

**BY ORDER OF THE COMMANDER  
1ST SPECIAL OPERATIONS WING  
(1 SOW)**



**AIR FORCE INSTRUCTION 31-401  
HURLBURTFIELD  
Supplement**

**21 SEPTEMBER 2010  
Certified Current 2 October 2014  
Security**

**INFORMATION SECURITY  
PROGRAM MANAGEMENT**

---

**COMPLIANCE WITH THIS PUBLICATION IS MANDATORY**

---

**ACCESSIBILITY:** Publication and forms are available on the e-Publishing website at <http://www.e-publishing.af.mil/>.

**RELEASABILITY:** There are no releasability restrictions on this publication.

---

OPR: 1 SOW/IP  
Supersedes: AFI31-401\_  
HURLBURTFIELD  
SUP1, 1 July 2006

Certified by: 1 SOW/IP  
(Mr. Patrick T. Cooper)  
Pages: 42

---

**AFI31-401, 1 November 2005 is supplemented as follows:**

This supplement establishes procedures for protecting classified national security and sensitive unclassified information (regardless of its classification, sensitivity, physical form, media or characteristics) at Hurlburt Field. It assigns responsibility for implementing and managing the Information Security Program in accordance with Air Force Policy Directive (AFPD) 31-4, *Information Security* and Air Force Instruction (AFI) 31-401, *Information Security Program Management*. It applies to all activities assigned at Hurlburt Field unless stated otherwise in the installation support agreement. Ensure that all records created as a result of processes prescribed in this publication are maintained in accordance with Air Force Manual (AFMAN) 33-363, *Management of Records*, and disposed of in accordance with Air Force Records Information Management System (AFRIMS) Records Disposition Schedule (RDS) located at <https://www.my.af.mil/gcss-af61a/afrims/afrims/>. The use of the name or mark of any specific manufacturer, commercial product, commodity, or service in this publication does not imply endorsement by the Air Force.

**SUMMARY OF CHANGES**

This supplement reflects new and revised requirements for management of the Information Security Program. Changes include those necessary to conform/realign with changes to DoD, Air Force, and MAJCOM policy changes for program management. Other administrative and operational in nature changes include; the contents of the Security Manager's Handbook,

clarification for the release of information to foreign nationals, access to classified by historical researchers, non-punitive Information Security Program Review procedures, change from semi-annual self inspection to annual, coordination of classification challenges, coordination requirements for security classification guides, marking, accountability, sanitizing and destruction of removable media (flash, jump and thumb-drives), construction standards for Secure Conference Facilities, required contents of Top Secret Control Account Log, Foreign participation in classified and unclassified meetings, the requirement to secure single drawer GSA containers, and reporting requirements for of Classified Message Incidents (CMI). This publication does not apply to Air Force Reserve Command (AFRC) Units or the Air National Guard (ANG). Refer recommended changes and questions about this publication to the Office of Primary Responsibility (OPR) using the AF Form 847, *Recommendation for Change of Publication*; route AF Form 847s from the field through Major Command (MAJCOM) publications/forms managers. Ensure that all records created as a result of processes prescribed in this publication are maintained in accordance with AFMAN 33-363, and disposed of in accordance with Air Force Records Information Management System (AFRIMS), and Records Disposition Schedule (RDS) located on the Air Force Portal at <https://www.my.af.mil/gcss-af61a/afrims/afrims/rims.cfm/>.

1.3.4. The 1st Special Operations Wing Information Protection Chief (1 SOW/IP) is designated as the Hurlburt Field, Information Security Program Manager (ISPM). The ISPM has oversight and management control of the Information Security Program on Hurlburt Field, including all associate and tenant organizations. The 1 SOW/IPI Branch, implements the Information Security Program on behalf of the ISPM. Route all material requiring ISPM coordination or signature through 1 SOW/IPI to the 1 SOW/IP.

1.3.4.5. The ISPM conducts security manager meetings quarterly or as needed.

1.3.4.5.1. All 1 SOW organizations, associates and tenants are required to have representation at all security managers meetings.

