Administrative Change to OO-ALCI16-1401, *Information Protection*

OPR: OO-ALC/OMD

To bring the instruction into compliance with DAFMAN90-161, *Publishing Processes and Procedures*, paragraph 4.5.10.

The publication signature block is hereby changed to:

"RICHARD W. GIBBS, Brigadier General, USAF; Commander, Ogden Air Logistics Complex."

25 JANUARY 2023

BY ORDER OF THE COMMANDER
OGDEN AIR LOGISTICS COMPLEX

OGDEN AIR LOGISTICS COMPLEX
INSTRUCTION 16-1401

19 MARCH 2021
Incorporating Change 1, 13 SEPTEMBER 2022

Operations Support

INFORMATION PROTECTION

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

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

RELEASABILITY: There are no releasability restrictions on this publication

---

OPR: OO-ALC/OMD

Certified by: OO-ALC/OM
(Ms. Yoon M. Hamrick)
Pages: 63

PURPOSE

This instruction implements Air Force Instruction (AFI) 16-1401, Information Protection. It outlines responsibilities and procedures for the Unit Personnel, Industrial, and Information Security Programs and related activities. It applies to individuals assigned to or performing duties within the Ogden Air Logistics Complex (OO-ALC), including Air Force (AF) Reserve, Air National Guard, and contractors when stated in the contract or DD Form 254, Department of Defense Contract Security Classification Specification. This instruction contains material specifically enforced as to military, civilian, and contract personnel. Failure to comply with such material is punishable as a violation of Article 92 of the Uniformed Code of Military Justice, for military personnel; or criminal, civil, and administrative sanctions for civilian and contract personnel. Refer recommended changes and questions about this publication to the Office of Primary Responsibility using the AF Form 847, Recommendation for Change of Publication; route AF Forms 847 from the field through the appropriate functional chain of command. Ensure all records generated as a result of processes prescribed in this publication adhere to AFI 33-322, *Records Management and Information Governance Program*, and are disposed of in accordance with (IAW) the Air Force Records Disposition Schedule which is located in the Air Force Records Information Management System. This publication requires the collection and/or maintenance of information protected by the Privacy Act (PA) of 1974, in accordance with System of Records Notice (F031 AF SP B). PA Systems Notices are available at: **http://www.defenselink.mil/privacy/notices/usaf**. The authorities to collect and/or maintain the records prescribed in this instruction are Title 10 U.S.C., Section 8013; Department of Defense

Instruction 7730.47, *Defense Incident-Based Reporting System (DIBRS)*; and Department of Defense Instruction (DoDI) 5505.17, *Collection, Maintenance, Use and Dissemination of Personally Identifiable Information and Law Enforcement Information by DoD Law Enforcement Activities.*

SUMMARY OF CHANGES

This interim change removes the requirement for a favorable review of local files check originally addressed in **paragraph 3.5.4**, and changes paragraph references to DoDM 5220.22V2_AFMAN16-1406V2_AFMCSUP due to paragraph realignments. It also updates references within the publication and **Attachment 1**, and updates records management statement in opening paragraph.

1. Background/Overview. This instruction provides unit security policies, procedures, and protocols required to meet DoD, AF, and Major Command (MAJCOM) Information Protection requirements. This instruction is applicable to all permanently and temporarily assigned DoD military, civilian, and contractor personnel and where appropriate, assigned foreign national personnel and foreign national visitors. This instruction serves as the unit authoritative source to ensure the protection of classified information, controlled unclassified information (CUI), other sensitive information in support of the unit, MAJCOM, AF, and DoD mission requirements.

2. Safeguarding, Transmission and Transportation of Classified.

2.1. **Purpose.** This section outlines procedures for successful safeguarding, transmission and transportation of classified information. Refer to Department of Defense Manual (DoDM) 5200.01_AFMAN16-1404V1, *Information Security Program: Overview, Classification, and Declassification*; DoDM 5200.01V2_AFMAN16-1404V2, *DoD Information Security Program: Marking of Information*, DoDM 5200.01V3_AFMAN16-1404V3, *DoD Information Security Program: Protection of Classified Information*, AFI 16-1404_ Air Force Materiel Command Supplement (AFMCSUP), *Air Force Information Security Program*, and DoDM 5200.01V1_AFMAN 16-1404V1_AFMCSUP_Hill Air Force Base Supplement (HILLAFBSUP) for additional guidance.

2.2. Safeguarding Classified. Individuals working with classified are personally responsible for its safeguarding while in their possession and will keep classified under constant visual control to prevent inadvertent access by unauthorized personnel.

2.2.1. If the individual needs to leave the area they must return classified to the security container or have a cleared co-worker keep visual contact of the classified until their return. At no time will classified be left unattended.

2.2.2. An authorized person shall keep classified material removed from storage under constant surveillance. Classified document cover sheets: Standard Form (SF) 703, *Top Secret (Coversheet)*, SF 704, *Secret (Cover Sheet)*, or SF 705, *Confidential (Cover Sheet)*, shall be placed on classified documents whenever they are removed from secure storage. The cover sheets indicate the applicable classification level by color and other immediately recognizable format or legend.

2.2.3. At the end of the employee's shift, classified removable hard drives will be removed from computers and returned to the proper storage container.

2.2.4. Uncleared personnel will not be assigned to a work center inside a classified processing area. If an uncleared person is inside a classified area, they will be escorted at all times while in the classified area. Only cleared personnel will be assigned to a classified work area. All cleared personnel must be granted the appropriate clearance eligibility, have a signed a SF 312, *Classified Information Non-Disclosure Agreement* (NDA), access has been annotated in the Joint Personnel Adjudication System (JPAS), Defense Information System for Security (DISS) or the DoD System of Record, and required training is completed.

2.2.5. All visitors to classified areas will be escorted 100 percent of the time. A visitor is considered someone who does not have the need-to-know regarding the classified in that area. If a visitor needs access to any classified, prior arrangements will be made with the shop supervisor and a visit request must be submitted via JPAS, DISS, or the DoD System of Record from the visitor(s) Security Specialist (SS).

2.2.6. The use of government or personal cellular/personal communications system and or radio frequency, infrared wireless devices, and other devices such as cell phone and tablets, and devices that have photographic or audio recording capabilities are prohibited in areas identified for classified processing per AFI 16-1404_AFMCSUP, paragraph 2.7.7.2 and DoDD 8100.02, *Use of Commercial Wireless Devices, Services, and Technologies in the Department of Defense (DoD) Global Information Grid (GIG)*, unless written approval has been received by the authorization official, formerly called designated approving authority. Some examples of prohibited items are cell phones, smart watches, laptops, tablets, ipods, personally wearable fitness devices, wireless headphones, and wireless keyboards/mouse.

2.2.7. Emergency Action Plan (EAP). Plans shall be developed to protect, remove, or destroy classified material in case of fire, natural disaster, civil disturbance, terrorist activities, or enemy action, to minimize the risk of compromise. See unit Classified Processing Area (CPA) operating instruction for the EAP.

2.3. Transmission and Transportation of Classified Material. Persons transmitting or transporting classified information are responsible for ensuring the intended recipients are authorized access, have a need to know, and have the capability to store and properly destroy classified information.

2.3.1. Preparation and Transmission of Classified Information. Refer to DoDM 5200.01V3_AFMAN16-1404, Volume 3, Enclosure 4, for proper methods of preparing and shipping classified information. Each person mailing classified material is responsible for ensuring the material is marked, wrapped, addressed, mailed by authorized means, proper receipts attached, protected, and secured. Consult the SS for assistance.

2.3.2. Escort, Courier, or Hand-Carrying Classified Material. Only authorized and trained personnel will escort, courier, or hand-carry classified material.

2.3.2.1. Hand-Carrying Classified Material on the Installation. If carrying outside a secure facility, material must be double wrapped. A locked briefcase, zippered pouch or an opaque sealed/taped container may serve as the outer wrapper. Classified material shall be packaged in the same manner as prescribed for material being shipped. The office symbol or similar identifying markings along with the highest level of classification will be placed on the inside envelope. If carrying within the same work center/facility, a coversheet will suffice.

2.3.2.2. Personnel carrying classified material will not deviate from their route between departure and arrival points. Stops for unofficial business such as conversations, snacks, and mailbox check, etc., are prohibited.

2.3.2.3. Hand-Carrying Classified Material Off the Installation. Hand carrying of classified material off Hill AFB is only utilized as a last resort in accordance with DoDM 5200.01V3_AFMAN16-1404V3, Enclosure 4, Section 12, paragraph a. Two authorized personnel are required to transport classified material off the installation to always have positive control of the material in case of emergency situations. Personnel must be in possession of a valid DD Form 2501, *Courier Authorization,* or courier authorization memo when carrying classified material off the installation. Prior coordination must be coordinated through and approved by the appropriate authorizing official and Security Manager.

2.3.3. Use of Secure Communications. Classified information shall be transmitted only over secure communications circuits approved for transmission of information at the specified level of classification. This includes communication by telephone, facsimile, e-mail, and other forms of electronic communications (e.g., messages, websites).

3. Personnel Security.

3.1. **Purpose.** This section outlines procedures for successful management of the Unit Personnel Security Program. Refer to DoDI 5200.02, *DoD Personnel Security Program (PSP),* and DoDM 5200.02_AFMAN 16-1405, *Air Force Personnel Security Program*, for additional guidance.

3.2. Unit Manning Document. The commander/director will designate the security sensitivity for manpower positions identified on the Unit Manpower Document (UMD).

3.2.1. The SS will request and receive any updates to the UMD. Supervisors and the SS will review each position on the UMD to ensure position codes accurately reflect the access level required to perform assigned duties. Recommended changes will be forwarded to the commander/director for approval.

3.2.2. The SS will ensure at a minimum the annual review and validation of position attributes within the Manpower Programming and Execution System (MPES) are conducted no later than May 15th. The review must be available during self-inspection, assessment or upon SAF/AAZ requests.

3.3. In-Processing Actions. New unit personnel will meet with the SS for security in-processing prior to receiving squadron badges, access to classified information and classified government systems, and specialized unit security programs. The SS must have an approved/signed DD Form 254 on file prior to processing contractors. Contractors MUST complete in-processing prior to receiving access to ANY communications systems. (See **Attachment 2**, *Sample Unit In-Processing Procedures*, for required in-processing actions).

3.3.1. New personnel will complete Security Indoctrination/Orientation Training, which will be documented via the in-processing checklist and maintained on file by the unit SS or commander's support staff until out-processing. The SS will verify that the new employee completed course MHPSEC9802900BR - Hill Air Force Base (AFB) Information Security (INFOSEC) for Cleared Personnel. This training is a mandatory requirement for all cleared personnel.

3.3.2. New personnel who will access classified information systems such as Secret Internet Protocol Router Network (SIPRNet), and personnel who will have authorized access to North Atlantic Treaty Organization (NATO) classified information, must acknowledge having received a NATO briefing by signing the Briefing/Rebriefing/Debriefing Certificate. This form is available from the Central United States (US) Registry for NATO website: **https://cusrcac.army.mil/Docs/NATOBriefingCertificateElectronicSignature.pdf**.

3.3.3. New personnel with a proper security clearance eligibility, or who will possess a security clearance, will read and sign an NDA. The SS will document the date the NDA was signed in JPAS, DISS or the designated DoD system of record. If able, the NDAs will be uploaded into DISS or the designated DoD system of record and maintained on file. If applicable the NDA will also be forwarded to the AF Personnel Center (military) or the Civilian Personnel Office (civilian).

3.3.4. New personnel will receive additional briefings for appropriate designated access, i.e., SECRET, TOP SECRET, NATO, Restricted Data (RD), Critical Nuclear Weapon Design Information (CNWDI), Nuclear Command Control Extremely Sensitive Information (NC2-ESI) as required.

3.3.5. The SS will establish ownership of new personnel in JPAS, DISS or the DoD system of record and notify the 75 ABW/IPP (Information Protection Personnel Security) or designated security offices to service these individuals under the unit Security Management Office (SMO) code. These relationships will allow the SS and security oversight offices notification of changes in an individual's security clearance eligibility status.

3.3.6. If the new member does not currently possess a security clearance, and does not have an open investigation in JPAS, DISS or the DoD system of record, the SS will contact their designated Civilian Personnel or SS to determine status and initiate the security clearance as required.

3.3.7. If the new member does not currently possess a security clearance, but does have an open investigation in JPAS, DISS or the DoD system of record, the SS will ask for a copy of their Electronic Questionnaire for Investigations (e-QIP) for interim eligibility or other requests as required. The SS will review and file in the designated folder per the unit file plan.

3.3.8. The SS will verify each in-processing member's eligibility level in JPAS, DISS or the DoD system of record. The SS will obtain the commander/director's decision to grant/indoctrinate classified access giving consideration to the Security Access Requirement (SAR) codes on the UMD as well as the Enlisted and Officer Classification Directory requirements. If the person is not eligible for classified access, the commander/director may make interim security access determinations IAW DoDM 5200.02_AFMAN 16-1405, section 7.16.

3.3.9. If Sensitive Compartmented Information (SCI) indoctrination is required, the SS will send a request to the Special Security Officer (SSO) with a memo signed by the commander/director indicating: rank and full name, Social Security Number (SSN), position title, SCI caveats required, work e-mail, duty location, justification, that JPAS, DISS or the DoD system of record reflects Top Secret access, a Point of Contact (POC), and whether the individual resides and works within a Sensitive Compartmented Information Facility (SCIF), frequently works in a local SCIF, or travels to locations requiring SCI access.

3.3.10. The SS will add new personnel to the JPAS, DISS or the DoD system of record personnel roster. The SS will provide the updated roster to the training section, TSS or other record keeping program for continued and up-to-date tracking purposes.

3.4. Nondisclosure Agreement. The SS will check JPAS, DISS or the DoD system of record to ensure personnel have signed an NDA. If a signed NDA is not on file, the SS must brief the member on its purpose and have an NDA signed. Record the NDA on-line through JPAS, DISS or the DoD system of record prior to sending the signed form for retention. When a person refuses to sign an NDA, the SS will:

3.4.1. Deny the individual access to classified information.

3.4.2. Inform the servicing Information Protection Office (IPO) and initiate actions to report/establish a Personnel Security Incident Report.

3.5. Interim Eligibility. Commanders/directors may grant temporary or interim eligibility to classified information for Confidential, Secret and Top Secret access pending final adjudication by the DoD Consolidated Adjudications Facility (CAF). In addition to the requirements listed below, interim Top Secret access requires a previous T3 or equivalent investigation that was favorably adjudicated to be considered for interim Confidential or Secret eligibility:

3.5.1. The member must be a US citizen.

3.5.2. A favorable review of the Federal Bureau of Investigations Criminal History Report (fingerprint results). If fingerprint results are not favorable, the FBI Criminal History Report must be downloaded from the Central Verification System and reviewed by the commander/director.

3.5.3. A favorable review of a completed SF 86, *Questionnaire for National Security Positions*, e-QIP worksheet.

3.5.4. Delete.

3.5.5. An appropriate national security investigation opened by the investigative service provider.

3.5.6. Interim eligibility will be documented in memorandum format that includes the justification for why the interim is needed.

3.5.7. Interim eligibility may be revoked at any time based on unfavorable information in the investigation process. If revoked, contact 75 ABW/IPP or designated IPO.

3.5.8. Interim eligibility is valid for up to 1 year without an extension. A 6-month extension can be granted based on specific conditions listed in DoDM 5200.02_AFMAN 16-1405.

3.5.9. Interim eligibility documentation granted by the commander/director must be kept on file with the SS until the final clearance has been adjudicated.

3.6. Security Executive Agent Directive (SEAD) 3 Reporting and Continuous Evaluation (CE). CE is the review of an individual's background to determine whether they continue to meet national security eligibility requirements. The commander/director and supervisors will continuously evaluate cleared personnel to ensure they continue to be trustworthy in accordance with the standards in SEAD 3.

3.6.1. The SS, supervisors and all cleared personnel will immediately notify unit leadership when unfavorable information is revealed which could have a direct impact upon an individual's security clearance and/or eligibility. The commander/director is responsible to review, evaluate, and consider any and all disqualifying factors and take appropriate action.

3.6.2. All unit personnel with secret eligibility or higher are obligated to immediately self-report adverse information to the SS that may affect their eligibility. In addition, all unit personnel are required to report any information on behavior or conditions that may pose a security concern, or that raise doubts about an eligible co-worker's continued access to classified information when they become aware of it. Examples include, but are not limited to:

3.6.2.1. Illegal drug involvement or use.

3.6.2.2. Misuse or abuse of alcohol.

3.6.2.3. Driving under the influence.

3.6.2.4. Bankruptcy.

3.6.2.5. Financial difficulties to include late payments of 120 days or more.

3.6.2.6. Wage garnishments.

3.6.2.7. Significant moving violations.

3.6.2.8. Any arrests, even if not formally charged.

3.6.2.9. Security violations to include misuse of information systems.

3.6.2.10. Emotional, mental, and personality disorders.

3.6.2.11. Foreign travel/foreign contacts.

3.6.3. The SS will prepare a CE report and forward it to the designated Information Protection (IP) or Security Oversight Office for submission to the DoD Validation Cell. An AF Form 2587, *Security Termination Statement*, will be prepared by the SS when access is temporarily withdrawn and/or revoked.

