equipment

STIG—Security Technical Implementation Guides

SVOIP—Secure Voice Over Internet Protocol

TACLANE—Tactical Local Area Network Encryptor

TDY—Temporary Duty

TS—Top Secret

TSCA—Top Secret Control Account

TSCO—Top Secret Control Officer

UCMJ—Uniform Code of Military Justice

UMD—Unit Manpower Document

USPS—U.S. Postal Service

USR—Unit Security Representative

VAR—Visit Access Request

VGSA—Visitor Group Security Agreement

WCO—Wing Cybersecurity Office

Attachment 2

SA APPOINTMENT LETTER

Figure A2.1. SA Appointment Letter.

DEPARTMENT OF THE AIR FORCE
HEADQUARTERS, 36TH WING (PACAF)
ANDERSEN AIR FORCE BASE, GUAM

DATE

MEMORANDUM FOR 36 WG/IP

FROM: (Unit Commander)

SUBJECT: Security Assistant (SA) Appointment Letter

1. The following members are appointed as SAs for (UNIT) and will be responsible for the Information, Personnel, and Industrial Security Programs for the unit. Program compliance will be in accordance with AFI 16-1404, *Air Force Information Security Management*, AFMAN 16-1405, *Air Force Personnel Security Program*, and AFI 16-1406, *Air Force Industrial Security Program*. These members will also manage and oversee all Controlled Unclassified Information (CUI) for the unit.

POSITION	NAME/RANK	ORG/OFF SYM	PHONE	DEROS
PRIMARY				
ALTERNATE				

2. SAs will provide personnel "Access" in the Joint Personnel Adjudication System (JPAS) or successor system only when the requirements have been met in 36 WG OI 16-1400, para 5.1.1.

3. The following Unit Security Representatives (USR) are required to use JPAS (or successor) in the performance of assigned security related duties trained by the SA above.

LEVEL	NAME/RANK	ORG/OFF SYM	PHONE	DEROS
Level 6 (Gives member full control of System)				
Level 10 (Gives member view and visit actions only)				

4. This memorandum supersedes all previous memorandums, same subject. Please direct questions or comments to (Unit POC), 366-XXXX.

COMMANDER'S SIGNATURE BLOCK

Attachment 3

SECURITY ASSISTANT (SA) TRAINING

Figure A3.1. Security Assistant (SA) Training.

Establishing an account:

- Start with the following web page. https://cdse.usalearning.gov
- Log in if you already have an account.
- If you don't have an account: Click "Create an account" and follow instructions to create.

1. INTRODUCTION TO INFORMATION SECURITY IF011.16
   a. Login and click on "Training" – "Information Security" in header at top of the screen.
   b. Click on "Enroll me" and complete the course.
   c. When completed, click on "Launch Exam" and save your certificate.

2. INTRODUCTION TO PERSONNEL SECURITY PS113.16
   a. Login and click on "Training" – "Personnel Security" in Catalog box in center of screen.
   b. Click on "Enroll me" and complete the course.
   c. When completed, click on "Launch Exam" and save your certificate.

3. INTRODUCTION TO INDUSTRIAL SECURITY IS011.16
   a. Login and click on "Training" – "Industrial Security" in Catalog box in center of screen.
   b. Click on "Enroll me" and complete the course.
   c. When completed, click on "Launch Exam" and save your certificate.

4. DERIVATIVE CLASSIFICATION COURSE IF103.16
   a. Login and click on "Training" – "Information Security" in header at top of the screen.
   b. Click on "Enroll me" and complete the course.
   c. When completed, click on "Launch Exam" and save your certificate.

5. MARKING CLASSIFIED INFORMATION COURSE IF105.16
   a. Login and click on "Training" – "Information Security" in header at top of the screen.
   b. Click on "Enroll me" and complete the course.
   c. When completed, click on "Launch Exam" and save your certificate.

6. STORAGE CONTAINERS AND FACILITIES PY105.06
   a. Login and click on "Training" – "Physical Security" in Catalog box in center of screen.
   b. Click on "Enroll me" and complete the course.
   c. When completed, click on "Launch Exam" and save your certificate.

7. JCAVS USER LEVELS 2-6 PS183.16, (*Required for JPAS Access)
   a. Login and click on "Training" – "Personnel Security" in Catalog box in center of screen.

b. Click on "Enroll me" and complete the course. *Complete the virtual training on the modules labeled (SM). The rest are overview/information only, some of which you will not use. Do not submit RRU's or use JPAS to submit e-QIP Requests.*
c. When completed, click on "Launch Exam" and save your certificate.