1.3.5.1. (Added) Unit Commanders or Equivalents appoint a primary and at least one alternate security manager. To ensure program success and continuity, it is recommended that personnel appointed have two years retainability and are not assigned to a highly deployable Unit Type Code. Forward a copy of appointment letters to the 1 SOW/IP, Information Security Branch (1 SOW/IPI). The following information is required on the security manager appointment letter: full name, SSN, grade, organization, office symbol, duty phone, complete mailing address, fax number, e-mail address **Attachment 8**. On the appointment letter, indicate previous (*formal*) security manager training and where the training was completed if applicable. The appointment letter template is available on the 1 SOW Information Protection share-point page at [https://eis.afsoc.af.mil/sites/1SOW\\_IP/default.aspx](https://eis.afsoc.af.mil/sites/1SOW_IP/default.aspx).

1.3.5.4. (Added) Commanders grant SMs the authority and access at all unit levels to resolve or work security-related issues, as necessary.

1.3.5.5. (Added) The appointment of additional Office/Section Security Managers (OSM/SSMs) is encouraged to assist the security manager based on unit's size, number of security containers, open storage areas and organization's physical layout.

1.3.6.1. Attachment 9 , Security Managers Duties and Responsibilities, list duties beyond those listed in AFI 31-401, *Information Security Program Management*.

1.3.6.2. Internal Operating Instructions (OI) will at a minimum address the following areas; SMs duties and responsibilities, in processing, security education and training (initial, annul/refresher, foreign travel and termination briefings), safe custodian duties, derivative classification process, marking, safeguarding classified in the office, transmission and transportation of classified, classified container(s) location(s), end of day checks and security incident procedures. A sample unit OI is available on the 1 SOW Information Protection share-point page at [https://eis.afsoc.af.mil/sites/ISOW\\_IP/default.aspx](https://eis.afsoc.af.mil/sites/ISOW_IP/default.aspx).

1.3.6.4. Security managers or alternates must attend mandatory Quarterly Security Manager Meetings. DoD contractors are encouraged to attend as well, but shall not represent an Air Force organization.

1.3.6.4.1. (Added) The SM will maintain a list of all unit classified networked and stand alone accredited automated information system AIS equipment (to include the serial numbers of each item) in the security manager's handbook.

1.3.6.10.1. Cleared contractor personnel working in the unit will be in and out-processed, and establish a servicing relationship in JPAS.

1.3.8. Forward requests for release of information to foreign nationals or their representatives to the servicing Foreign Disclosure Office (FDO).

1.3.9. The 1 SOW History Office will coordinate and forward requests for researcher access.

1.4.2. ISPM will forward Information Security Program Review reports to Commanders and Equivalents. Commanders and Equivalents ensure corrective actions are provided to 1 SOW/IPI by the report corrective actions suspense date.

1.4.2.1. (Added) 1 SOW/IPI will conduct out of cycle non-punitive Information Security Program Reviews (ISPR) of units, staff agencies and directorates on Hurlburt Field when two or more incidents occur in 30 days. The ISPR will examine only the areas affected/involved by the incident(s) and provide viable solutions and training to preclude future like incidents.

1.4.2.2. (Added) 1 SOW/IPI will conduct non-punitive ISPR of units, staff agencies and directorates on Hurlburt Field at commanders' and equivalents request. Request will be based on the recurrence of security incidents (two or more) involving an official classified approved process within 60 days. The ISPR will examine only the areas affected/involved by the incident(s) and provide viable solutions and training to preclude future like incidents.

1.4.3. Unit Information Security Self-inspections are conducted in January of each year. The ISPM will allow the annual program review to replace one of the semiannual self-inspections. A responsible person, other than SMs, performs these inspections (military member or government civilian assigned to the unit). Use the applicable Hurlburt Field Checklists, e.g. information, industrial or personnel security checklists. Unit commander must endorse self-inspection reports and ensure Hurlburt Field Form 191, *Discrepancy Reports*, are prepared for each discrepancy. Discrepancies must also be provided to the unit SI monitor for tracking. Submit a copy of the completed self-inspection report and HF Form 191s to 1 SOW/IPI by 5 February of each year. Discrepancies must be corrected and documented on HF Form 191s. Submit closed HF Form 191s to 1 SOW/IPI within 45 days of the inspection.