3.7. Foreign Travel. Unit personnel traveling to a foreign country, whether for official or unofficial travel, will notify their supervisor, the unit antiterrorism representative (ATR), and/or the SS no later than 30 days prior to travel or if less than 30 days immediately upon notification to meet mandated OCONUS travel requirements.

3.7.1. Unit personnel will complete the following antiterrorism requirements:

3.7.1.1. Review US State Department travel advisories and requirements for the country to be visited at: travel.state.gov.

3.7.1.2. Review DoD Foreign Clearance Guide entry and travel requirements for the country to be visited at: **https://www.fcg.pentagon.mil/**.

3.7.1.3. Complete Air Force Office of Special Investigations (AFOSI) Foreign Travel training: **https://www.my.af.mil/gcss-af/USAF/AFP40/d/s88B4F00B2D70DF4E012DBE0975FE0BAB/Files/AFOSI_Foreign_Travel_Training_v2.pdf**.

3.7.1.4. Per the AFOSI Foreign Travel training, schedule a face-to-face appointment with local AFOSI Detachment 113 for country pre-briefing: call 775-6017 or 777-1852 or email: **afosi.113ci@us.af.mil**. AFOSI will contact personnel to set up a face-to-face briefing no earlier than 2 weeks prior to departure based on destination. Not all foreign travel requires an in-person briefing.

3.7.1.5. As required, complete Antiterrorism Level 1 training in the Advanced Distributed Learning Service (ADLS): **https://golearn.adls.af.mil/**.

3.7.1.6. As required, submit country clearance for Aircraft and Personnel Automated Clearance System (APACS) approval: **https://apacs.dtic.mil/apacs/login.jsp**.

3.7.1.7. For high risk/identified countries, submit documentation to obtain travel approval from the first O-6 in the individual's chain of command.

3.7.2. Prior to departure, unit personnel will email the ATR and/or the SS the following pre-travel reporting information for each visit:

3.7.2.1. Complete itinerary.

3.7.2.2. Dates of travel.

3.7.2.3. Mode of transportation and identity of carriers.

3.7.2.4. Passport number and issuing location/date.

3.7.2.5. Names and association (business, friend, relative, etc.) of foreign national traveling companions, if applicable.

3.7.2.6. Name, address, telephone number, and relationship of emergency point of contact.

3.7.2.7. Planned contact with foreign governments, companies, or citizens during foreign travel and reason for contact.

3.7.3. If emergency circumstances exist, at a minimum unit personnel will verbally advise their supervisor, ATR and/or the SS of all pertinent travel specifics prior to departure. Full reporting shall be accomplished within 5 business days of return.

3.7.4. Upon return, unit personnel will inform their supervisor/SS and complete post-travel reporting requirements via the SF-86C, *Standard Form 86 Certification*, to include the following:

3.7.4.1. Unplanned contacts with foreign governments, companies, or citizens during foreign travel and the reason for contact.

3.7.4.2. Unusual or suspicious occurrences during travel, including those of possible security or counterintelligence significance.

3.7.4.3. Any foreign legal or customs incidents encountered.

3.7.5. As required, schedule a face-to-face debriefing with the local AFOSI Detachment 113. Call 775-6017 or 777-1852 or email: **afosi.113ci@us.af.mil**.

3.7.6. The SS will document personnel foreign travel in the DISS or the DoD system of record, under the employee's "Subject Details" on the "Foreign Travel" tab.

3.8. Personnel Security Investigations. Clearances for unit personnel will be tracked by JPAS, DISS or the DoD system of record, which is the system of record and final authority on the status of all investigations, adjudications, and a person's eligibility for access.

3.8.1. Initial Investigations.

3.8.1.1. These investigations are initiated only when a necessity exists for an investigation action such as an eligibility upgrade required by the specific career field, UMD SAR code, or by permanent change of station (PCS)/retraining orders, or when an uncleared person is assigned to the unit.

3.8.1.2. Investigations Initiated Due to Eligibility Upgrade Requirement. If a member's career field requires an eligibility upgrade and there is official justification, an upgrade investigation will be initiated as soon as possible by the SS.

3.8.1.3. Investigations Initiated by PCS and/or Retraining Orders. The 75th Force Support Squadron (75 FSS) requires a locally generated security memorandum (formerly Form-08), to confirm clearance requirements or a required investigation has been completed or opened in JPAS, DISS or the DoD system of record before processing orders. Upon receipt from 75 FSS, the unit member must provide their security memorandum and assignment Report on Individual Personnel (RIP) to the SS. After validation, the SS will complete the form, sign, and return to the member who will submit it to 75 FSS for assignment processing. For assignments requiring SCI access/eligibility, the SS will work with the designated SSO.

3.8.2. Periodic Reinvestigations.

3.8.2.1. Periodic Reinvestigations can be submitted to 75 ABW/IPP up to 3 months before the respective anniversary date of the close date of the last investigation. Anniversary dates are 10 years for Secret clearances and 6 years for Top Secret clearances and 5 years for Special Access Programs (SAP). Reinvestigations will not be completed for members with less than 12 months of retainability. However, the commander/director can grant continued access for military or civilian personnel with less than 12 months retainability consistent with accomplishing the unit mission.

3.8.3. Investigations Process. The SS will utilize DoDM 5200.02_AFMAN 16-1405, related DoD and AF-issued policy, and this instruction to ensure the investigation process is accurate and timely. The unit investigation process is as follows:

3.8.3.1. Justification. Official justification is required for Secret or higher investigations. Provide official justification from the UMD, assignment notification, Officer or Enlisted Classification Directory, or other documentation approved by 75 ABW/IPP. Justification will be e-mailed to 75 ABW/IPP or designated IPO by the SS at the same time the SF 86 is released to the approver in the e-QIP system.

3.8.3.2. Electronic Questionnaires for Investigations Processing. Initiate e-QIP access for unit personnel. Notify personnel via e-mail stating e-QIP access has been initiated along with their personal registration code. Due to the Personally Identifiable Information (PII) that can be accessed using this registration code, the e-mail must be Controlled Unclassified Information (CUI)/PII-encrypted or the registration code can be provided in person.

3.8.3.3. 30-day Suspense. Unit personnel must log-into the online e-QIP within 30 days of it being initiated. Once the subject has logged into their e-QIP they will have an additional 90 days to complete it and provide a review copy to the SS. Personnel requiring more than 30 days to log onto e-QIP must request an extension from the SS; extensions will be reviewed and granted by the SS on a case-by-case basis. A member's failure to complete their SF 86 may result in termination of access to classified information, revocation of systems access, or establishment of a personnel security incident report with the DoD CAF by the commander/director.

3.8.3.4. SS Review. The SS will review the SF 86 for errors and applicants will make corrections as necessary.

3.8.3.5. Release to SS. When the SS gives final approval, unit personnel will certify their SF 86 and release it to the SS in e-QIP. NOTE: It is recommended that unit personnel save an archival copy of the SF 86 for their personal records.

3.8.3.6. Release to Approver. The SS will save an archival copy of the member's SF 86, verify that all signature pages have been signed, and release the SF 86 to the approver/designated IPO. For Top Secret, include official justification in the e-mail.

3.8.4. Fingerprint Requirements. Fingerprints are required when receiving an initial T1, T3, or T5 Personnel Security Investigation, as well as when an employee is being upgraded to a T3 or T5 security clearance. New civilian hire fingerprinting is conducted by the 75 FSS Civilian Personnel Section at building 430. Fingerprinting for military and civilian personnel upgrades is conducted by the 75 ABW/IPP office at building 1102 or per additional instructions. Fingerprinting for contractors requiring a clearance will be performed within a contractor specified facility.

3.9. Out-processing Actions. Personnel leaving the unit will out-process with the SS and turn in all issued security-related items (i.e., restricted area badges, vindicator card, SIPRNet token, etc.) Photo badges will be shredded. SIPR tokens will be turned back in to the base issuing office. The member will take both the Restricted Area Badge (RAB) and the AF Form 2586, *Unescorted Entry Authorization Certificate*, to Security Forces Pass & ID. The RAB will be turned into security forces and the AF Form 2586 will be signed off via security forces. The signed AF Form 2586 will then be returned to unit SS. Unit issued vindicator cards, keys, or security-related items will be returned to the unit issuing/sensitive item authority. Additionally, contractors will turn in their Common Access Card (CAC) to the contractor representative or SS. (See **Attachment 3**, *Sample Unit Personnel Out-Processing Procedures*, for required out-processing actions).

3.9.1. The SS will review the unit member's JPAS, DISS or the DoD system of record profile, and debrief the member of all collateral access requirements (i.e., Secret, Top Secret, NATO, RD, CNWDI, NC2-ESI, etc).

3.9.2. The SS will notify 75 ABW/IPP or designated IPO with names and SSNs of out-processing personnel so that their servicing relationship can be terminated.

3.9.3. As applicable, out-processing personnel will read, sign, and date the AF Form 2587. Both the SS and employee must sign these forms. Signed copies of the AF Form 2587 must be maintained and destroyed by the SS according to AFRIMS disposition instructions.

3.9.4. If the employee is currently briefed into SAP or SCI, the Government SAP Security Officer and/or SSO will debrief prior to the employee being debriefed of all collateral access.

3.9.5. If an SCI debrief or transfer-in-status (TIS) is required, the SS will send a request to the designated SSO with the member's name and SSN. The SSO will coordinate with the appropriate offices to debrief personnel or accept a TIS.

3.10. Security Termination & Debriefing. The SS will obtain the commander/director's decision to terminate classified access based on separation or retirement, PCS or temporary duty, and temporary duty assignments, no longer require access, have their access suspended, or have their clearance revoked or denied The SS will conduct and document the security termination debriefings, as follows.

3.10.1. Debrief individuals having access to classified information or security clearance eligibility.

3.10.2. An AF Form 2587 will be used to document the debriefing.

3.10.3. The debriefing must emphasize to individuals their continued responsibility to:

3.10.3.1. Protect classified and CUI to which they had access.

3.10.3.2. Report any unauthorized attempts to gain access to such information.

3.10.3.3. Adhere to the prohibition against retaining material upon departure.

3.10.3.4. Potential civil and criminal penalties for failure to fulfill their continuing security responsibilities.

3.10.4. Update JPAS, DISS or the DoD System of Record to reflect termination of accesses under the debrief link.

3.10.5. Retain the AF Form 2587 for 2 years from the date of signature and destroy according to AFRIMS record disposition.

3.10.6. Refusal to Sign a Termination Statement. When an individual willfully refuses to execute AF Form 2587, the supervisor, in the presence of a witness, will:

3.10.6.1. Debrief the individual orally.

3.10.6.2. Generate a MFR indicating the fact that the individual refused to execute the termination statement and was orally debriefed with signatures of both the SS and a witness.

3.10.6.3. Remove the individual's access to classified information.

3.10.6.4. Contact the servicing IPO for mandatory Personnel Security Incident Report processing according to DoDM 5200.02_AFMAN 16-1405.

4. Industrial Security.

4.1. **Purpose.** This section outlines procedures for successful management of the Unit Industrial Security Program. Refer to DoDM 5220.22_AFMAN 16-1406, Volume 2, *National Industrial Security Program: Industrial Security Procedures For Government Activities,* and DoDM 5220.22V2_AFMAN16-1406V2_AFMCSUP, for additional guidance.

4.2. Drafting the DD Form 254.

4.2.1. The contracting officer representative (COR) or designees will utilize the DD Form 254 Handbook available on the 75 ABW/IP SharePoint at: **https://org2.eis.af.mil/sites/21341/IP/IndustrialSecurity/DD%20Form%20254/Forms/AllItems.aspx**, when drafting the DD Form 254.

4.2.2. The contracting officer representative or designees will draft the initial DD Form 254, using the Procurement Integrated Enterprise Environment (PIEE) system, then route to the SS through the PIEE system for a review prior to further coordination. The SS will perform a review of the DD Form 254 to verify what access will be required and security requirements for classified contracts. The SS will identify any discrepancies or security corrections required and return the DD Form 254 to the COR, program/project manager for corrections. The COR, program/project manager or designee will implement all required changes prior to returning the draft to the SS using the PIEE system for final review. After a final favorable SS review, the designated SS will sign the DD Form 254 within the PIEE system generating an automatic forward to the next reviewer in the PIEE system for review/coordination. This process will continue until all reviewers in Item 13 of the DD Form 254 have reviewed and signed the DD Form 254. Once all reviewers/coordinators identified in Item 13 have signed, the PIEE system will route the DD Form 254 back to the COR for final review and signature by the contracting representative. The SS will receive a copy of the completed DD Form 254 for filing and reference for the duration of the contract.

4.2.3. The contracting officer representative, program/project managers or designee and SSs will obtain and maintain access to the National Industrial Security System (NISS) in order to verify the facility clearance and safeguarding level (if performance will be at the contractor's facility versus a government location) for all contractor locations identified in Items 6 and 8 of the DD Form 254. Contracting officers and/or representatives will maintain sponsorship capability for contractors who require facility clearance and safeguarding sponsorship submittals or upgrades. Instructions for establishing a National Industrial Security Program Contracts Classification System account and NISS access may be found on the 75 ABW/IP SharePoint at: **https://org2.eis.af.mil/sites/21341/IP/IndustrialSecurity/DD%20Form%20254/Forms/AllItems.aspx**.

4.2.4. Once signed/certified by a contracting officer, the signed/certified DD Form 254 will be sent to all cognizant security offices identified within Items 6, 8 and 18 of the DD Form 254.

4.2.5. All DD Forms 254 and applicable Security Classification Guides (SCG) identified within the form will be reviewed annually to ensure accuracy and currency. When changes are necessary, the DD Form 254 must be modified and a revision issued IAW the DD Form 254 handbook available on the 75 ABW/IP SharePoint at: **https://org2.eis.af.mil/sites/21341/IP/IndustrialSecurity/DD%20Form%20254/Forms/AllItems.aspx**.

4.3. Visitor Group Security Addendum (VGSA).

4.3.1. Contract performance located on military installations identified within Item 8 of an awarded DD Form 254 require the contractor, IAW AF Federal Acquisition Regulation Supplement 5352.204-9000, to enter into a VGSA with the installation commander, for those respective installations. On Hill AFB, contract personnel will not be allowed to in-process or receive a CAC until the SS and the 75 ABW/IPD office have received copies of a signed/certified DD Form 254 and fully signed VGSA identifying the security requirements unique to Hill AFB.

4.3.2. Once the SS receives a signed/certified and awarded DD Form 254, they will assist the contracting officer/program/project managers or designee in the completion of the VGSA. Templates for the VGSAs may be found on the 75 ABW/IP SharePoint at: **https://org2.eis.af.mil/sites/21341/IP/IndustrialSecurity/VGSAs/Forms/AllItems.aspx**.

4.3.3. To identify which type of VGSA (integrated or independent) either look in Item 13, reference 11.m of the DD Form 254 or use the following general guidelines:

4.3.3.1. Intermittent Visitors. In accordance with DoDM5220.22V2_AFMAN16-1406V2_AFMCSUP, paragraph 3.8a(4), if a contractor employee/employees will work less than 90 days consecutively on the installation, the contractor company/employees are considered intermittent visitors. Intermittent visitors will send a visit access request (VAR) through JPAS, DISS or the DoD system of record to the unit/s they support, which will be verified against the requirements of the contractor's DD Form 254.

4.3.3.2. Integrated VGSA. Used when a contractor will **NOT** store classified separately from the AF unit they support (they access classified from security containers, secure rooms, etc., under the unit's control). The vast majority of contracts on Hill AFB are integrated.

4.3.3.3. Independent VGSA. Used when a contractor will store classified separately from the AF unit they support (the security containers, secure rooms, etc., are under the control of the contractor).

4.3.4. To complete the VGSA, fill in the contractor's complete company name within the applicable yellow highlighted areas, as the company name appears within NISS. If the company will operate as an independent visitor group, fill in the applicable yellow highlighted areas showing where the storage of classified will occur by building and room number. Once the company's information has been added, and for independent visitor groups where storage will occur, ensure the signature blocks on the VGSA for the Facility Security Officer (FSO) and on-base official (usually a supervisor from the contract company working on base) are filled in on page 9 and the SS and contracting officer/program/project managers or designee signature blocks are completed on page 10 (it is beneficial to get the individuals names and titles, fill in the signature blocks; once done convert the document to PDF format and send to all for signature). Once you have the FSO's, on-base officials', program manager's and SS's signatures, send to 75 ABW/IPD. 75 ABW/IPD will sign and distribute to all VGSA signatories.