8. IDENTIFYING AND SAFEGUARDING PERSONALLY IDENTIFIABLE INFORMATION (PII) DS-IF101.06 (*Required for JPAS/DISS Access)

a. Login and click on "Training" – "Information Security" in header at top of the screen.
b. Click on "Enroll me" and complete the course.
c. When completed, click on "Launch Exam" and save your certificate.

Obtaining Course Completion Certificates:

- On the "Home" page, click on your name at the top right corner of the page.
- Click on "View Profile".
- Under Miscellaneous, click on "My Certificates"
- Click on icon on far right of screen beside the course to print or save the certificate.
- Download to print or save the certificate.
- Certificates from the previous version of STePP may not be available. Please check the "My Transcript" link under your name on the home page for certificates taken previously.

Completing Final 36 WG/SA Certification:

- Update SA Appointment Letter ensuring all required personnel annotated.
- Complete DD Form 2962. Have unit CC fill/sign Part 5.
- Provide a copy of each course certificate listed and a copy of your CYBERAWARNESS certificate with the signed DD FM 2962 to the 36 WG/IP Office.
- Contact 36 WG/IP to schedule a final training appointment.
- Once training is complete, 36 WG/IP will issue a SA Training Certificate.

Attachment 4

SCC APPOINTMENT LETTER

Figure A4.1. SCC Appointment Letter.

DEPARTMENT OF THE AIR FORCE
HEADQUARTERS, 36TH WING (PACAF)
ANDERSEN AIR FORCE BASE, GUAM

DATE

MEMORANDUM FOR 36 WG/IP

FROM: (Unit/CC)

SUBJECT: (UNIT) Appointment of Security Container and/or Open Storage Custodians

1. In accordance with 36 WG OI 16-1400, *Wing Information Protection Program*, each security container and open storage area will have a primary and alternate member identified to maintain oversight of assigned classified storage requirements.

2. The following personnel are responsible for (***enter security container or OSA number***) located at (***enter building and room number***).

POSITION	**NAME/RANK**	**OFF SYM**	**DEROS**	**ACCESS LEVEL**
PRIMARY				
ALTERNATE				

3. *(If you need to identify more than one security container or OSA)* The following personnel are responsible for (***enter security container or OSA number***) located at (***enter building and room number***).

POSITION	**NAME/RANK**	**OFF SYM**	**DEROS**	**ACCESS LEVEL**
PRIMARY				
ALTERNATE				

4. This memorandum supersedes all previous memorandums, same subject. Please direct questions or comments to (Unit POC), 366-XXXX.

COMMANDER'S SIGNATURE BLOCK

Attachment 5

SECURITY CONTAINER CUSTODIAN (SCC) TRAINING

Figure A5.1. Security Container Custodian (SCC) Training.

Establishing an account:

- Start with the following web page. https://cdse.usalearning.gov
- Log in if you already have an account.
- If you don't have an account: Click "Create an account" and follow instructions to create.

1. DERIVATIVE CLASSIFICATION COURSE IF103.16
   a. Login and click on "Training" – "Information Security" in header at top of the screen.
   b. Click on "Enroll me" and complete the course.
   c. When completed, click on "Launch Exam" and save your certificate.

2. MARKING CLASSIFIED INFORMATION COURSE IF105.16
   a. Login and click on "Training" – "Information Security" in header at top of the screen.
   b. Click on "Enroll me" and complete the course.
   c. When completed, click on "Launch Exam" and save your certificate.

3. STORAGE CONTAINERS AND FACILITIES PY105.06
   a. Login and click on "Training" – "Physical Security" in Catalog box in center of screen.
   b. Click on "Enroll me" and complete the course.
   c. When completed, click on "Launch Exam" and save your certificate.

Obtaining Course Completion Certificates:

- On the "Home" page, click on your name at the top right corner of the page.
- Click on "View Profile".
- Under Miscellaneous, click on "My Certificates"
- Click on icon on far right of screen beside the course to print or save the certificate.
- Download to print or save the certificate.
- Certificates from the previous version of STePP may not be available. Please check the "My Transcript" link under your name on the home page for certificates taken previously.