1.4.3.1. The applicable self-inspection checklist and Self-Inspection Guide are available on the 1 SOW Information Protection share-point page at [https://eis.afsoc.af.mil/sites/1SOW\\_IP/default.aspx](https://eis.afsoc.af.mil/sites/1SOW_IP/default.aspx).

1.5.1.2.1. At Hurlburt the CNWDI approving officials for briefings and access are listed in Table 1.5.

**Table 1.5. (Added) CNWDI Approving/Briefing Officials.**

HQ AFSOC	1 SOW
AFSOC/IP - Director of Information Protection	1 SOW/IP - Chief of Information Protection
AFSOC/A7XD - Command Explosive Ordnance Disposal Manager	1 SOCES/CC – Commander

1.5.2.3. (Added) The ISPM provides policy, guidance and oversees the installation North Atlantic Organization (NATO) safeguarding program. AFSOC/A6OK maintains and has management oversight of the local subregistry.

1.5.3. 1 SOW/IPI is responsible for FOUO training materials available on the 1 SOW Information Protection share-point page at [https://eis.afsoc.af.mil/sites/1SOW\\_IP/default.aspx](https://eis.afsoc.af.mil/sites/1SOW_IP/default.aspx).

1.5.6. (Added) 1 SOW/XP is responsible for in-brief access to FOCAL POINT.

1.6.1. Coordinate request for waivers through 1 SOW/IPI to ISPM. Use AF Form 1768, *Staff Summary Sheet*, with supporting documentation to document all deviations. Consolidate multiple deviations caused by a single deficiency on one AF Form 1768.

1.6.1.1. (Added) The responsible activity must implement supplemental controls/compensatory measures for all temporary and permanent deviations. Activities may not use blanket waivers for several different deficiencies.

1.6.1.2. (Added) The responsible/owning activity commander or two letter staff agency chief signs the AF Form 1768 and submits the request to the servicing ISPM. The ISPM forwards request through ISPM command IP channels to SAF/AAP for approval/disapproval.

1.7.1. 1 SOW units, associates and tenants as instructed by their MAJCOM or DRU submit quarterly Standard Form 311, *Agency Information Security Program Data*, to 1 SOW/IPI by 5 Dec, 5 Mar, 5 Jun and 5 Sep of each fiscal year. Those tenant units not reporting to the 1 SOW/IP will send their SF 311 directly to their respective MAJCOMs by their suspense date. Standard Form 311, tally sheets and instructions are available on 1 SOW Information Protection share-point page at [https://eis.afsoc.af.mil/sites/1SOW\\_IP/default.aspx](https://eis.afsoc.af.mil/sites/1SOW_IP/default.aspx).

1.7.1.2. (Added) If tenant units respective MAJCOMs have supplemented AFI 31-401, paragraph 1.7.1., to have the Host ISPM receive the SF 311, then coordinate with 1 SOW/IPI and forward the SF 311.

2.5.1. Send classification challenges through the ISPM. SM records challenges, preserves anonymity of challenger when requested, processes challenge within 72 hours of receipt. Challenges will be documented in writing via the “Notification of Improperly Marked Document” MFR template **Attachment 10** and forwarded to 1 SOW/IPI. The ISPM ensures

follow-up and review with OCA is accomplished within 60 days. Send 1 SOW/IPI all damage assessment results.

2.5.2. Coordinate challenges of Non-Air Force classified material through the ISPM. The ISPM forwards challenges through ISPM command IP channels to SAF/AAP for action.