4.3.5. Subcontractors who work with their prime contractors (integrated or independent VGs) may simply sign a "Subcontractor Agreement Certification" whereby they agree to abide by the prime's VGSA. A "Subcontract Agreement Certification" may be found at: **https://org2.eis.af.mil/sites/21341/IP/IndustrialSecurity/VGSAs/Forms/AllItems.aspx** . However, if the subcontractor is operating alone on the installation without a prime contractor present, the subcontractor will need to complete their own integrated or independent VGSA.

4.4. Contractor Training. Contractors are required to receive initial and annual refresher training for cleared personnel meeting the requirements of DoD 5220.22-M, *National Industrial Security Program Operating Manual* (NISPOM) 5220.22-M, paragraphs 3-107 and 3-108. How these training requirements are met depends on how they operate on the installation. The following are the requirements for the different categories operating on Hill AFB:

4.4.1. Integrated VGSA. In accordance with DoDM5220.22V2_AFMAN16-1406V2_AFMCSUP, paragraph 3.8.a.(4a).2 (Added)(AFMC), integrated visitor group contractor personnel are required to complete all applicable security training mandated by contract and follow local security procedures. The unit security assistant will ensure the COR is provided all training requirements for integrated visitor group contractor personnel. This requirement is already captured in the draft integrated VGSA template, paragraph h (2), available on the 75 ABW/IP SharePoint.

4.4.2. Independent VGSA. DoDM5220.22V2_AFMAN16-1406V2_AFMCSUP, paragraph 3.8.a.(4b) (Added)(AF), operate independently from an on-base Air Force activity. In these cases, the contractor employees operate independently from day-to-day oversight by Air Force employees and typically have a separately assigned space for which they are responsible as described in memoranda of agreement, support agreements, etc. Further, contractors are normally only categorized this way when their contract requires them to store classified information and they do so separately from other Air Force operations. Contractors who operate as an independent visitor group remain subject to this volume and DoDM5200.01V3_AFMAN16-1404V3 and must identify an on-site security point of contact to the Information Protection Office as required by contract. The security point of contact will ensure the required security responsibilities of the contractor are performed. If the contractor intends on doing this by bringing a corporate network/information system onto the installation, then the contractor must receive approval for the information system from 75 ABW/SC. The system must be identified in the independent visitor group's security agreement, which will need to be signed by 75 ABW/SC following attestation/proof the contractor meets all DFARS Subpart 252.204-7012, NIST 800-171 requirements.

4.5. **Contractor Access.** The level of access to classified information and to unclassified and classified network systems granted to contractors is determined by the Performance Work Statement (PWS), Statement of Work (SOW), or the Statement of Objective and/or the signed DD Form 254 (identified within Items 1.a, 1.b, 9 and 10) associated with the contract.

4.6. Contractor Personnel Security Investigations. Contractors requiring a CAC will need to have a minimum of a T1 investigation initiated and a current favorable fingerprint report on file. Contractor T1 investigations will be initiated by the SS. Contractor T3/T5 investigations will be initiated by the contractor FSO for contract performance where a DD Form 254 has been issued. However, T3/T5 investigation requirements falling outside of the National Industrial Security Program (i.e., positions of trust and unclassified information systems administrator access [IT Levels/IT I/II System Administrator]) are the responsibility of the government contracting activity and will be initiated by the SS.

4.7. Servicing Contractors.

4.7.1. JPAS, DISS or the DoD system of record will be used to verify the security clearance level on all contractor personnel requiring access to classified information. Integrated/independent visitor group contractor personnel will be serviced in JPAS, DISS and/or the DoD system of record. The SS will also notify the 75 ABW/IPP office or designated IPO, so they may service the contractor personnel in JPAS, DISS or the DoD system of record as well.

4.7.2. Visitor group personnel performing on a contract will be unserviced once the contract is terminated, or when the SS receives notification from the FSO, program/project managers or designee or the COR that a contractor is no longer employed by their organization. The visitor group FSO is responsible for maintaining the records of their visitor group employees in JPAS, DISS or the DoD system of record and ensuring the organization has an updated VAR in JPAS, DISS or the DoD system of record, or by letter (Visit Access List [VAL]), at all times to reflect any newly hired employees or when an employee leaves the installation for another assignment, retires or terminates from the contract.

4.7.3. The SS will notify 75 ABW/IPP once the contractor out-processes or is no longer employed by the contractor organization. 75 ABW/IPP will then out-process the employee.

4.7.4. The SS, program/project manager (or designee) and COR (if appointed) must ensure all contractor personnel return government access credentials and property when terminating and will notify the contracting officer when contractor employees fail to return these items.

4.7.5. Program/project manager and SS are required to notify 75 ABW/IPD when a contract has terminated.

4.8. Contractor Security Incidents. Security incidents involving contractors are processed based on the following categories:

4.8.1. On Base-Cleared Facility Contractors. Cleared contractor facilities located on Hill AFB will report security incidents directly to the 75 ABW/IP office. These incidents are processed between the FSO and 75 ABW/IP as the Servicing Security Agency. The contractor will complete an initial and final report in accordance with NISPOM 5220.22-M, paragraph 1-303. If compromise has occurred, 75 ABW/IP will contact the SS and program/project manager (or designee) to notify the Original Classification Authority (OCA) with responsibility for the compromised information and to obtain a damage assessment.

4.8.2. Integrated/Independent Visitor Group Contractors. Security incidents initiated by integrated/independent contractors located on Hill AFB will report directly to the SS. The SS will report the incident to the 75 ABW/IPI office, then follow the unit security incident process in accordance with AFI 16-1404_AFMCSUP, Chapter 7. Units will use the guidance provided in the Hill AFB Information Security Incident Handbook found at: **https://org2.eis.af.mil/sites/21341/IP/InformationSecurity/Handbooks/Forms/AllItems.aspx**.

4.9. Contractor Inspections. Contractor inspections on Hill AFB must be completed in the following manner:

4.9.1. On Base-Cleared Facility Contractors. In accordance with DoDM5220.22V2_AFMAN16-1406V2_AFMCSUP, paragraph, 14.1.c, 75 ABW/IPD will conduct annual Industrial Security Reviews on on-base cleared contractors. Upon completion of security reviews of on-installation cleared facilities, the servicing IP office with security oversight responsibility will send a copy of the report to DCSA via encrypted email at **dcsa.quantico.dcsa.mbx.ctpoperations@mail.mil** (or successor email) and copy the HQ AFMC/IP Industrial Security Program Manager, or designee. The HQ AFMC/IP Industrial Security Program Manager, or designee, will maintain up-to-date information security reviews for on-installation cleared facilities in the SAF/AAZ designated repository. (T-2).

4.9.2. Integrated Visitor Group Contractors. In accordance with DoDM5220.22V2_AFMAN16-1406V2_AFMCSUP, paragraph, 14.1.f, installation commanders will include contractor integrated visitor groups within their self-inspection programs in accordance with AFI 16-1404.

4.9.3. Independent Visitor Group Contractors. In accordance with DoDM5220.22V2_AFMAN16-1406V2_AFMCSUP, paragraph, 14.1.f, 75 ABW/IPD and other security relevant program areas (e.g., Cybersecurity squadron, AFOSI) will evaluate independent visitor groups separate from their government sponsor. Evaluation criteria will be based upon requirements identified in DoDM5220.01V3_AFMAN16-1404V3 and local security policy communicated to the contractor. Information Protection Offices and other security relevant program areas will evaluate independent visitor groups not to exceed 24 months. Contracting officers will ensure a requirement for contractors to support these activities is included in appropriate contracts.

4.10. **Contractor Folders.** In accordance with DoDM5220.22V2_AFMAN16-1406_AFMCSUP, paragraphs 3.8.a.(4).(a) (AFMC), 75 ABW/IPD and unit SS will maintain a file folder, electronic or hard copy, on all integrated visitor groups that will contain a copy of the applicable DD Form 254 (prime and subcontractor, as applicable), communication of how the local security procedures were sent to the contractor (if not included as part of the DD Form 254), documentation of non-compliance with local security procedures (if applicable), copies of all consultant documentation, if applicable to the unit, and a copy of the last unit self-assessment, IAW paragraph 14.1.f of this manual, that included integrated visitor group operations.

4.10.1. Delete.

4.10.2. Delete.

4.10.3. Delete.

4.10.4. Delete.

4.10.5. Delete.

4.10.6. Delete.

4.11. Industrial Security for Unclassified Contracts.

4.11.1. Contractors shall comply with the contract requirements, SOW and PWS.

4.11.2. Contractors requiring access to the installation will complete a Hill AFB Form 496, *Application for Installation Access Control* and forward to the COR. If approved, the COR will notify the contractor(s) and provide location to obtain a Defense Biometric Identification System (DBIDS) access card. The COR or contractor supervisor will escort the new contractor(s) to obtain DBIDS if they do not have initial access to the installation.

4.11.3. If Security Forces deny access to the installation, due to derogatory information obtained in the local file background check, the contractor will surrender all issued credentials/passes and be removed from the installation immediately. Upon request, Security Forces will provide an appeal process to a contractor if denial of access is questioned. A final determination for access is made by the 75th Air Base Wing Commander.

4.11.4. Contractors requiring access to Information Technology (IT) systems and the need for a government CAC will meet the following requirements:

4.11.4.1. A verified, successfully submitted and opened background investigation to the Defense Counterintelligence Security Agency and verified through JPAS, DISS or the DoD system of record.

4.11.4.2. Those without a verifiable investigation will require the following:

4.11.4.2.1. Complete investigative questionnaire via the e-QIP (**https://nbib.opm.gov/e-qip-background-investigations/**) within 2 weeks of initiation. Once complete, a 100 percent review will be conducted by the initiator prior to submitting the investigation to 75 ABW/IPP via e-mail.

4.11.4.2.2. Create a JPAS, DISS, or the DoD system of record, Person Category for the newly hired contractor using the "Instructions on adding a contractor in JPAS, DISS or the DoD System of Record" located on the 75 ABW/IPP SharePoint at: **https://org2.eis.af.mil/sites/21341/IP/PersonnelSecurity/JPAS/Forms/AllItems.aspx**. Notify 75 ABW/IPP to "service" the employee under the correct SMO code.

4.11.4.2.3. A completed Optional Form 306, *Declaration for Federal Employment.*

4.11.4.2.4. Submission of fingerprints verified through JPAS, DISS or the DoD system of record with favorable results. If derogatory prints are returned, a local determination may be conducted by a certified government representative who has been appointed by the commander/director and completed "Introduction to DoD HSPD-12 CAC Credentialing" course (PS112.16 in Security Training, Education, and Professionalization Portal [STEPP]). If an unfavorable determination is made, then no CAC card will be issued and the contracting officer/COR will be notified of an unfavorable determination and any necessary administrative actions.

4.11.4.2.4.1. Fingerprints will be coordinated by the security specialist. The employee must have a JPAS, DISS or DoD system of record account established under the correct SMO and show they are owned by the requesting organization.

4.11.4.2.5. Reciprocity of prior background check or security clearance. Contractors with a favorable background check, or security clearance, within 2 years of leaving military, civilian or contractor service may be issued a CAC by an authorized Trusted Agent through the Trusted Associate Sponsorship System.

4.11.4.2.5.1. Contractors not meeting reciprocity or without a current background check/clearance will be submitted for a new Tier 1 (T1) investigation through the organization security office and NP2 Portal: **https://np2.opm.gov/webcenter/portal/NP2**. The contractor must meet all requirements to submit a new investigation, complete new fingerprints and any required training.

5. Controlled Unclassified Information.

5.1. Purpose. This section outlines procedures for successful management of CUI. All unit personnel are responsible for properly protecting sensitive unclassified information (i.e., FOUO, Privacy Act, Unclassified Nuclear Information) also known as CUI. Refer to DoDI 5200.48, *Controlled Unclassified Information*, for additional guidance.

5.2. CUI Overview. Unlike classified information, individuals and organizations generally do not need to demonstrate a need-to-know to access CUI unless specifically required by law or policy. However, due to CUI's sensitive nature; access is based on a lawful governmental purpose. To ensure proper access and use, CUI has additional protective and safeguarding measures to include training, handling, marking, dissemination, decontrolling, and destruction among others.

5.3. CUI Training. All personnel in the organization, including DoD civilians, military members and on-site support contractors with access to CUI, shall receive an initial orientation and annual refresher training that reinforces the policies, principles, and procedures.

5.3.1. CUI refresher training shall also address the threat and the techniques foreign intelligence activities use while attempting to obtain DoD CUI, the importance of unclassified information, its potential sensitivity, and the requirement to have all information reviewed and approved for release prior to public disclosure or Web posting. In addition, unit CUI refresher training will also cover the penalties for unauthorized disclosure.

5.4. Handling Requirements. The authorized holder of a document or material is responsible for determining, at the time of creation, whether the information falls into a CUI category. If so, the authorized holder is responsible for applying CUI markings and dissemination instructions accordingly.

5.5. Marking Requirements.

5.5.1. At a minimum, CUI markings for unclassified DoD documents will include the acronym "CUI" in the banner and footer of the document.

5.5.2. If portion markings are selected, then all document subjects and titles, as well as individual sections, parts, paragraphs, or similar portions of a CUI document known to contain CUI, will be portion marked with "(CUI)." Use of the unclassified marking "(U)" as a portion marking for unclassified information within CUI documents or materials is required.

5.5.2.1. There is no requirement to add the "U", signifying unclassified, to the banner and footer as was required with the old FOUO marking (i.e., U//FOUO).

5.5.2.2. Banners, footers, and portion marking will only be marked "Unclassified" or "(U)" for unclassified information in accordance with the June 4, 2019 Information Security Oversight Office letter. If the document also contains CUI, it will be marked in accordance with **paragraph 3.4**a. and additional forthcoming guidance.

5.5.2.3. CUI markings in classified documents will appear in paragraphs or subparagraphs known to contain only CUI and must be portion marked with "(CUI)." "CUI" will not appear in the banner or footer.

5.5.2.4. All classified documents, including legacy documents will be reviewed for CUI and properly marked upon changes in the document's classification level, particularly if the documents are to be completely declassified.

5.5.3. The first page or cover of any document or material containing CUI, including a document with commingled classified information, will include a CUI designation indicator. Documents and materials containing CUI will require a generic "CUI" marking at the top and bottom of each page.

5.5.3.1. The CUI designation indicator must contain, at minimum, the name of the DoD component determining that the information is CUI. If letterhead or another standard indicator of origination is used, this line may be omitted.

5.5.3.2. The second line must identify the office making the determination.

5.5.3.3. The third line must identify all types of CUI contained in the document.

5.5.3.4. The fourth line must contain the distribution statement or the dissemination controls applicable to the document.

5.5.3.5. The fifth line must contain the phone number or office mailbox for the originating DoD component or authorized CUI holder.

5.5.4. Legacy Information Requirements. DoD legacy information does not automatically become CUI. It must be reviewed by the owner of the information to determine if it meets the CUI requirements. DoD legacy material will not be required to be re-marked or redacted while it remains under DoD control or is accessed online and downloaded for use within the DoD. However, any such document or new derivative document must be marked as CUI if the information qualifies as CUI and the document is being shared outside DoD.

5.6. CUI Safeguarding Requirements. CUI requires safeguarding measures based on law, regulation, or government-wide policy. Safeguarding procedures include the following:

5.6.1. At a minimum, CUI may be disseminated to DoD personnel to conduct official DoD and US Government business under the following conditions.

5.6.1.1. No individual may have access to CUI information unless it is determined he or she has an authorized, lawful government purpose.

5.6.1.2. The person with authorized possession, knowledge, or control of CUI will determine whether an individual has an authorized, lawful government purpose to access designated CUI.

5.6.1.3. CUI information may be disseminated within the DoD Components and between DoD Component officials and DoD contractors, consultants, and grantees to conduct official business for the DoD, provided dissemination is consistent with controls imposed by a distribution statement or limited dissemination controls.

5.6.1.4. CUI designated information may be disseminated to a foreign recipient in order to conduct official business for the DoD, provided the dissemination has been approved by the foreign disclosure office and is appropriately marked as releasable to the intended foreign recipient.

5.6.2. Scientific, technical, and engineering information beyond basic research shall be treated as CUI. Examples include preliminary research and engineering data, engineering drawings, and associated specifications, lists, standards, process sheets, manuals, technical reports, technical orders, studies and analyses on topics requested by DoD Components, catalog-item identifications, data sets, and computer software with executable or source code. In addition, Distribution Statements B through F may be required. Refer to DoDI 5230.24, *Distribution Statements on Technical Documents,* for additional safeguarding guidance.