2.6. Security Classification/Declassification Guides. Coordinate publishing of Security Classification Guides (SCG) through 1 SOW/IPI. Submit an original hard copy and two copies of DD Form 2024, *Security Classification Guide Data Elements, DOD*, and a copy of the SCG to 1 SOW/IPI. Units must obtain and maintain applicable SCGs for their programs and systems. Units are also responsible for providing applicable SCG to contractor personnel. See **Attachment 11** for particulars on development and coordination of SCGs. Sample guides are available on the 1 SOW Information Protection share-point page at [https://eis.afsoc.af.mil/sites/1SOW\\_IP/default.aspx](https://eis.afsoc.af.mil/sites/1SOW_IP/default.aspx).

2.6.2.1. SCGs may be issued only by the OCA that originally classified the information and who has jurisdiction and control of the classified information.

3.6.1. (Added) During Command Clean Out all units will use the “Hurlburt Classified Review” checklist and submit a report of findings/results to the 1 SOW/IPI. Checklist and report template are available on the 1 SOW Information Protection share-point page at [https://eis.afsoc.af.mil/sites/1SOW\\_IP/default.aspx](https://eis.afsoc.af.mil/sites/1SOW_IP/default.aspx).

4.2.10. (Added) Single Page Documents. Single page documents shall be page marked on the front and back for easy identification. Holders must notify originator of improperly marked documents in writing, or record with a memo any telephonic notification. Notification must be kept with the document.

4.2.11. (Added) Use a classified addendum whenever classified information constitutes a small portion of an otherwise unclassified document. Separate and store the classified.

4.2.12. (Added) Bound documents, including binders (1/2 inch or greater) will also be marked on the spines with highest level of classification.

4.5.4. (Added) File US collateral, Focal Point, NATO and Critical Nuclear Weapons Design Information (CNWDI) classified material separated by guide cards for each record group, or in separate container drawers. Unclassified material should be stored separately from classified whenever possible.

4.8. Removable Information Systems Storage Media. Annotate on Standard Form 711, *Data Descriptor (Label)*, or locally devised label, the following: Classified By or Derived From, Reason for Classification and Declassify On. See Executive Order (EO) 12958, *Classified National Security Information*, DoD 5200.1-PH, *DoD Guide to Marking Classified Documents*.

4.8.1. Procedures for the permanent marking of thumb drives and any other removable storage media will be addressed in unit’s security operating instructions. When such devices are no longer needed or malfunction, they will be destroyed in accordance with AFSSI 8580 *Remanence Security*, Table 6-2, Destroying Media. Presently these types of devices are not allowed for classified use.

4.8.4. (Added) Flash, Thumb or Jump Drives; when used/maintained an accountability log will be kept in the security container that houses these removable media devices when and if they are to be used for storing classified material. All classified removable media will be marked with

the highest classification stored to include unclassified items within a security container or Secure Room/Open Storage Area.

4.8.4.1. (Added) For use in classified information systems (IS).

4.8.4.1.1. (Added) These devices must be clearly marked with decals, tags or labels, indicating the highest level of classification on the device. Classified labels, SF 707, *Secret (Label)*; SF 708, *Confidential (Label)*; SF 710, *Unclassified (Label)*, may be too large for most devices, if this is the case use a colored permanent ink, which is the same color as the label, for marking. Ensure accountability procedures are outline in the unit OI; due to the size of these devices they can be easily overlooked in a physical security check of classified areas.

4.8.4.2. (Added) Sanitizing these devices in accordance with AFSSI 8580, Table 4-1, Sanitizing Media. These devices will be mark and controlled at its original classification level until destroyed.

4.8.4.2.1. (Added) Store the devices in an approved security container until a certified sanitizing program is available to allow recycling of the devices or process them for destruction.

4.12. (Added) Special Types of Materials. All electronic media (for example, slides, transparencies, photographs, maps, and charts) will be marked consistent with DoD 5200.1-R, Section 4. All information contained within will be portion marked. If slides are not portion marked, their classifications will be recorded in the "Notes Pages" of the power point slide presentation, along with the overall markings present on each briefing slide.

5.3. Nondisclosure Agreement (NdA). Provide a copy of the completed SF 312, *Classified Information Nondisclosure Agreement*, to the individual upon request. Once the Nondisclosure is recorded in JPAS and mailed to the respective agency there is no requirement to maintain a local file copy of the SF 312.

5.3.1.4. 1 SOFSS/DPCO, Hurlburt Field, FL 32544.

5.3.1.5. 1 SOW/IPI will maintain the SF 312, IAW the Air Force *Records Disposition Schedule*.

5.4.1.4. 1 SOW/IPI will maintain the AF Form 2587, *Security Termination Statement*, within the approval package file.

5.5.1. Security managers prepare visit request for duration of visit, for the minimum amount of time necessary not to exceed one year via JPAS.

5.8. Administrative Controls. Controls for Top Secret Control Account establishment and maintenance are listed in Hurlburt Field Handbook for Top Secret Control Officer, available on the 1 SOW Information Protection share-point page at [https://eis.afsoc.af.mil/sites/1SOW\\_IP/default.aspx](https://eis.afsoc.af.mil/sites/1SOW_IP/default.aspx).

5.8.1.1. Provide a copy of the Top Secret Control Officer (TSCO) appointment memorandum to the servicing ISPM. ISPMs provide training to newly appointed TSCOs on request. Send written notice of TSCA establishments and closures to 1 SOW/IPI. Upon receipt, 1 SOW/IPI will schedule TSCO training and use the information to annually publish and distribute a roster of TSCAs that lists primary and alternate TSCOs. TSCOs will keep a copy of the current roster and use it to verify information concerning the local TSCAs and TSCOs. Contractor employees cannot be a TSCO for government units.

5.8.1.2.3. (Added) Remove the AF Form 144, *Top Secret Access Record and Cover Sheet* when Top Secret (TS) material is destroyed, downgraded or declassified and retain it with the inactive records IAW the AFRIMS. If the TS material is transferred to another TSCA, send the AF Form 144 with the material.

5.8.1.3.1. Conduct annual inventory by 31 December each year. Do not inventory material received or with disposition entries after 31 December. The incoming TSCO may conduct the inventory prior to assuming responsibility for the TSCA. Only contractor employees who work with the TSCA are authorized to conduct the inventory for a government organization. Provide a copy of the annual inventory report to the servicing ISPM by 15 January.

5.8.1.7. (Added) TSCA Records Maintenance. The TSCO will maintain a TS Control Log consisting of the following records:

5.8.1.7.1. Letter establishing the TSCA.

5.8.1.7.2. Appointment record for primary and each alternate TSCO.

5.8.1.7.3. Copy of the TSCO Roster (listing of TSCAs/TSCOs on base)

5.8.1.7.4. Active records. AF Form 143, *Top Secret Register Page*, to document receipt of TS documents or material and to show change actions performed.

5.8.1.7.5. Inactive records. AF Form 143 to document final action taken to dispose of the TS documents or material by transfer or destruction. - The last annual inventory report.

5.8.1.8. (Added) Recontrolling. When register pages contain active and inactive entries, the TSCO uses recontrolling procedures to close the inactive entries and transfer the active entries to a new register page in the next calendar year. Recontrolling actions are completed by the end of December. To close a register page that contains active and inactive entries, transfer active entries to a new form/year in the current year register and enter a recontrolling remark (to and from) in item 12f of the previous register page and item 15 on the new register page. No further action or documentation is required on inactive register page.

5.8.6. (Added) Develop plans for the protection, removal, or destruction of classified material in case of natural disaster, fire, civil disturbance, terrorist activities, or enemy action. (DoD 5200.1-R, *Information Security Program*, paragraph 6-303). Include in your unit operating instruction.

5.9.1. To provide security-in-depth and reduce or prevent inadvertent access to classified information, *Classified Work in Progress*, signs will be posted in a conspicuous manner when processing such information in normal office settings. Additionally, precautions must be taken when working with classified information such as securing office doors and notifying or announcing classified work is in progress to fellow office workers to heighten their awareness.