5.6.3. During an acquisition life cycle, CUI category or treatment of information may change. Safeguarding requirements must be reviewed for any necessary adjustments, including potential changes to the CUI designation, category, subcategory or type, or controls.

5.6.4. CUI will be identified in SCGs to ensure such information receives appropriate protection. If the SCG is canceled, a memorandum or other guidance document may be issued to identify CUI instead.

5.6.5. DoD is required to provide documents and records requested by members of the public, unless those records are exempt from disclosure per DoDD 5400.07, *DoD Freedom of Information Act (FOIA) Program*.

5.6.6. Other CUI category information may qualify for withholding from public release based on a specific FOIA exemption. Determining whether information meets the requirements for CUI shall be done separately and prior to identifying any potential FOIA exemptions.

5.6.7. CUI requiring distribution statements that does not qualify as classified information will be protected in accordance DoD CUI guidance.

5.6.8. Restricted data or formerly restricted data are classified and shall not be commingled with CUI in an unclassified document. For restricted data or formerly restricted data, follow the marking requirements per DoDM 5200.01, Volume 3, and the Atomic Energy Act of 1954.

5.6.9. Unit personnel will submit waiver requests for a specific CUI Program requirement to the SS. Waiver requests involving classified national security information will be accomplished according to DoDM 5200.01, Volume 1.

5.7. CUI System Network Requirements. Unit personnel will not use unofficial or personal (i.e., .net; .com; .org) e-mail accounts, messaging systems, or other non-DoD information systems, except approved or authorized government contractor systems, to conduct official business involving CUI.

5.8. CUI Dissemination. Dissemination controls identify the audience deemed to have a lawful government purpose to use the CUI and specify the rationale for applying the controls by specific codes. To ensure CUI protection, the following measures will be implemented:

5.8.1. During working hours, steps will be taken to minimize the risk of access by unauthorized personnel, such as not reading, discussing, or leaving CUI information unattended where unauthorized personnel are present. After working hours, CUI information will be stored in unlocked containers, desks, or cabinets if the government or government-contract building provides security for continuous monitoring of access. If building security is not provided, the information will be stored in locked desks, file cabinets, bookcases, locked rooms, or similarly secured areas. The concept of a controlled environment means there are sufficient internal security measures in place to prevent or detect unauthorized access to CUI. For DoD, an open storage environment meets these requirements.

5.8.2. CUI information and material may be transmitted via first class mail, parcel post, or bulk shipments. When practical, CUI information may be transmitted electronically (e.g., data, website, or e-mail), via approved secure communications systems or systems utilizing other protective measures such as Public Key Infrastructure or transport layer security (e.g., https). Avoid wireless telephone transmission of CUI when other options are available. CUI transmission via facsimile machine is permitted; however, the sender is responsible for determining whether appropriate protection will be available at the receiving location before transmission (e.g., facsimile machine attended by a person authorized to receive CUI; facsimile machine located in a controlled government environment).

5.8.3. CUI export-controlled technical information or other scientific, technical, and engineering information will still use distribution statements. Export-controlled information must also be marked with an export control warning.

5.9. CUI Decontrolling. CUI must be promptly and properly decontrolled unless doing so conflicts with a law, regulation, or government-wide policy. CUI documents and materials will be formally reviewed before being decontrolled or released to the public. The originator or other competent authority will terminate the CUI status of specific information when the information no longer requires protection from public disclosure. When the CUI status of information is terminated, all known holders will be notified by email or other means. Upon notification, holders will remove the CUI markings.

5.10. CUI Destruction. CUI material will be destroyed according to DoD and AF records management guidance. When destroying CUI, to include electronic forms, unit personnel will ensure all material is unreadable, indecipherable, and irrecoverable. CUI record and non-record documents may be destroyed by means approved for destroying classified information or by any other means making it unreadable, indecipherable, and unrecoverable.

6. Security Education and Training.

6.1. Purpose. This section outlines procedures for successful management of Unit Security Education and Training. The SS oversees, conducts, and documents all unit security training and is responsible to ensure security training records are properly maintained. Refer to DoD Manual 5200.01, Volume 3, Enclosure 5, and AFI 16-1404, Chapter 6, for additional guidance.

6.2. Types of Training. All AF military, civilians, and contractor personnel must complete required security training based on their manpower position and duty requirements. At a minimum, unit security training is accomplished upon assignment to the unit, prior to accessing classified information, annually, and as directed for specialized training requirements. Current unit security training includes the following:

6.2.1. Initial Indoctrination/Orientation Training. The SS will provide initial security indoctrination training in accordance with AFI 16-1404, Chapter 6, for all newly assigned personnel within 30 calendar days of assignment for active duty, civilians, and contractors and 90 calendar days for traditional reservists. For cleared personnel, initial indoctrination/ orientation training is required before access to classified information is granted.

6.2.2. Annual Security Refresher Training. The SS will provide annual refresher security training in accordance with AFI 16-1404, Chapter 6, for all assigned personnel.

6.2.3. Specialized Training. The SS will provide specialized security training in accordance with AFI 16-1404, Chapter 6, for personnel based on job responsibilities. Specialized training for derivative classification, transmission of classified information, courier, escort, hand-carry, deployments, foreign travel, or unique classified program access may involve other installation agencies or organizations. As such, all specialized training will be conducted in consultation with the SS.

6.3. Unit Security Training Plan. Security Education and Training shall be continuous, rather than periodic. To ensure all unit personnel properly maintain security proficiency and awareness, the SS will consult with the Unit Training Manager (UTM) to develop an annual training plan. This plan uses various means to provide the most effective method of maintaining security awareness to include the following: Periodic briefings, training sessions, formal presentations, and computer-based learning, among others. The current unit training plan is located on **Attachment 4**, *Sample Unit Security Training Plan*.

6.4. Security Training Course Descriptions. The following security training courses are applicable to unit personnel:

6.4.1. Annual Security Refresher Training. This training is required annually for all employees to include military, civilians, and contractors. This training is done via briefings, training sessions, or other formal presentations by the SS. Topics include CUI, local threat, counterintelligence, NATO & US classified security requirements and other relevant general security topics.

6.4.2. Cybersecurity Awareness Challenge. This training covers computer security information. This course is required annually for all employees with computer access and is located in AF myLearning.

6.4.3. Force Protection. This training covers Level I Antiterrorism, Active Shooter, and Counterintelligence awareness training. This course is required annually for all employees and is located in AF myLearning.

6.4.4. Controlled Unclassified Information. This training covers how to handle the various types of CUI to include FOUO, Privacy Act Information, Law Enforcement Sensitive, Unclassified Controlled Nuclear Information, contractor-owned proprietary information, etc., and unique marking and protection requirements. This course is required for all employees initially upon in-processing and annually as part of the annual security refresher training.

6.4.5. Counterintelligence Awareness and Reporting (CIAR). This training covers procedures for reporting foreign intelligence threats, local threat assessments and warnings, and counterintelligence insider threats among others. This course is required per DoDD 5240.06, *Counterintelligence Awareness and Reporting (CIAR),* initially upon in-processing and annually for all employees as part of the annual security refresher training. This training is satisfied by completing Force Protection Training.

6.4.6. Insider Threat (InT) Training. This training covers procedures for insider threat reporting. This training is required per AFI 16-1402, *Insider Threat Program Management,* paragraph 3.1.4, initially upon in-processing and annually for all employees as part of the annual security refresher training.

6.4.7. Hill AFB INFOSEC for Cleared Personnel. This course covers rules regarding classified information/material. This course is required prior to initial access to classified information and annually thereafter for all cleared personnel/personnel with security eligibility. This course is located in Training Scheduling System (TSS), course #MHPSEC9802900BR.

6.4.8. Security Education & Motivation Phase I/II. This training covers the rules and regulations regarding restricted/controlled areas and the RAB. This course is required initially for personnel with access to restricted/controlled areas and annually thereafter for personnel who possess a RAB. This course is located in TSS, course #MHPSEC9802100BR.

6.4.9. NATO Training. This training covers NATO security classified marking, handling, and storage requirements. Initial NATO security awareness training is only required for personnel when requesting SIPRNet access. Annual NATO security awareness training is included as part of unit security refresher training. If a unit member requires access to NATO classified, the SS will ensure the NATO awareness training is current, the NATO Security Awareness Form is accomplished and maintained on file until member is out-processed, and JPAS, DISS or the DoD system of record is updated to reflect the NATO access/date.

6.4.10. Derivative Classifier Training. This training covers proper procedures to perform derivative classification. This training is required for unit personnel appointed by the commander/director as a derivative classifier and all unit personnel with access to a classified information system (i.e., SIPRNet). This training is required as an initial and annual refresher training. This course is located on the Center for Development of Security Excellence (CDSE) website or in TSS, course MHPSEC9801900DL.

6.4.11. Marking Classified Information. This training covers classified marking requirements. This training is required when establishing a SIPRNet account. This course is required only as initial training and is located on the CDSE website or in TSS, course MHPSEC9801902DL.

6.4.12. Security Container and Classified Processing Area Custodian. This course covers policies and procedures regarding the management of safes and secure rooms. This training is required for all personnel who manage a Government Service Agency approved security container, secure room, vault, or CPA. There is a one-time instructor-led training requirement; however, personnel are welcome to re-attend refresher training at any time. Contact the SS who will request training slot(s) through 75 ABW/IP.

6.4.13. Alarm Custodian Training. This course covers the rules regarding the operation of the secure room alarm system. This course is required annually for all secure room custodians and is located in TSS, course #MHPSEC9800700DL.

6.4.14. Courier Training. This course is for all personnel designated as a classified courier. Commanders/directors determine the need for escort, courier, or hand-carry of classified material. At a minimum, verbal authority must be granted to carry classified material outside of normal work areas. Documentation of designated couriers is required via letter or DD Form 2501, when hand carrying classified material though an installation or facility check point. Refer to DoDM 5200.01, Volume 3, Enclosure 4, for additional guidance. The SS will maintain a roster of all unit-designated couriers and courier training acknowledgement for all personnel who transport classified material.

6.4.15. RD and CNWDI Training. This specialized training is for personnel granted access to RD and CNWDI by the commander/director. The SS will provide the Department of Energy approved briefing. The briefing slides are posted on the SAF/AAZ SharePoint: **https://cs2.eis.af.mil/sites/10260/SitePages/SharePoint%20for%20Security%20Personnel.aspx**.

6.5. **Security Training Locations.** Unit security training is not centralized but is located on various DoD, AF, and Hill AFB training sites to include:

6.5.1. DoD CDSE (**https://cdse.usalearning.gov**). Examples include: Derivative Classification Course and Marking Classified Information Course. (Note: CDSE site will not keep records; the member must get their certificate of completion at the time the training is taken, if they navigate away or go back later they must re-take the computer-based training to get another certificate.)

6.5.2. AF myLearning (**https://lms-jets.cce.af.mil/moodle/my/**). Examples include: Total Force Awareness Training courses consisting of Cybersecurity Awareness Challenge and Force Protection.

6.5.3. Hill AFB TSS: **https://ooafmctss.hill.af.mil/tssportal**. Examples include: Security Education and Motivation Training Phase I/II and Hill AFB INFOSEC for cleared personnel.

6.5.4. Joint Knowledge Online (JKO): **https://jkodirect.jten.mil/Atlas2/page/login/Login.jsf**. Examples include: Protecting Sensitive Information.

7. Foreign Nationals.

7.1. Purpose. This section outlines procedures for successful management of unit foreign national requirements. Foreign national visit procedures are for any person that is not a citizen or naturalized citizen of the United States or is a US citizen employed by a foreign nation or organization. Refer to DoDD 5230.20, *Visits and Assignments of Foreign Nationals*, and AFI 16-201, *Air Force Foreign Disclosure and Technology Transfer Program*, for additional guidance.

7.2. Foreign National Visit. The host/sponsor will notify the SS of any foreign national visit within the unit or subordinate organizations (squadrons, flights, etc.) for proper security protocols and procedures prior to the visit.

7.2.1. At a minimum, the host/sponsor will provide the following information during the coordination process:

7.2.1.1. Dates, times and exact location of the proposed visit.

7.2.1.2. Country submitting the request.

7.2.1.3. Names of foreign representatives to participate in the visit.

7.2.1.4. Stated purpose of the visit.

7.2.1.5. Classification level of the visit.

7.2.1.6. Any requested disclosure of classified information, CUI or other protected information.

7.2.2. The US point of contact will coordinate all details associated with the foreign visit, including the base security requirement of submitting a VAL to the Hill AFB base visitor control center at: **https://usaf.dps.mil/site.2.s/HillAFB/VCC/** not less than 3 business days prior to the visit. If during the coordination process, any proposed change to the visit by the foreign visitor will be reported to the AFOSI.

7.2.3. All foreign national visits must be requested in the Foreign Visit System (FVS) by the foreign visitor's embassy and approved locally by a Foreign Disclosure Officer. Such requests should be submitted 30 days prior to the requested visit. It is incumbent upon the visitor to complete this process with their own embassy. Foreign organizations that do not have access to the FVS, i.e. foreign contractors, the local Foreign Disclosure Office (FDO) has procedures that permit them direct input into the FVS. The US POC shall contact the FDO 30 days prior to the requested visit for assistance in completing the process and documentation requirements. No foreign national shall be escorted onto Hill AFB without an approved foreign visit request.

7.3. Escort Training. Escort training should be conducted prior to a visit to ensure security protocols are implemented to safeguard information being discussed. Only US military or United States Government employees may serve as escorts. Contractors or other foreign nationals may not serve as escorts. At a minimum, ensure escort training includes all personnel participating and they understand the contents of the visit and their responsibilities to safeguard sensitive information and materials from observation by visitors. Designate appropriate number of escort personnel and identify appropriate security measures to implement during the visit.

7.3.1. At minimum, the escorts should prohibit any type of photography, detailed note taking of areas, people or material observed and ensuring individuals are accounted for at all times. Escorts will be assigned as a primary escort to lead and a follow escort to walk behind and observe any abnormal behavior that could compromise government information.

7.4. Official Foreign Visit. An official foreign visit is a visit to the organization by a foreign national who is sponsored by their foreign government or international organization to perform official duties approved by the government. Therefore, it is important that such visits are processed, planned and conducted in a professional, respectful and policy compliant manner. Unit personnel must be careful not to make or insinuate the making of a commitment to disclose or transfer of classified information, CUI, controlled technology, technical data, or defense-related articles and/or services unless they have been granted such authority (in writing) by an appropriately authorized official.

7.4.1. Classified information, CUI, controlled technology, technical data, or defense-related articles and/or services shall not be disclosed to a foreign visitor unless specifically authorized by a FDO and only if it is directly related to the purpose of the visit as stated in the case detail report of an approved foreign visit request. Foreign nationals are not authorized to receive documentary information (classified information, CUI or other protected information) without the advance written approval of a foreign disclosure officer. Requests for oral, visual or documentary disclosures must be submitted for FDO review 10 business days prior to desired disclosure and may only be transferred via government-to-government channels.

7.4.2. Export controlled technical information is defined as any information which is required for the design, development, production, manufacture, assembly, operation, repair, testing, maintenance or modification of defense articles.

7.5. Host Supervisor Duties. The host supervisor shall notify AFOSI Detachment 113 at duty station number (DSN) 777-6112 for pre-brief and post-brief instructions. Notify security forces at DSN 777-3056 to complete access requirements to the installation and notify the FDO at DSN 586-1387 to receive proper instruction prior to any visit.

7.6. Foreign National Local System. Access for both unclassified and classified US DoD systems is not authorized. If a foreign national requests access to a US DoD System, contact the SS. The SS will coordinate with the appropriate FDO and 75 ABW/SC to determine required authorization and applicable requirements IAW DoD 8570.01-M, *Information Assurance Workforce Improvement Program*.

8. Counterintelligence Awareness and Reporting.

8.1. Purpose. This section outlines procedures for successful management of the unit CIAR Program. Refer to DoDD 5240.06 for additional guidance.

8.2. Counterintelligence Activities. Counterintelligence is an integral part of the DoD effort to detect, assess, exploit and counter collection, sabotage, espionage, and terrorist activities conducted by our adversaries. In today's environment, our adversaries are a diverse set of actors to include but not limited to foreign powers, international and domestic terrorist organizations, and radicalized individuals among others.

8.3. Counterintelligence Reporting. To protect US and DoD security interests such as personnel, information, and activities, unit personnel should immediately report to their supervisor, SS, or the commander/director any contacts, activities, indicators, or behaviors identified in paragraphs **8.4** - **8.6** below associated with a potential Foreign Intelligence Entity (FIE).

8.3.1. In the event a contact, activity, or behavior is not associated with a FIE, unit personnel should report these activities to include self-radicalization, to the Hill AFB AFOSI Detachment 113, Security Forces or the SS.

8.4. Reportable Foreign Intelligence Contacts, Activities, Indicators, and Behaviors.

8.4.1. When not related to official duties, contact with anyone known or believed to have information of planned, attempted, actual, or suspected espionage, sabotage, subversion, or other intelligence activities against DoD facilities, organizations, personnel, or information systems. This includes contact through social networking services that is not related to official duties.

8.4.2. Contact with an individual who is known or suspected of being associated with a foreign intelligence or security organization.

8.4.3. Visits to foreign diplomatic facilities that are unexplained or inconsistent with an individual's official duties.

8.4.4. Acquiring, or permitting others to acquire, unauthorized access to classified or sensitive information systems.

8.4.5. Attempts to obtain classified or sensitive information by an individual not authorized to receive such information.

8.4.6. Persons attempting to obtain access to sensitive information inconsistent with their duty requirements.

8.4.7. Attempting to expand access to classified information by volunteering for assignments or duties beyond the normal scope of responsibilities.

8.4.8. Discovery of suspected listening or surveillance devices in classified or secure areas.

8.4.9. Unauthorized possession or operation of cameras, recording devices, computers, and communication devices where classified information is handled or stored.

8.4.10. Discussions of classified information over a non-secure communication device.

8.4.11. Reading or discussing classified or sensitive information in a location where such activity is not permitted.

8.4.12. Transmitting or transporting classified information by unsecured or unauthorized means.

8.4.13. Removing or sending classified or sensitive material out of secured areas without proper authorization.

8.4.14. Unauthorized storage of classified material, regardless of medium or location, to include unauthorized storage of classified material at home.

8.4.15. Unauthorized copying, printing, faxing, e-mailing, or transmitting classified material.

8.4.16. Improperly removing classification markings from documents or improperly changing classification markings on documents.

8.4.17. Unwarranted work outside of normal duty hours.

8.4.18. Attempts to entice co-workers into criminal situations that could lead to blackmail or extortion.

8.4.19. Attempts to entice DoD personnel or contractors into situations that could place them in a compromising position.

8.4.20. Attempts to place DoD personnel or contractors under obligation through special treatment, favors, gifts, or money.

8.4.21. Requests for witness signatures certifying the destruction of classified information when the witness did not observe the destruction.

8.4.22. Requests for DoD information that make an individual suspicious, to include suspicious or questionable requests over the internet or social networking sites.

8.4.23. Trips to foreign countries that are:

8.4.23.1. Short trips inconsistent with logical vacation travel or not part of official duties.

8.4.23.2. Trips inconsistent with an individual's financial ability and official duties.

8.4.24. Unexplained or undue affluence.

8.4.24.1. Expensive purchases an individual's income does not logically support.

8.4.24.2. Attempts to explain wealth by reference to an inheritance, luck in gambling, or a successful business venture.

8.4.24.3. Sudden reversal of a bad financial situation or repayment of large debts.

8.5. Reportable International Terrorism contacts, activities, indicators, and behaviors.

8.5.1. Advocating violence, the threat of violence, or the use of force to achieve goals on behalf of a known or suspected international terrorist organization.

8.5.2. Advocating support for a known or suspected international terrorist organizations or objectives.

8.5.3. Providing financial or other material support to a known or suspected international terrorist organization or to someone suspected of being an international terrorist.

8.5.4. Procuring supplies and equipment, to include purchasing bomb-making materials or obtaining information about the construction of explosives, on behalf of a known or suspected international terrorist organization.

8.5.5. Contact, association, or connections to known or suspected international terrorists, including online, e-mail, and social networking contacts.

8.5.6. Expressing an obligation to engage in violence in support of known or suspected international terrorism or inciting others to do the same.

8.5.7. Any attempt to recruit personnel on behalf of a known or suspected international terrorist organization or for terrorist activities.

8.5.8. Collecting intelligence, including information regarding installation security, on behalf of a known or suspected international terrorist organization.

8.5.9. Familial ties, or other close associations, to known or suspected international terrorists or terrorist supporters.

8.5.10. Repeated browsing or visiting known or suspected international terrorist websites that promote or advocate violence directed against the US or US forces, or that promote international terrorism or terrorist themes, without official sanction in the performance of duty.

8.6. Reportable FIE-associated cyberspace contacts, activities, indicators, and behaviors.

8.6.1. Actual or attempted unauthorized access into US automated information systems and unauthorized transmissions of classified or CUI.

8.6.2. Password cracking, key logging, encryption, steganography, privilege escalation, and account masquerading.

8.6.3. Network spillage incidents or information compromise.

8.6.4. Use of DoD account credentials by unauthorized parties.

8.6.5. Tampering with or introducing unauthorized elements into information systems.

8.6.6. Unauthorized downloads or uploads of sensitive data.

8.6.7. Unauthorized use of Universal Serial Bus (USB), removable media, or other transfer devices.

8.6.8. Downloading or installing non-approved computer applications.

8.6.9. Unauthorized network access.

8.6.10. Unauthorized e-mail traffic to foreign destinations.

8.6.11. Denial of service attacks or suspicious network communications failures.

8.6.12. Excessive and abnormal intranet browsing, beyond the individual's duties and responsibilities, of internal file servers or other networked system contents.

8.6.13. Any credible anomaly, finding, observation, or indicator associated with other activity or behavior that may also be an indicator of terrorism or espionage.

8.6.14. Data exfiltrated to unauthorized domains.

8.6.15. Unexplained storage of encrypted data.

8.6.16. Unexplained user accounts.

8.6.17. Hacking or cracking activities.

8.6.18. Social engineering, electronic elicitation, e-mail spoofing or spear phishing.

8.6.19. Malicious codes or blended threats such as viruses, worms, trojans, logic bombs, malware, spyware, or browser hijackers, especially those used for clandestine data exfiltration.

9. Security Specialist Appointment and Training/Certification.

9.1. Purpose. This section outlines procedures for successful management of SS appointment and training/certification. Refer to DoDM 5200.01, Volume 1, Enclosure 3 and Volume 3, Enclosure 5, AFI 16-1404, Chapter 6 for additional guidance.

9.2. SS Appointment. The commander/director will designate/appoint in writing a primary SS (formerly unit security manager) and at least one alternate to administer the unit's Information Protection Program. The unit will complete an updated SS appointment letter using the most current Hill AFB SS appointment letter template (see **Attachment 5**, *Sample Unit Security Specialist Appointment Letter*). Obtain the commander/director's signature and email the new appointment letter to the 75 ABW/IP Chief, Information Protection via the 75 ABW/IP Workflow address: **75ABW.IP.Workflow@us.af.mil**. The SS will be:

9.2.1. A military officer, senior noncommissioned officer, or a civilian employee.

9.2.2. A US citizen.

9.2.3. Possess a favorably adjudicated, current personnel security investigation appropriate for the highest level of classification of information maintained/handled by the unit.

9.2.4. Have access to the level of information managed.

9.3. SS Training. Newly appointed unit SSs must complete the AF SS curriculum located on the CDSE STEPP website: **https://cdse.usalearning.gov**. There are five courses within the curriculum and tests for each course. After registering for the curriculum, the SS will automatically be assigned the five courses along with each test. Upon completion of the five courses, the AF SS curriculum certificate will be generated. Please send the AF SS curriculum certificate to the 75 ABW/IP, Chief, Information Protection, for permanent record using the 75 ABW/IP Workflow address: **75ABW.IP.Workflow@us.af.mil**. Note: If you do not have a STEPP account (**https://cdse.usalearning.gov**), you must create an account and wait 24 hours before you can register for any courses.

9.3.1. Reappointed unit SS do not need to complete the AF SS curriculum unless there has been a break of more than 5 years since your last AF SS curriculum certification. Contact the 75 ABW/IP, Chief, Information Protection using the 75 ABW/IP Workflow address: **75ABW.IP.Workflow@us.af.mil** to determine if your most current training certificate is still on file and valid. If not, please follow the instructions in **paragraph 9.3** above.

9.3.2. Security Professionals (career field 0080) are waived from the AF SS curriculum requirement if they possess a CDSE Security Professional Education Development (SPeD) Program Certification (i.e., Security Fundamentals Professional Certification, Security Asset Protection Professional Certification, or Security Program Integration Professional Certification). Please submit a copy of the SPeD certificate, most recent SPeD transcript, or conferral approval form in lieu of the SS curriculum certificate.

9.3.3. All newly appointed SSs must attend local Hill AFB SS training conducted every third Wednesday of the month from 0800-1700. This training is required in order to receive access to specialized Information Protection systems (JPAS, DISS, eQIP, InT, Enterprise Protection Risk Management, etc.) To attend the monthly training, please email the 75 ABW/IP Workflow address: **75ABW.IP.Workflow@us.af.mil** or call 777-5490 to schedule a class date.

9.4. Specialized SS Training Requirements.

9.4.1. JPAS.

9.4.1.1. For access to JPAS, link to the Personnel Security SharePoint (**https://org2.eis.af.mil/sites/21341/IP/PersonnelSecurity/default.aspx**). Consider adding to your favorites for future use and references. Click on the "JPAS, DISS or the DoD system of record" link under the documents listing. There you will find the JPAS SAR instructions document. Open and follow the steps to obtain access.

9.4.1.2. Complete the Joint Clearance and Access Verification System user levels 2-6 training certificate from CDSE/STEPP (located under "Personnel Security" drop down; course #PS183.16).

9.4.1.3. Complete DD Form 2962, V1, *Personnel Security System Access Request (PSSAR) Defense Manpower Data Center (DMDC),* for JPAS, DISS or the DoD system of record (Instructions on bottom of form and IPP SharePoint; under section 16, select box for Level 6 [GOV Only]).

9.4.2. DISS Training.

9.4.2.1. For access to DISS which is the system eventually replacing JPAS, you will need to request a DISS account. Click on the DISS folder, then open the DISS guide for instructions on how to obtain access for DISS.

9.4.2.2. Complete Joint Verification System short form CDSE/STEPP (located under DISS Training drop down; course #EX101.16).

9.4.2.3. Complete DD Form 2962 V1 for DISS (Instructions on bottom of form & Information Protection Personnel SharePoint; under section 16 select box for Security Officer Admin). Note: The DD Forms 2962 are different for each system.

9.4.3. e-QIP Access.

9.4.3.1. For access to e-QIP, click on the e-QIP Toolkit link under the "Documents" listing. Open the document for NP2 Portal and e-QIP access. This provides step-by-step instructions on how to fill out a DD Form 2875, System Authorization Access Request. Member's UPN (part of the CAC number) must be obtained and listed on the DD Form 2875, *System Authorization Access Request (SAAR),* as well. Click on the OPM NP2 Portal Registration UPN Instructions document.

9.4.3.2. Complete registration form for NP2 Portal Access Spreadsheet.

9.4.3.3. Complete DD Form 2875 for e-QIP access.

9.4.4. Personally Identifiable Information.

9.4.4.1. Complete Identifying and Safeguarding PII training certificate from CDSE/STEPP (located under "Information Security" drop down; course #DS-IF101.06).

9.4.5. Cyber Awareness.

9.4.5.1. Complete annual Cyber Awareness Training certificate from AF myLearning or TSS (must be current).

9.4.6. Once complete, provide all JPAS/DISS/e-QIP training certificates/documents to the 75 ABW/IPP Workflow using: **75ABW.IPP@us.af.mil**. Upon verification all required training requirements are complete, you will be contacted to establish your JPAS/DISS/e-QIP user access.

10. Classified Meetings and Conferences.

10.1. Purpose. This section outlines procedures for successful management of unit classified meetings and conferences. Refer to DoDM 5200.01, Volume 3, Enclosure 2, paragraph 16, AFI 16-1404, paragraph 2.7.13 and Attachment 4 checklist for additional guidance.

10.2. Classified Meeting Requirements. Classified meetings and conferences will normally be held in facilities that are already approved for processing and/or discussion of classified information.

10.2.1. Individuals requesting to hold/sponsor a classified meeting will contact the SS as soon as possible but no later than 5 duty days prior to the meeting. The host/sponsor will determine if the unit has an approved classified meeting plan (see **Attachment 6**, *Sample Classified Meeting Plan*) that meets their needs. If the location for the classified meeting is currently approved, the host/sponsor will review the classified meeting plan for specific requirements. If the locations is not currently approved, the host/sponsor will consult with the SS to determine the feasibility to conduct the classified meeting or other potential locations better suited to conduct the classified meeting.

10.2.2. An official will need to be designated as a security point of contact POC for the meeting if the organization's security specialist does not or is unavailable to perform these duties. The meeting security POC will use the Classified Meeting Conference Checklist in AFI 16-1404, Attachment 4.

10.3. Classified Meeting Criteria. In order to hold a classified meeting, the following criteria must be met IAW DoDM 5200.01, Volume 3, Enclosure 2, paragraph 16:

10.3.1. The meeting will serve a specific US Government purpose.

10.3.2. The use of other appropriate channels for dissemination of classified information or material is insufficient.

10.3.3. The meeting location will be under the security control of a US Government agency or a US contractor with an appropriate facility security clearance.

10.3.4. Adequate security procedures identified in a classified meeting plan have been developed and will be implemented to minimize risk to the classified information involved.

10.3.5. Classified sessions shall be segregated from unclassified sessions whenever possible.

10.3.6. Access to the meeting or conference, or specific sessions thereof, at which classified information will be discussed or disseminated, will be limited to persons who possess an appropriate security clearance and need-to-know, and have a current JPAS/DISS visit request on file with the organization conducting the meeting.

10.3.7. Any participation by foreign nationals or foreign representatives complies with the requirements of DoDD 5230.20 and DoDD 5230.11, *Disclosure of Classified Military to Foreign Governments and International Organizations*, (i.e., assurance is obtained in writing from the responsible US Government FDOs that the information to be presented has been cleared for foreign disclosure).

10.3.8. Announcement of the classified meeting will be unclassified and limited to a general description of topics expected to be presented, names of speakers, logistical information, and administrative and security instructions.

10.3.9. Non-government appropriately cleared US Government contractor personnel may provide administrative support and assist for a classified meeting, but all security requirements remain the sole responsibility of the DoD component sponsoring the meeting.

10.3.10. Procedures must ensure all classified documents, recordings, audiovisual material, notes, and other materials created, distributed, or used during the meeting are marked accordingly, controlled, safeguarded, and transported as required by other provisions of this instruction. Note taking or electronic recording during classified sessions shall be permitted only when it is determined that such action is necessary to fulfill the US Government purpose for the meeting.

10.4. Classified Meeting Preparation Actions. For all classified visits, a visit request, time permitting, will be submitted through JPAS, DISS or the DoD system of record to SMO Code of unit being visited, or an approved memorandum provided by approved base-level agencies. All personnel attending must meet the following requirements:

10.4.1. A valid need-to-know. Personnel attending the classified meeting must have a mission-related need to know, regarding the classified information to be discussed. Contractor need-to-know must also be verified via DD Form 254.

10.4.2. A clearance level equal to or greater than the material being accessed.

10.4.3. Proper government-issued ID.

10.4.4. An NDA on file. The SS will access JPAS, DISS or the DoD system of record to verify an NDA is on file. If an NDA is not on file, the SS will complete a new one and keep newly signed NDAs on file; the SS has the responsibility to update/annotate this information in JPAS, DISS or the DoD system of record.

10.5. Entry Authority List (EAL). The meeting security POC must compile an EAL to be vetted through the SS to ensure all personnel have signed an NDA and are authorized access to the level of information involved, according to JPAS, DISS or the DoD system of record. The vetted EAL will be used to control entry to the meeting. Anyone not listed must be denied entry. It is authorized for the meeting security POC to request the SS to vet an individual and add their name to the EAL with pen and ink.

10.5.1. Units are authorized to use an AF Form 1109, *Visitor Register Log*, or other locally developed sign in roster to provide record of attendance. The SS will maintain classified meeting records (AF Form 1109/sign in roster, etc.) as determined by the commander/director. File copies of classified meetings (AF Form 1109/sign in roster) will be maintained according to the unit file plan and disposed of per unit guidance.

10.6. Specific Classified Meeting Requirements. Specific requirements for protecting classified material during unit-sponsored meetings and conferences, to include seminars, exhibits, symposiums, conventions, training activities, workshops, or other such gatherings, during which classified material is disseminated, are outlined as follows:

10.6.1. All attendees' security clearance levels must be verified by the SS prior to allowing access to classified information or discussions. Personal recognition is not allowed in place of proper vetting. A roster of attendees must be submitted to the SS for JPAS, DISS or the DoD system of record security clearance vetting NLT 24 hours prior to the start of the classified meeting or discussion.

10.6.2. Classified information will be properly packaged and double wrapped prior to entering and exiting the meeting room. Classified notes and handouts are allowed, but must be appropriately portion marked and double wrapped prior to exiting the room.

10.6.3. Entry is controlled to ensure that only authorized personnel gain access to the area. Particular caution shall be taken to ensure that any individual who is not authorized to attend the classified meeting is denied entry.