5.10. End-of-Day Security Checks. End of day checks will be annotated on the SF 702, *Security Container Checksheet*, as well as the SF 701, *Activity Security Checklist*, in the "Checked By" column for all classified storage containers and open storage areas/secure rooms. Unit Commanders and equivalents shall establish procedures for end of the day security checks, and document them in their unit OI. Procedures will address properly securing all areas which process classified information. Additionally, an SF 702, *Security Container Check Sheet*, shall be utilized to record that classified vaults, secure rooms (strong rooms), and containers have been properly secured at the end of the day. The SF 701 and 702 shall be annotated to reflect after hours, weekend, and holiday activities in secure areas.

5.10.1. (Added) Include on the SF 701 (if applicable): Check all classified computers to ensure that the hard drive has been removed and locked in a GSA approved container. Check all Global Command and Control System (GCCS)/SIPRNET connections to ensure they have been disconnected and properly secured.

5.12.1. The 1st Special Operation Wing Installation Control Center, building 90208, is designated as “classified transit storage” up to and including Top Secret material. The 1st Special Operations Logistics Readiness Squadron, Material Storage and Distribution Flight, is designated as “transit storage” for bulk-storage material up to and including Secret. For HQ AFSOC personnel, the HQ AFSOC/COD is designated as “transit storage” for up to and including Top Secret in Bldg 90069.

5.13. Classified Meetings and Conferences. This section does not apply to local, routine meetings where classified briefings and discussions take place, such as wing or unit level staff meetings. However, the host of such meetings is responsible for ensuring appropriate security measures are in place to properly control access and protect national security information. Use classified briefing checklist (AFI 31-401, 20 June 2008, AFSOC Sup 1, **Attachment 8** and classified briefing lead in slide **Attachment 12**.

5.13.1. For classified meetings, conferences and symposiums the OPR will complete and submit a security plan to the 1 SOW/IP 10 days prior (see Hurlburt Field Classified Conference Handbook at [https://eis.afsoc.af.mil/sites/1SOW\\_IP/default.aspx](https://eis.afsoc.af.mil/sites/1SOW_IP/default.aspx). The OPR and briefer responsible for approving the use of telephones, radios, tape recorders or any device that can transmit or record within rooms/areas used for classified meetings, during such meetings. The facility used must afford adequate security against unauthorized access, from both physical intruders and sound emissions. Entry control and perimeter surveillance will be established by posting personnel from the sponsoring activity in and around the room or facility, as necessary. **Note:** The ISPM is not responsible for this function, but will assist in the review/approval of unit security plans.

5.13.2. The ISPM approves secure conference facilities. Appoint a Government Security Manager for meetings, conferences, seminars, and other meeting activities and for physical security of actual site of each classified function. Contractors may be appointed to assist security managers, but they cannot act as security managers for government sponsored meetings.

5.13.2.1. (Added) Facility Approval Authority. Secure conference facilities are not required when conducting classified meetings or conferences on government installations.

5.13.2.2. (Added) Organizations will notify the 1 SOW/IP, in writing, of all secure conference facility requirements (new/upgrade construction). 1 SOW/IP and 1 SOCES personnel will inspect all new and modified secure conference facilities to ensure security requirements and construction standards are met IAW **Attachment 13**. Results of the inspection will be documented in writing and maintained in the official records repository. The 1 SOW/IP certifies secure conference facilities in writing. The requesting organization maintains the original certification package, 1 SOW/IP will maintain a copy as well.

5.13.2.3. (Added) Proposed structural modifications to secure conference facilities must be coordinated with the 1 SOW/IP and 1 SOCES. The 1 SOW/IP and 1 SOCES must recertify, in writing, the structural integrity of secure conference facilities that have been modified.

5.13.3. Foreign participation in classified or unclassified meetings and conferences will take place only after approval from the servicing FDO.

5.13.4. (Added) Cellular phones, two-way radios, two-way beepers, and other electronic equipment that can receive and transmit a signal are prohibited in all offices and areas where classified and sensitive information may be discussed or processed. Staff directors and commanders will determine which work areas are affected and implement this requirement accordingly. Owners of designated areas should make every effort to inform personnel of the prohibited use of electronic equipment, to include but not limited to posting signs and visual aids, and including the information in briefings and training, etc. For further guidance refer to AFSOI 33-202, *Portable Electronic Device (PED) Security*.