10.6.4. Prior to the start of the meeting, all perimeter doors to the room will be locked. A cleared person will be posted outside the door (door guard) to ensure unauthorized personnel cannot overhear classified discussions, or introduce devices that would result in the compromise of classified information. A sign will be placed on the outer door that reads, "DO NOT ENTER, CLASSIFIED MEETING IN PROGRESS."

10.6.5. Use of cell phones, cameras, recording devices, PEDs, 2-way pagers, USB, Bluetooth, wireless, and any other electronic devices that record, transmit and receive information, are prohibited. Medical devices are not allowed without prior written approval from the authorizing official, IAW AFI 16-1404, AFMC Supplement, paragraph 2.7.7.2..

10.6.6. Upon conclusion of the classified meeting, classified information will be delivered to an approved secure facility or container. If it is after duty hours and arrangements have not been made or the unit is incapable of securing the classified material, contact the Command Post, 777-3007, to determine the feasibility of courtesy storage or destruction. An inspection of the room will be conducted at the conclusion of each meeting to ensure all classified materials are properly accounted for and sanitized from the room.

11. Sensitive Item Control.

11.1. Purpose. This section outlines procedures for successful management of Unit Sensitive Item Control.

11.2. Keys, Locks, and Access Cards. Government issued keys, locks, badges and proxy cards are an integral part for unit security process, procedures, and protocols. They are intended to limit access to authorized individuals of classified, CUI, and other sensitive information, material, or items.

11.2.1. To ensure proper accountability, all unit issued keys, locks, badges and proxy cards will be maintained using an inventory/issue record form and/or individual hand receipt. The individual hand receipt will be destroyed when keys, locks, badges and smart cards are returned and/or when no longer needed.

11.2.2. The commander/director will appoint/designate a unit key control/credential officer and/or key/credential custodian(s) in writing. The credential officer/custodian(s) are responsible to implement the unit system for controlling keys, locks and access control credentials.

11.2.3. The key control/credential officer will ensure all government issued keys, badges and proxy cards are inventoried upon change of key/credential control officer or key/credential custodian or at a minimum annually. Inventories will include all issued keys/credentials along with all items on-hand. Discrepancies involving NIPRNet computer rooms and SIPRNet classified processing areas will be immediately reported to the SS.

11.3. Access Control. Access to computer rooms/communications closets containing information system equipment (servers and network components) must be controlled at all times. Unescorted access to computer rooms/communication closets are only granted to persons with at least a favorable T-1. Contact the SS to verify personnel have the appropriate personnel security investigation. All other personnel must be physically escorted while accessing unit computer rooms/communications closets.

11.3.1. Access control measures such as reception personnel, guards, keyed locks, cipher locks or automated access control systems may be used to control access to computer rooms and/or communications closets.

12. Security Incident Procedures.

12.1. Purpose. This section outlines procedures for successful management of unit security incidents. The compromise of classified information presents a threat to the national security and may damage intelligence or operational capabilities, lessen the AF's ability to protect critical information, technologies, and programs, or reduce the effectiveness of AF management. Refer to DoDM 5200.01, Volume 3, Enclosures 6 & 7 and AFI 16-1404, Chapter 7 for additional guidance.

12.2. Initial Actions. Anyone discovering classified information unsecured or on an unauthorized information system, must immediately take custody and safeguard the information. Personnel must immediately notify the commander/director, supervisor, or SS. Do not use unsecured communications to provide specific details, which may lead an adversary to unprotected classified information. The commander/director and/or SS must contact 75 ABW/IP within the first duty day of discovery.

12.3. Notifications. The supervisor must immediately forward notification of an incident to the SS. The SS must immediately forward notification of an incident to the commander/director. The commander/director must defer to the next element in the chain of command if they are involved or in a position of bias. Notifications of a security incident include:

12.3.1. The type or level of information involved.

12.3.2. All persons involved.

12.3.3. Where the incident occurred.

12.3.4. When the incident was discovered.

12.4. Immediate Safeguarding Actions.

12.4.1. For incidents involving computers, unplug the Ethernet cable of each computer suspected to have been contaminated by classified information. Follow the Computer Incident Quick Reference Guide tri-fold: **https://org2.eis.af.mil/sites/21563/ia/Incident** Response Guidesand Information/Forms/AllItems.aspx.

12.4.2. The cybersecurity liaison and SS will work together to ensure all steps from the Data Spill–Classified Message Incident (DS-CMI) Response Guide are completed: **https://org2.eis.af.mil/sites/21341/IP/InformationSecurity/Samples,%20Templates/DS-CMI%20Response%20Guide.xlsx**

12.5. OCA Reporting. The commander/director must immediately notify the OCA, or direct someone to notify the OCA, in cases where classified information is lost or compromised, so damage may be assessed. Contact the POC, as listed in the applicable SCG, to request instructions on sending notification of compromise. Loss/compromise may not be apparent until after the inquiry is completed. Hence, this step is not necessarily sequential.

12.6. Incident/Inquiry Processing. The SS must contact 75 ABW/IPI or the designated IPO to obtain a security incident number within the first duty day.

12.6.1. The SS must draft an inquiry official appointment memorandum using the template from 75 ABW/IPI. The inquiry official must not be in a position of bias regarding the person(s) believed to have caused the incident. The inquiry official must be the same or greater rank/grade of the person(s) believed to have caused the incident. The inquiry official must have the same or greater eligibility and authorized access to the level of information involved according to JPAS, DISS or the DoD system of record.

12.6.2. The SS must issue the appointment memorandum to the inquiry official.

12.6.3. The SS must brief the inquiry official's supervisor. The inquiry official's primary duty is to provide the completed report to 75 ABW/IPI or designated IPO within the allotted time. Relief from other duties is required and leave and other absences are not permissible.

12.6.4. The SS must forward a completed/signed file copy of the appointment memorandum to 75 ABW/IPI or designated IPO within 2 duty days of receiving the incident number.

12.6.5. The SS must consult personnel with knowledge of the incident and supervisors of personnel suspected of having caused the incident and recommend to the commander/director whether access to classified information or user accounts should be suspended pending the outcome of the inquiry.

12.6.6. The SS must obtain the commander/director's decision whether the incident is to be opened in JPAS, DISS or the DoD system of record. The SS should consult 75 ABW/IPP or designated IPO prior to opening an incident in JPAS, DISS or the DoD system of record.

12.6.7. The inquiry official must immediately notify the commander/director if they believe classified information may have been lost or compromised.

12.7. Inquiry Report. The inquiry official must provide the completed report to 75 ABW/IPI or designated IPO within 10 duty days of the appointment memorandum by using the template provided from 75 ABW/IPI or designated IPO. The report of inquiry must include:

12.7.1. Summarization of what happened, the date the incident occurred, classification of information involved, and the source of classification.

12.7.2. Personnel interviewed.

12.7.3. Facts: Who, what, where, when, why, and how the incident occurred.

12.7.4. Conclusion:

12.7.5. Categorize the incident.

12.7.5.1. Whether the incident is unfounded, a security infraction, or a security violation.

12.7.5.2. The names of each person who caused the incident and whether the action of each person who caused the incident was willful, negligent, or inadvertent.

12.7.5.3. Whether it was possible to prove no classified information was lost or compromised.

12.7.6. Recommendations:

12.7.6.1. Explain what could/should be done to prevent recurrence.

12.7.6.2. Whether the OCA has been, or needs to be notified, based on whether the inquiry was able to prove there was no loss or compromise of classified information.

12.7.6.3. Whether the inquiry should be closed. If more time is needed, the commander/director may provide extensions in 10-day increments by sending an email to 75 ABW/IPI or designated IPO.

12.7.7. The inquiry official must provide additional information and/or update the report of inquiry as requested by 75 ABW/IPI or designated IPO.

12.8. Technical Review. Once the technical review is received from 75 ABW/IP the SS will draft an incident closure memorandum, to be signed by the commander/director, by using the template from 75 ABW/IPI or designated IPO. The SS should consult the commander/director as necessary.

12.9. Closure Memorandum. The SS must forward the completed/signed closure memorandum to 75 ABW/IPI or designated IPO within 20 duty days. The closure memorandum must include:

12.9.1. Whether the commander/director concurs with the IP technical review.

12.9.2. Whether the inquiry proved there was no compromise of classified information.

12.9.3. Close the incident as unfounded, a security violation, or security infraction. Note: loss/compromise of classified information is a mandatory security violation.

12.9.4. Actions to be taken to prevent recurrence of the incident.

12.9.5. Whether any administrative, disciplinary, or punitive action was taken against each person who caused the incident.

12.9.6. Whether the action of each culpable person who caused the incident was willful, negligent, or inadvertent.

12.9.7. Whether a Personnel Security Incident Report will be reported to the DoD CAF. Note: willful and negligent incidents are mandatorily reported to CAF.

12.9.8. Whether the OCA was notified to complete a damage assessment. Note: OCA notification is required unless there is proof positive no classified information was compromised.

12.10. Security Incident Follow-on Actions.

12.10.1. The SS must consult 75 ABW/IPP prior to forwarding Personnel Security Incident Reports to the DoD CAF.

12.10.2. The SS will coordinate with 75 ABW/IPI to ensure up-channel notifications are accomplished as required.

MICHELLE D. HATHAWAY, NH-04, DAF
Vice Director, Ogden Air Logistics Complex

Attachment 1

GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

References

Security Executive Agent Directive 3, *Reporting Requirements for Personnel with Access to Classified Information or Who Hold a Sensitive Position*, 12 June 2017

Code of Federal Regulations, Title 32, Part 117, *National Industrial Security Program Operating Manual*

DoDD 5100.55, *United States Security Authority for North Atlantic Treaty Organization Affairs (USSAN)*, 27 February 2006

DoDD 5230.11, *Disclosure of Classified Military Information to Foreign Governments and International Organizations*, 16 June 1992

DoDD 5230.20, *Visits and Assignments of Foreign Nationals*, 22 June 2005

DoDD 5240.06, *Counterintelligence Awareness and Reporting (CIAR)*, 17 May 2011, Incorporating Change 3, July 21, 2020

DoDD 5400.07, *DoD Freedom of Information Act (FOIA) Program*, 5 April 2019

DoDD 8100.02, *Use of Commercial Wireless Devices, Services, and Technologies in the Department of Defense (DoD) Global Information Grid (GIG)*, 14 April 2004

DoDI 5200.02, *DoD Personnel Security Program (PSP)*, 21 March 2014

DoDI 5200.48, *Controlled Unclassified Information (CUI)*, 6 March 2020

DoDI 5230.24, *Distribution Statements on Technical Documents*, 23 August 2012

DoDI 5505.17, *Collection, Maintenance, Use, and Dissemination of Personally Identifiable Information and Law Enforcement Information by DoD Law Enforcement Activities*, 19 December 2012

DoDM 5200.01, Volume 1_AFMAN16-1404 Volume 1, *Information Security Program*: *Overview, Classification, and Declassification*, 11 January 2021

DoDM 5200.01, Volume 1_AFMAN16-1404, Volume 1, HILLAFBSUP, *Information Security Program: Overview, Classification, and Declassification*, 10 March 2022

DoDM 5200.01, Volume 2_AFMAN16-1404, Volume 2, *Information Security Program*: *Marking of Information*, 7 January 2021

DoDM 5200.01, Volume 3_AFMAN16-1404, Volume 3, *Information Security Program: Protection of Classified Information*, 23 December 2020

DoDI 5200.02, *Procedures for the DoD Personnel Security Program (PSP)*, 3 April 2017

DoDM 5200.02_AFMAN 16-1405, *Air Force Personnel Security Program*, 1 August 2018

DoDM 5220.22_AFMAN16-1406, Vol 2, *National Industrial Security Program: Industrial Security Procedures For Government Activities*, 8 May 2020

DoDM5220.22V2_AFMAN16-1406V2_AFMCSUP, *National Industrial Security Program: Industrial Security Procedures for Government Activities*, 3 December 2021

DoDI 7730.47, *Defense Incident-Based Reporting System (DIBRS)*, 23 January 2014

DoD 8570.01-M, *Information Assurance Workforce Improvement Program*, 19 December 2005

DAFMAN 16-201, *Department of the Air Force Foreign Disclosure and Technology Transfer Program*, 19 January 2021

AFI 16-1401, *Information Protection*, 29 July 2019

AFI 16-1402, *Counter-Insider Threat Program Management*, 17 June 2020

AFI 16-1404_AFMCSUP, *Air Force Information Security Program*, 17 February 2016

AFI 33-322, *Records Management and Information Governance Program*, 23 March 2020

Prescribed Forms

None

Adopted Forms

AF Form 847, *Recommendation for Change of Publication*

AF Form 1109, *Visitor Register Log*

AF Form 2583, *Request for Personnel Security Action*

AF Form 2586, *Unescorted Entry Authorization Certificate*

AF Form 2587, *Security Termination Statement*

DD Form 254, *Department of Defense Contract Security Classification Specification*

DD Form 2501, *Courier Authorization*

DD Form 2875, *System Authorization Access Request (SAAR)*

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

Optional Form 306, *Declaration for Federal Employment*

SF 86, *Questionnaire for National Security Positions*

SF 312, *Classified Information Nondisclosure Agreement*

SF 703, *Top Secret (Coversheet)*

SF 704, *Secret (Coversheet)*

SF 705, *Confidential (Coversheet)*

HILL AFB Form 496, *Application for Installation Access Control*

Abbreviations and Acronyms

AF—Air Force

AFB—Air Force Base

AFMC—Air Force Materiel Command

AFOSI—Air Force Office of Special Investigations

APACS—Aircraft and Personnel Automated Clearance System

ATR—Antiterrorism Representative

CAC—Common Access Card

CAF—Consolidated Adjudications Facility

CDSE—Center for Development of Security Excellence

CE—Continuous Evaluation

CIAR—Counterintelligence Awareness and Reporting

CMI—Classified Message Incident

CNWDI—Critical Nuclear Weapon Design Information

COR—Contracting Officer Representative

CPA—Classified Processing Area

CUI—Controlled Unclassified Information

DBIDS—Defense Biometric Identification System

DISS—Defense Information System for Security

DoD—Department of Defense

DODD—Department of Defense Directive

DODI—Department of Defense Instruction

DS-CMI—Data Spill-Classified Message Incident

E-QIP—Electronic Questionnaire for Investigations Processing

FBI—Federal Bureau of Investigations

FDO—Foreign Disclosure Office

FIE—Foreign Intelligence Entity

FOIA—Freedom of Information Act

FOUO—For Official Use Only

FSO—Facility Security Officer

FVS—Foreign Visit System

IAW—In Accordance With

InT—Insider Threat

IP—Information Protection

IPO—Information Protection Office

JKO—Joint Knowledge Online

JPAS—Joint Personnel Adjudication System

MAJCOM—Major Command

MFR—Memo for Record

NATO—North Atlantic Treaty Organization

NC2-ESI—Nuclear Command Control Extremely Sensitive Information

NISS—National Industrial Security System

NISPOM—National Industrial Security Program Operating Manual

OCA—Original Classification Authority

OO-ALC—Ogden Air Logistics Complex

PA—Privacy Act

PCS—Permanent Change of Station

PII—Personally Identifiable Information

POC—Point of Contact

PWS—Priority Work Statement

RAB—Restricted Area Badge

RD—Restricted Data

RIP—Report on Individual Personnel

SAP—Special Access Program

SAR—Security Access Requirement

SCG—Security Classification Guide

SCI—Sensitive Compartmented Information

SCIF—Sensitive Compartmented Information Facility

SEAD—Security Executive Agent Directive

SIPRNet—Secret Internet Protocol Router Network

SMO—Security Management Office

SNM—Special Nuclear Material

SON—Security Office Number

SOW—Statement of Work

SPēD—Security Professional Education Development

SS—Security Specialist

SSI—Special Security Instructions

SSN—Social Security Number

SSO—Special Security Officer

STEPP—Security Training, Education, and Professionalization Portal

SUP—Supplement

TIS—Transfer in Status

TSS—Training Scheduling System

US—United States

UMD—Unit Manning Document

USB—Universal Serial Bus

UTM—Unit Training Manager

VAL—Visit Access List

VAR—Visit Access Request

VGSA—Visitor Group Security Agreement

75 FSS—75th Force Support Squadron

Terms

Access—The ability and opportunity to obtain knowledge of national security information. An individual may have access to national security information by being in a place where such information is kept, if the security measures that are in force do not prevent the individual from gaining knowledge of such information.

Accountable Forms—Forms that the AF stringently controls and which cannot be released to unauthorized personnel, since their misuse could jeopardize DoD security or result in fraudulent financial gain or claims against the government.

Activity Security Specialist (i.e., Information Protection Office)—The activity security specialist manages and implements the activity's information security program and ensures its visibility and effectiveness on behalf of the activity head, who retains the responsibility for overall management and functioning of the program. The activity security specialist must have sufficient delegated authority to ensure that personnel adhere to program requirements, and their position within the organizational hierarchy must ensure their credibility and enable them to raise security issues directly to their respective activity head.