5.14.2.4. (Added) If the facility does not meet the requirements of an open storage area/room then U.S. cleared personnel must provide continuous surveillance over all classified material when present.

5.15.1. Each individual unit Information Assurance Officer (IAO) approves equipment used to reproduce classified material. IAOs use checklist at [Attachment 15](#) for reproduction approval. For analog copiers, run at least two blank sheets through the copier to remove latent images. Digital copiers with hard drives are not authorized for reproduction of classified, FOUO and Privacy Act information at Hurlburt. Post reproduction rules or locally produced visual aid. Prohibit classified reproduction by posting computer generated sign, *STOP Do Not Use This Machine For Classified Reproduction STOP*. Ensure signs or visual aids are conspicuously placed on machine. Examples of reproduction equipment include copiers, fax machine, multi-function printer, copier, fax and scanner, etc. Post the completed Hurlburt Field Form 2, *Classified Copying Equipment Approval*, on or near the approved reproduction device and submit a copy to the ISPM. Unit or staff agency certification procedures for classified information processing equipment (for example, copiers, and fax machines) will be incorporated into unit security OIs.

5.17.2. The 1 SOW/IPI provides initial and periodic inspections of security containers and training to unit security container custodians on a limited basis. Units are highly encouraged to contact the 1 SOW/IPI office prior to contracting a GSA technician to service or naturalize a container.

5.18.2. The ISPM acts as *Approving Authority* on behalf of the installation commander for secure storage areas. Open storage and secure areas (OSSA's) are synonymous. 1 SOW/IPI is the installation focal point for all non-SCI classified OSSA requests. When the potential need for open storage is initially identified, contact 1 SOW/IPI. Do not start construction of these areas without prior consultation. 1 SOW/IPI ensures coordination with the 1 SOCES. 1 SOW/IPI will coordinate on all work order request for OSSA alarms, X-0 series locks, and for construction or modification of a secure room. Panels controlling fire alarms, mass-notification and fire suppression are not to be placed within secure rooms/classified portion of the facility.

5.18.2.1. (Added) Commanders submit a written request with justification to the 1 SOW/IPI prior to construction of vaults and OSSA. OSSA's are reserved for operational necessity and the storage of items that cannot be easily stored in GSA containers. Operational convenience is not justification.

5.18.2.2. (Added) After reviewing the justification, an initial survey is conducted using DoD 5200.1-R, Appendix “G”. Results of the survey are sent to the commander identifying construction, modification, and other security requirements.

5.18.2.2.1. (Added) Before final approval for open storage is granted, commanders submit written OI detailing security procedures for positive entry control, emergency protection plan, training plan and classified protection in the open storage area. 1 SOW/IPI endorses the OI and forwards the open storage package to the ISPM for approval/certification. Once approved, post approval letter on the inside entrance door of secure room or vault. O SSA approval is revalidated annually as part of the annual Information Security Program Review. Sample OI is available on the 1 SOW Information Protection share-point page at [https://eis.afsoc.af.mil/sites/ISOW\\_IP/default.aspx](https://eis.afsoc.af.mil/sites/ISOW_IP/default.aspx).

5.18.2.3. (Added) Any structural or procedural modification to certified vault or OSSAs requires recertification. Modified OSSAs or vaults approved prior to 1 October 1995 will be required to upgrade to DoD 5200.1-R, Appendix “G “ standards prior to recertification.

5.18.2.4. (Added) Units must develop emergency protection plans (EPP) to protect classified material in safes, OSSAs and vaults. Post plan near safe or O SSA entrance door. Emergency plans incorporate procedures to protect classified in the event of impending natural disasters, civil disturbance, terrorist threats, bomb threats, and Force Protection Conditions. Coordinate EPP's with 1 SOW/IPI for approval. Ensure the plan identifies a priority of destruction and personnel with access are trained on the order of destruction: The priorities for emergency destruction are: Priority One - Top Secret Information, Priority Two - Secret Information, Priority Three - Confidential Information. Deployed units outside CONUS must also have plans, which address protection, removal and destruction while deployed overseas as outlined in DoD 5200.1-R.