Adjudication Facility—A facility with assigned adjudicators certified to evaluate Personnel Security Investigations and other relevant information to determine if granting or continuing national security eligibility is clearly consistent with the interests of national security. The DoD consolidated adjudications facility is known as the DoD CAF.

Adopted Form—A form used (required) in a publication other than the prescribing publication.

Assistant Security Specialist—In large activities and where circumstances warrant, activities may designate US Government civilian or military members as assistant security specialist(s) to assist the activity security specialist with program implementation, maintenance, and local oversight.

Classified Meeting or Conference—Includes seminars, exhibits, symposia, conventions, training classes, workshops, or other such gatherings, during which classified information is disseminated. This does not apply to operational meetings conducted in combat situations, classes conducted by DoD schools, or gatherings of personnel of a DoD component and foreign government representatives or US and/or foreign contractor representatives on a matter related to a specific US Government contract, program, or project, or routine day-to-day staff meetings or discussion within an office on specific topics.

Classified Message Incidents (CMI)—A higher classification level of data is transferred to a lower classification level system/device via messaging systems, e.g., e-mail, instant messaging.

Collateral Eligibility—Top Secret, Secret, or Confidential levels of eligibility.

Controlled Substance—Any drug, material, or other chemical compound identified and listed in DNI Memorandum ES 2014-00674.

Counterintelligence—Information gathered and activities conducted to identify, deceive, exploit, disrupt, or protect against espionage, other intelligence activities, sabotage, or assassinations conducted for or on behalf of foreign powers, organizations, or persons, or their agents, or international terrorist organizations or activities.

Current—An investigation that is no more than 5 years old. If JPAS, DISS or the DoD system of record reflects an open investigation, or a pending adjudication not more than 1 year beyond the 5-year anniversary date, the investigation is considered current.

Damage to the National Security—Harm to the national defense or foreign relations of the United States from the unauthorized disclosure of information, taking into consideration such aspects of the information as the sensitivity, value, utility, and provenance of that information, or other breach of security responsibilities by personnel serving in national security positions.

Data Spillage—Occurs whenever classified information or CUI is transferred onto an information system not authorized for the appropriate security level or not having the required CUI protection or access controls. For example, when a user takes a file such as a word document and copies it to removable media (e.g., DVD or CD) from the SIPRNet and then the user takes that media and loads the data onto a NIPRNET computer. A classified data spillage is a security violation. A data spillage is not necessarily a CMI.

Derivative Classification—Incorporating, paraphrasing, restating, or generating in new form, information that is already classified, and marking the newly developed material consistent with the classification markings that apply to the source information. Includes the classification of information based on classification guidance. The duplication or reproduction of existing classified information is not derivative classification.

Derogatory Information—Information that reflects on the integrity or character of an individual, or circumstances that suggests that their ability to safeguard national security information may be impaired, that their access to classified or sensitive information clearly may not be in the best interest of national security, or that their activity may be in conflict with the personnel security standards or adjudicative guidelines.

Eligibility Determination—The decision to grant eligibility for access to classified information or performance of national security duties.

Electronic Questionnaire for Investigations Processing—A secure web-based automated system that facilitates timely and accurate processing of investigation requests to OPM. Agencies authorize applicants to access the system to enter data and documents required for the investigation; the system collects information from the applicant based on the appropriate investigative questionnaire.

Illegal Drug—A controlled substance included in Schedule I or II, as defined by Section 802(6) of E.O. 12564.

Inadvertent Spillage or Unauthorized Disclosure of Classified Information on Information Systems—An incident where a person did not know, and had no reasonable basis to know, that the security violation or unauthorized disclosure was occurring while using an information system (e.g., a person reasonably relied on improper markings).

Information Protection—Information Protection is a subset of the AF Security Enterprise and consists of the core security disciplines (Personnel, Industrial, and Information Security) used to determine military, civilian, and contractor personnel's eligibility to access classified information, ensure the protection of classified information released or disclosed to industry in connection with classified contracts, and protect classified information and CUI that, if subject to unauthorized disclosure, could reasonably be expected to cause damage to national security.

Joint Personnel Adjudication System—The DoD system of record for personnel security adjudication, clearance, verification, and history. The term applies not only to this system but to any successor DoD personnel security system of record. JPAS has two applications, the Joint Adjudication Management System and the Joint Clearance and Access Verification System. The Joint Adjudication Management System is the application that supports central adjudication facilities personnel and provides capabilities and data such as case management and distribution, adjudication history, due process history, revocations and denial action information. Joint Clearance and Access Verification System is the application that supports command security personnel and provides capabilities and data such as local access record capabilities, debriefings, incident file reports and eligibility data, and security management reports.

Limited Access Authorization—Authorization for access to confidential or secret information granted to non-US citizens and immigrant aliens, limited to only that information determined releasable by a US Government designated disclosure authority to the country of which the individual is a citizen, in accordance with DoDD 5230.11. Access is necessary for the performance of the individual's assigned duties with the military or a federal agency and is based on favorable adjudication of a 10-year Single Scope Background Investigation or its equivalent under the Federal Investigative Services.

National Security Duties—Duties performed by individuals working for or, on behalf of, the Federal Government that are concerned with the protection of the United States from foreign aggression or espionage, including development of defense plans or policies, intelligence or Counter Intelligence activities, and related activities concerned with the preservation of the military strength of the United States, including duties that require eligibility for access to classified information in accordance with E.O. 12968.

National Security Eligibility—The status that results from a formal determination by an adjudication facility that a person meets the personnel security requirements for access to classified information or to occupy a national security position or one requiring the performance of national security duties.

National Security Information—Information that has been determined, pursuant to E.O. 13526, to require protection against unauthorized disclosure and is so marked when in documentary form.

Need-To-Know—A determination made by a possessor of classified information that a prospective recipient, in the interest of the national security, has a requirement for access to, knowledge of, or possession of the classified information in order to perform tasks or services essential to the fulfillment of an official US Government program. Knowledge of, possession of, or access to, classified information will not be afforded to any individual solely by virtue of the individual's office, position, or security eligibility. For contractors their need-to-know is their requirements of the contract and DD Form 254.

Negligent Discharge of Classified Information—Term based on the familiar firearms term "Negligent Discharge" to connote the seriousness of a spillage or unauthorized disclosure of classified information while using an information system.

Negligent Spillage or Unauthorized Disclosure of Classified Information on Information Systems—An incident where a person acted unreasonably in causing a spillage or unauthorized disclosure while using an information system (e.g., a careless lack of attention to detail, or reckless disregard for proper procedures).

National Industrial Security Program—The program established by DoDM 5200.01 to safeguard Federal Government classified information that is released to contractors, licensees, and grantees of the United States Government as the single, integrated, cohesive industrial security program to protect classified information and to preserve our Nation's economic and technological interests, as governed by the US Office of Personnel Management Booklet and E.O. 10865.

Nuclear Weapon Data—RD and formerly restricted data concerning the design, manufacture, or utilization (including theory, development, storage, characteristics, performance, and effects) of nuclear weapons or nuclear weapon components, including information incorporated in or related to nuclear explosive devices.

Original Classification—Initial determination information requires, in the interests of national security, protection against unauthorized disclosure.

Position Designation—The assessment of the potential for adverse impact on the integrity and efficiency of the service, and the degree to which, by the nature of the civilian position, the occupant could bring about a material adverse effect on the national security.

Periodic Reinvestigation—A national security investigation conducted to update a previously completed investigation on persons holding a national security position or performing national security duties to determine whether that individual continues to meet national security requirements.

Personnel Security Investigation—Any investigation required for the purpose of determining the eligibility of DoD military and civilian personnel, contractor employees, consultants, and other persons affiliated with the DoD for access to classified information, acceptance or retention in the military departments, assignment or retention in sensitive duties, or other designated duties requiring such investigation. It also includes investigations of allegations that arise subsequent to adjudicative action and require resolution to determine an individual's current eligibility for a national security position.

Public Trust—Defined in Federal investigative standards.

Reportable Behavior—Acts by persons with favorable national security eligibility determinations that may not be consistent with the interests of national security.

Sensitive Compartmented Information—Classified information concerning or derived from intelligence sources, methods, or analytical process that is required to be handled within a formal access control system established by the Director of National Intelligence.

Scope—The time period to be covered and the sources of information to be contacted during the prescribed course of a national security investigation.

Security Specialist (formerly unit security manager)—SSs are US Government civilian, military, or contractor employees who perform administrative security functions under the direction of their commander/director or Information Protection Office (i.e., Activity Security Specialist), without regard for job series, title, or rank, rate, or grade provided they have the clearance required for the access needed to perform their assigned duties and tasks.

Senior Agency Official—The SECAF designated position for directing, administering, and overseeing the AF Information Security Program in accordance with DoDM 5200.01, Volume 1, *DoD Information Security Program: Overview, Classification, and Declassification*, Enclosure 2, SAF/AA is the AF Senior Agency Official. There are no other Senior Agency Officials within the AF.

Security Clearance—A personnel security determination by competent authority that an individual is eligible for access to national security information, under the standards of this manual. Also called a clearance. The individual must have both eligibility and access to have a security clearance. Eligibility is granted by the central adjudication facilities, and the access is granted by the individual agencies.

Security-in-Depth—Determinations by the senior agency official that a facility's security program consists of layered and complimentary security controls sufficient to deter, detect, and document unauthorized entry and movement within the facility. AF facilities located on installations with a perimeter fence or other type of legal boundary, perimeter access controls for employees and visitors, law enforcement and security patrols, and have locking doors and or another type of access controls have security-in-depth. All other determinations are made by the security program executive or wing commander for storage of Top Secret, Secret, and Confidential information.

Sensitive Position—Any position so designated by the head of any department or DoD Component in accordance with E.O. 10450.

Security Office Number (SON)—A number that identifies the office that initiates the investigation and is recorded in the appropriate 'Agency Use' block of the investigative form. The SON is issued by OPM after authorization by the Office of the Director Defense Intelligence (Intelligence & Security).

Security Professional Education Development—The SPēD Program is part of the DoD initiative to professionalize the security workforce. This initiative is intended to ensure that there is a common set of competencies among security practitioners that promotes interoperability, facilitates professional development and training, and develops a workforce of certified security professionals.

Standard Form 86—The standard form that the DoD uses for most national security background investigations. The automated version of the SF 86 is the e-QIP. As used in this manual, includes SF 86 and related forms.

Unclassified Controlled Nuclear Information—Relates to physical protection of DoD Special Nuclear Material (SNM), SNM equipment, and SNM facilities, including unclassified information on the physical protection of nuclear weapons containing SNM in the custody of DoD.

Valid Passport—A passport that is current (i.e., has not expired and has not been cancelled or revoked).

Willful Spillage or Unauthorized Disclosure of Classified Information on Information Systems—An incident where a person purposefully disregards DoD or AF security or information safeguarding policies or requirements (e.g., intentionally bypassing a known security control).

Attachment 2

SAMPLE UNIT PERSONNEL IN-PROCESSING PROCEDURES

A2.1. Personnel Procedures. Personnel in-processing the unit must complete the following training prior to the commander authorizing classified access:

A2.1.1. Initial Unit Security Training.

A2.1.2. NATO Briefing (Need signature last page).

A2.1.3. Cleared Personnel Training (Need signature last page).

A2.1.4. SEAD 3/Continuous Evaluation Training (Review/provide trifold).

A2.1.5. Derivative Classifier Training (Provide certificate).

A2.1.6. Eagle Eyes/Counterintelligence Awareness Training (Review briefing).

A2.2. SS Procedures.

A2.2.1. JPAS.

A2.2.1.1. Own/service.

A2.2.1.2. Validate clearance/eligibility (Ensure last security clearance is current).

A2.2.1.3. Verify signed SF 312 (NDA) date or accomplish.

A2.2.1.4. Brief access as appropriate.

A2.2.1.5. Inform 75 ABW/IPP for servicing relationship in JPAS, DISS or the DoD System of Record.

A2.3. Vindicator.

A2.3.1. Issue vindicator card.

A2.3.2. Activate vindicator card.

A2.3.3. Ensure correct building access (Lan/Comm/Remote Monitoring and Control).

A2.4. Flight Line Access.

A2.4.1. Complete initial controlled/restricted area line badge training, TSS course # MHPSEC9802100BR, Security Education and Training Phase I/II.

A2.4.2. E-mail UTM with the initial date to load in the TSS profile.

A2.4.3. Update the training roster with annual controlled/restricted area training date.

A2.4.4. Fill out an AF Form 2586 for a line badge and route it for signatures. Once it is signed, provide it to the member who contacts 75 SFS Pass & ID to obtain a badge. The member returns the AF Form 2586 copy to the SS.

A2.5. CAC issuance.

A2.6. SIPRNet account.

A2.6.1. Verify derivative classifier training date.

A2.6.2. If it is an initial SIPRNet account, complete both Marking Classified Information and Derivative Classification courses (**https://securityawareness.usalearning.gov/**).

A2.6.3. E-mail the UTM the course training dates.

A2.7. Update SS records as appropriate.

A2.8. Sign/date the member's in-processing sheet and return it to the member.

Attachment 3

SAMPLE UNIT PERSONNEL OUT-PROCESSING PROCEDURES

A3.1. Personnel Procedures. Personnel out-processing the unit must complete the following actions prior to leaving:

A3.1.1. Return their vindicator card, issued keys and locks.

A3.1.2. Sign an AF Form 2587, *Security Termination Statement.*

A3.1.3. Sign a NATO access signature page debrief.

A3.1.4. If the individual is separating or retiring, sign a SF 312, NDA (military/civilian).

A3.1.5. If they are industrial personnel, ensure the contractor supervisor takes the individual's CAC and turns it in.

A3.2. SS Procedures.

A3.2.1. Remove the vindicator card access.

A3.2.2. Access JPAS, DISS or the DoD System of Record.

A3.2.2.1. Ensure classified access is removed.

A3.2.2.2. Out-process the individual from the unit.

A3.2.3. Send an out-processing email to 75 ABW/IPP (name, SSN no dashes, military/civilian/industrial partners).

A3.2.4. Scan all out-processing documents (AF Form 2587, NATO) to the unit security out-processing folder.

A3.2.5. Open the unit Information Security Program.

A3.2.5.1. Copy or type individual's name onto the out-processing sheet.

A3.2.5.2. Input the vindicator card turn-in and debrief dates.

A3.2.5.3. Delete individuals:

A3.2.5.3.1. From the appropriate civilian, military, industrial sheet and re-adjust sheet (copy/paste) so there are no blanks between individuals.

A3.2.5.3.2. Classified access authorization, AF Form 2583.

A3.2.5.3.3. Cleared personnel training certificate.

A3.2.5.3.4. Derivative training certificate.

A3.2.6. Update SS records.

A3.2.7. Sign/date out-processing sheet/return to member.

Attachment 4

SAMPLE UNIT SECURITY TRAINING PLAN

A4.1. References:

A4.1.1. DoDI5200.48

A4.1.2. DoDM5200.01 Volume 1_AFMAN16-1404, Volume 1

A4.1.3. DoDM5200.01, Volume 2_AFMAN16-1404, Volume 2

A4.1.4. DoDM5200.01, Volume 3_AFMAN16-1404, Volume 3

A4.1.5. DoDM 5200.01, Volume 3, Enclosure 5

A4.1.6. AFI 16-1404 AFMCSUP

A4.1.7. AFI 16-1404 HILLSUP

A4.1.8. DoDD 5240.06

A4.2. Purpose. DoD Components shall implement a training program so that personnel understand their day-to-day security responsibilities, are familiar with security vulnerabilities and the vulnerabilities of the facility and are prepared to implement emergency security actions. The specific training requirements for training are listed in references (a) through (g).

A4.3. All personnel in the organization: Including DoD civilians, military members, and on-site contractor personnel shall receive the following training:

A4.3.1. Initial Orientation Training (includes CUI) (A4.1.1/A4.1.2/A4.1.3/A4.1.4/A4.1.5).

A4.3.2. Cyber Awareness Training (A4.1.3/A4.1.5).

A4.3.3. Annual Refresher Training (A4.1.1/A4.1.2/A4.1.3/A4.1.4/A4.1.5).

A4.3.4. Recurring Security Education (includes CUI) (Continuous, not periodic, read and sign .not sole source of education) (A4.1.1/A4.1.2/A4.1.3/A4.1.5).

A4.3.5. Counter-Intelligence Training (Initial and Annual) (A4.1.7).

A4.3.6. NATO Awareness Brief (A4.1.3/A4.1.5).

A4.4. All personnel in the organization: Including DoD civilians, military members, and on-site contractor personnel shall receive initial security training (SF 312 if not documented previously).

A4.5. All personnel in the organization: Including DoD civilians, military members, and on-site contractor personnel with access to classified systems will complete the below training:

A4.5.1. Derivative classification training courses (**http://cdsetrain.dtic.mil**) or local equivalent (A.4.1.3/A.4.1.5)

A4.5.2. Derivative Classification (Initial and Annual) (A4.1.3/A4.1.4/A4.1.5).

A4.5.3. Marking Classified Information (Initial and Annual) (A4.1.3/A4.1.4/A4.1.5).

A4.5.4. NATO Indoctrination (if designated for access utilize AF Form 2583 or SIPRNet) (A4.1.3/A4.1.5).

A4.6. Unit Quarterly Security Training. Quarterly security training will contain annual unit security training requirements along with suggested 75 ABW/IP quarterly security training. Additional security training will be added based on the unit's security training needs.

Attachment 5

SAMPLE UNIT SECURITY SPECIALIST APPOINTMENT LETTER

Figure A5.1. Unit Security Specialist Appointment Letter.

[Use unit letter head]

XX XXX XX

MEMORANDUM FOR 75 ABW/IP

FROM: XXX XXXX

SUBJECT: Security Specialist Appointment Letter

1. The following individuals are appointed Security Specialists (SS) for (organization).

a. Primary
Name: Grade/Rank:
Duty Title: Security Specialist Clearance:
Mailing Address:
Office Symbol:
DSN/Commercial Phone:
FAX Number:
Training Date:
Email:

b. Alternate
Name: Grade/Rank:
Duty Title: Clearance:
Mailing Address:
Office Symbol:
DSN/Commercial Phone:
FAX Number:
Training Date:
Email:

2. This supersedes previous letter, same subject.

X
Signature Block
Commander or Director

Attachment:
AF SS Curriculum Certificate(s)

Attachment 6

SAMPLE CLASSIFIED MEETING PLAN

A6.1. Building 123 Conference Room 2 Classified Meeting Plan.

A6.1.1. **Initial Preparation.**

A6.1.1.1. SECRET is the highest approved classification level.

A6.1.2. Transmission of classified information is not approved, whether electronic, hardcopy, or otherwise.

A6.1.3. Attendees must have the appropriate eligibility and access according to JPAS, DISS or the DoD System of Record, a signed Nondisclosure Agreement and need-to-know.

A6.1.4. Entry control will be conducted by checking the attendee's CAC and comparing it to the JPAS, DISS or DoD System of Record visit request (or other appropriate access roster). If personnel are not included on the access roster, it is permissible to verify eligibility and access via JPAS, DISS or the DoD Sysem of Record and then add the attendee to the access roster.

A6.2. Before the Meeting.

A6.2.1. Designate the Meeting SS. If the SS from the organization hosting the meeting is not available to perform these duties, request the highest ranking authority from the organization hosting the classified meeting to verbally designate the meeting SS on behalf of the commander/director. The meeting SS implements the security provisions established in DoDM 5200.01, Volume 3, Enclosure 2. For quick reference, use the Classified Meeting/Briefing/ Conference Checklist which was included as **Attachment 2** of 75 ABW/IP's approval memorandum for this classified meeting plan. The meeting SS may also perform as the entry controller.

A6.2.2. Post signs.

A6.2.2.1. Place "Please Do Not Enter, Classified Meeting in Progress" signs (or similar) at the rear door near the West stairway and at the double glass doors near the center stairway.

A6.2.2.2. Open the right hand door to the cell phone cubby halfway so that the sign "Please, No Electronic Devices Beyond this Point" is clearly visible as personnel proceed through the hallway towards Conference Room 2. Open the left hand door all the way to make the cell phone cubby accessible to attendees.

A6.2.3. Post rear door guard. The rear door guard must have appropriate eligibility, access, and listed on the visit request (or other appropriate access roster). The rear door guard must have in their possession the special security instructions for this post.

A6.2.4. Remove or disable known electronic devices.

A6.2.4.1. Classified electronic devices, such as a SIPRNet laptop, are not authorized unless approved by the Hill AFB Emmissions Security Manager, 75 ABW/SCXO, 777-0362. Keep all unclassified electronic devices at least 3 meters away from classified electronic devices.

A6.2.4.2. Disconnect the speaker phone on the Conference Room 2 conference table and move to the cell phone cubby. Include the two extension microphones and cords as well. Do not un-tape the power cord from the floor, it may remain in Conference Room 2.

A6.2.4.3. Disconnect the phone from the wall jack near the rear door and move to the cell phone cubby.

A6.2.4.4. Disconnect the speaker phone receiver on the table in the projection room and move to the cell phone cubby.

A6.2.4.5. Unplug the cord to the landline phone on the wall in the projection room.

A6.2.5. Purge Conference Room 2 of personnel, identify unknown devices, and search for anomalies: Look under each chair, table, or other furniture item as you go. Look behind, under, over, and inside each picture, monitor screen, speaker, curtain, flag, wastebasket, etc. Pick up and look at the bottoms and inside of decorative plants, baskets, and any other item. Look for any object that is not normally there, or otherwise appears out of the ordinary. Look for any holes or anomalies in the floors, walls, ceilings, vents, phone jack, thermostat and everything else.

A6.2.5.1. Starting at the rear door, ensure Conference Room 2 is cleared of personnel.

A6.2.5.2. Proceeding clockwise around the room, scan each wall from bottom to top about 3 feet at a time. Check each item (picture, monitor, vent, etc.). Be careful as some of these items are heavy. Avoid injury, avoid damaging the items. Do not disgrace flags.

A6.2.5.3. Carefully inspect the podium. Remove to the cell phone cubby all objects not required for the meeting.

A6.2.5.4. Scan the ceiling by each row of tiles from one end of the room to the other.

A6.2.5.5. Scan the floor from wall to wall about 3 feet at a time. Start at the blue curtain and go all the way to the other end of Conference Room 2.

A6.2.5.6. Report any findings to AFOSI, 777-1852. Secure the area. Terminate the meeting.

A6.2.6. Purge the projection room of personnel, identify unknown devices, search for anomalies by the same techniques as Conference Room 2.

A6.2.7. Check Room 6 and require personnel to depart outside of the double glass doors. If possible, provide an estimated time they will be allowed to return.

A6.2.8. Check Conference Room 1. If Conference Room 1 is being used, implement compensatory measures provided in **paragraph A6.2.14** below.

A6.2.9. Check the blower room and require personnel to depart outside of the double glass doors.

A6.2.10. Check the storage room and require personnel to depart outside of the double glass doors.

A6.2.11. Check the female restroom and require personnel to depart outside the double glass doors.

A6.2.12. Check the male restroom and require personnel to depart outside the double glass doors.

A6.2.13. Establish an entry control point at the double glass doors.

A6.2.13.1. The entry controller must have appropriate eligibility, access, and is listed on the visit request. The entry controller must have in their possession the special security instructions for this post.

A6.2.13.2. From the point in time the classified portion of the Conference Room 2 meeting starts until the classified portion of the Conference Room 2 meeting is terminated, the entire area from the double glass doors through the West stairway must be kept clear of personnel who do not have authorized access. This is to provide for acoustic control of classified meetings in Conference Room 2.

A6.2.14. Compensatory measures when Conference room 1 is in use:

A6.2.14.1. The entry controller must establish the entry control point at the Conference Room 2 door.

A6.2.14.2. The entry controller must control entry to projection room.

A6.2.14.3. The entry controller must ensure the projection room door remains closed/locked until the classified portion of the meeting is terminated.

A6.2.14.4. The entry controller must ensure personnel do not linger in the hallway.

A6.2.14.5. Follow all other instructions except as deviated in this paragraph.

A6.3. During the Meeting.

A6.3.1. Rear door must be locked from inside Conference Room 2 at the start of the classified portion of the meeting and remain locked until the classified portion is terminated.

A6.3.2. Rear door guard must remain on post until notified the classified portion of the meeting is terminated.

A6.3.2.1. Prevent unauthorized personnel from approaching the rear door.

A6.3.2.2. Provide acoustic security by ensuring personnel do not linger in the West stairway. Patrol the West stairway to the extent it is possible to do so and ensure no one is attempting to approach the rear door.

A6.3.2.3. Refer personnel to go around to the entry control point for access. Exception: The rear door guard may grant access to XWZ/CC, CV, CS and CCE. Before each meeting the rear door guard must check that each of these individuals has not been dropped from the visit request. The rear door guard must know the personnel assigned to these positions by personal recognition.

A6.3.3. Entry controller must remain on post until the classified portion of the meeting is terminated.

A6.3.3.1. Control entry by assuring attendees are listed on the visit request (or other appropriate access roster). This includes reentry when personnel exit past the entry control point during breaks, etc.

A6.3.3.2. Personal baggage (backpack, briefcase, purse, etc.) will not be allowed past the double glass doors. Recommend to attendees that they return personal baggage to their vehicles. The entry controller must not attempt to hold or monitor personal baggage for attendees. Unattended personal baggage is not acceptable as it will trigger a suspicious package incident.

A6.3.3.3. Electronic devices (cell phone, smartwatch, personal digital assistant, Blackberry, laptop, tablet, radio, recorder, camera, etc.) that can record, store, or transmit sound, images, electronic files, or data are not permitted past the cell phone cubby. Attendees leave such items in the cell phone cubby at their own risk. The entry controller must not be held accountable for electronic devices left in the cell phone cubby.

A6.3.3.4. Lock the Conference Room 2 door knob from the inside, shut the door.

A6.3.4. Hosts and briefers must provide attendees the following reminders prior to the beginning of each classified portion of meetings:

A6.3.4.1. Remove electronic devices to the cell phone cubby.

A6.3.4.2. Highest classification level for the particular portion of the meeting.

A6.3.4.3. Note taking is not authorized. Make arrangements with briefers to transmit classified information through appropriate channels.

A6.3.4.4. Once the classified portion of the meeting is terminated, Conference Room 2 is no longer secured for classified discussion. Do not discuss classified information once the classified portion of the meeting is terminated.

A6.3.4.5. Unlock the Conference Room 2 door knob, open door, notify entry controller the classified portion of the meeting is terminated.

A6.4. After the Meeting.

A6.4.1. Close the right cell phone cubby door and open the left door halfway so the sign “Please Don’t Forget Your Electronic Devices” is visible as attendees exit towards the double glass doors.

A6.4.2. Notify personnel waiting outside of the double glass doors they may enter the meeting area for unclassified portions of the meeting.

A6.4.3. Unlock the rear roor.

A6.4.4. Notify the rear door guard the meeting is over.

Figure A6.1. Meeting Area Diagram.

A6.5. Rear Door Guard Special Security Instructions (SSI).

A6.5.1. OVERVIEW. This SSI is directive in nature. Your duties and responsibilities as rear door guard are outlined within. Review and familiarize yourself with this SSI. Resolve uncertainties and questions before assuming post by contacting your supervisor, the entry controller, or the SS, 586-7333.

A6.5.2. BACKGROUND. A classified meeting is being held in Conference Room 2. Only those personnel who have a valid security eligibility, need-to-know, and signed NDA are authorized to attend. Unauthorized personnel must be prevented from entering through the rear door of Conference Room 2. Unauthorized personnel must be denied the opportunity to listen to classified information from the West stairway.

A6.5.3. REQUIRED EQUIPMENT. CAC, Building 1102 Conference Room 2 Classified Meeting Plan, Rear Door Guard SSI.

A6.5.4. UNAUTHORIZED. Do not allow friends/coworkers to loiter in the area or distract you from your duties. Do not have cell phone, PDA, Blackberry, laptop, radio, tape recorder, cameras, etc., that can transmit, record, or store information/data. Do not have books, games, or anything that could distract you from your duties.

A6.5.5. POST LIMITS. Remain within the West stairway.

A6.5.6. DUTIES AND RESPONSIBLITIES.

A6.5.6.1. Assume post before Conference Room 2 and surrounding areas are purged.

A6.5.6.2. Grant access via the rear door to OO-ALC/CC, CV, CA, CS, and CCE. You must be capable of visually recognizing these five individuals before assuming this post. You must verify these five individuals are listed on the visit request just prior to assuming post. Remind these personnel to not bring electronic devices into Conference Room 2 during the classified portion of the meeting.

A6.5.6.3. Ensure the rear door is locked during classified meetings in Conference Room 2.

A6.5.6.4. Prevent unauthorized personnel from approaching the rear door during classified meetings in Conference Room 2.

A6.5.6.5. Provide acoustic security by ensuring personnel do not linger in the West stairway. Patrol the West stairway to the extent it is possible to do so while continuing to ensure no one is attempting to approach the rear door.

A6.5.6.6. Refer personnel to go around to the entry control point for access.

A6.5.6.7. Sound the alarm by any means possible in cases where personnel disobey instructions to depart or appear to be attempting to gain access to classified information. Since no communication devices are authorized, you may have to make verbal notice via a loud voice through the rear door or the back door to the command section offices.

A6.5.6.8. Report any suspicious situation to the SS, Security Forces, and/or AFOSI as soon as possible.

A6.5.6.9. Remain on post until notified the classified portion of the meeting is terminated or you are relieved by a qualified substitute. In emergencies you will need to decide when it is appropriate to leave your post, based on a danger or threat to your health or life.

A6.6. Entry Controller Special Security Instructions (SSI).

A6.6.1. OVERVIEW. This SSI is directive in nature. Your duties and responsibilities as entry controller are outlined within. Review and familiarize yourself with this SSI and the Building 1102 Conference Room 2 Classified Meeting Plan. Resolve uncertainties and questions before assuming post by contacting your supervisor or the SS, 586-7333.

A6.6.2. BACKGROUND. A classified meeting is being held in Conference Room 2. Only those personnel who have a valid security eligibility, need-to-know, and signed NDA are authorized to attend. Unauthorized personnel must be prevented from entering Conference Room 2. Unauthorized personnel must be denied the opportunity to listen to or otherwise observe classified information from the hallway. To accomplish this, you must secure the area from the rear door to the double glass doors.

A6.6.3. REQUIRED EQUIPMENT. CAC, Building 1102 Conference Room 2 Classified Meeting Plan, Entry Controller SSI, visit request (and/or other appropriate access list).

A6.6.4. UNAUTHORIZED. Do not allow friends/coworkers to loiter in the area or distract you from your duties. Do not have cell phone, PDA, Blackberry, laptop, radio, tape recorder, cameras, etc., that can transmit, record, or store information/data. Do not have books, games, or anything that could distract you from your duties.

A6.6.5. POST LIMITS. Remain within the area between the rear door and the double glass doors.

A6.6.6. DUTIES AND RESPONSIBILITIES.

A6.6.6.1. Ensure the rear door guard post is manned.

A6.6.6.2. Assume your post.

A6.6.6.3. Purge the meeting area of personnel, electronic devices, and suspected listening devices in accordance with the Building 1102 Conference Room 2 Classified Meeting Plan, **paragraph 2**, and all subparagraphs.

A6.6.6.4. When Conference Room 1 is in use, implement compensatory measures identified in **paragraph A6.7** below.

A6.6.6.5. Establish entry control point at the double glass doors (or the Conference Room 2 door when compensatory measures are implemented).

A6.6.6.5.1. Using attendee's CAC, verify identity.

A6.6.6.5.2. Verify attendee is listed on the visit request (or other access list in accordance with the Conference Room 1 meeting plan). Grant access as appropriate.

A6.6.6.5.3. Deny Access to personnel who are not listed on the visit request (or other appropriate access roster). When possible, refer the denied person to a qualified SS. The SS should verify need to know with the meeting POC, host, or briefer. The SS must verify eligibility and access via the DoD System of Record. If appropriate, the SS should then add the person as an attendee on the visit request (or other appropriate access roster).

A6.6.6.6. Sound the alarm by any means possible in cases where personnel disobey instructions to depart or appear to be attempting to gain access to classified information.

A6.6.6.7. Report any suspicious situation to the SS, Security Forces, and/or AFOSI as soon as possible.

A6.6.6.8. Follow instructions provided in the Building 1102 Conference room 2 Classified Meeting Plan. Notify your supervisor in any case not covered by instruction.

A6.6.6.9. Remain on post until notified the classified portion of the meeting is terminated or you are relieved by a qualified substitute. In emergencies you will need to decide when it is appropriate to leave your post, based on a danger or threat to your health or life.

A6.6.6.10. Notify the rear door guard when the classified portion of the meeting is terminated.

A6.7. Compensatory Measures When Conference Room Is In Use.

A6.7.1. The entry controller must establish the entry control point at Conference Room 2 Door.

A6.7.2. The entry controller must control entry to the projection room.

A6.7.3. The entry controller must ensure the projection room door remains closed until the classified portion of the meeting is terminated.

A6.7.4. The entry controller must ensure personnel do not linger in the hallway.

A6.7.5. Follow all other instructions except as deviated in this paragraph.