5.18.2.5. (Added) Authorization to approve Vaults and OSSAs for the storage of collateral classified material is delegated to the ISPM by the installation commander. If there is a disagreement between the requestor and the ISPM over the need to establish Open Storage, the installation commander will make the final decision.

5.18.2.6. (Added) Post the storage facility approval notices/letters inside the approved area on the pedestrian entry way door.

5.18.3. (Added) GSA–approved field safes and special purpose, one and two drawer, light–weight, security containers, approved by the GSA, are used primarily for storage of classified information in the field and in military platforms, are to be used only for those or similar purposes. Such containers will be securely fastened to the structure or under sufficient surveillance to prevent their theft or compromise.

5.21.2. All personnel possessing the combination to a security container, vault, or secure room, will be listed on SF 700. A continuation sheet may be used, but it must contain all the information required on SF 700. List safe custodian’s name first on the SF 700. Safe custodian is responsible for container(s) serviceability, preventive maintenance and contents.

5.21.4. (Added) Commanders must ensure a unique permanent number and/or office symbol to upper left or right corner on front of container’s frame.

5.21.5. (Added) Security managers must maintain a current listing of all unit security containers and secure rooms, to include all contractor security containers furnished by the government, using **Attachment 14**. Provide a current copy of the inventory report to 1 SOW/IPI. SMs must also ensure safe custodians are adequately trained.

5.21.6. (Added) Before transferring security containers to another unit, setting them aside for later use or turning them in, the SM will inspect them to verify all classified material is removed and standard combination is set (50-25-50). The SM will record written verification of the inspection on a "3x5" card, print name, office symbol, sign and date the card and affix it to the outside of the container. Example statements recorded on the card: " The lock is set on standard combination (50-25-50). The container/vault has been inspected and does not contain classified material."

5.22.4. Commanders must ensure safe custodians are adequately trained on their responsibilities. Contact 1 SOW/IPI for training and certification of custodians. Trained custodians conduct inspections in accordance with Technical Order (TO) 00-20F-2, Inspection and Preventive Maintenance Procedures for Classified Open Storage vaults, and secure rooms. They record inspection results on AFTO Form 36, *Maintenance Record for Security Type Equipment*. Post the form inside the locking drawers or doors, as applicable.

5.22.5. (Added) Security Container Custodians or SMs will pull out/remove all drawers, examine interior for classified material, and remove exterior security container ID markings before transferring to another unit or turned in to Defense Reutilization Marketing Office (DRMO). Annotate transfer using **Attachment 14**. Do not remove AFTO Form 36. Set empty security containers on manufacture shipping combination (25-50-25). Ensure personnel coordinate and report all safe transfers to the Base Locksmith at 884-6192.

5.24.3.1. Hurlburt Field Form 2, *Classified Copying Equipment Approval*, will be posted above or on all copiers, faxes, etc. approved for reproduction of classified material. Hurlburt Field Visual Aid (HFVA) 31-6, *Stop Classified Reproduction Not Authorized Unclassified Reproduction Only*, will be posted above or on all copiers, fax machines, and scanners not approved for reproduction of classified material. See classified copier checklist, **Attachment 15**. Hurlburt Field Form 2 and the classified copier checklist are available on the 1 SOW Information Protection share-point page at [https://eis.afsoc.af.mil/sites/1SOW\\_IP/default.aspx](https://eis.afsoc.af.mil/sites/1SOW_IP/default.aspx).

5.28.1. All shredders and disintegrators procured by units to destroy classified material will be inspected by the SM to ensure the shredder is an authorized model (using the NSA approved shredders or disintegrators listing). All procured shredders must meet or exceed requirements for Top Secret and Classified materials (1/32" x 7/16") and the NSA/CSS 02-01 = 1 x 5 mm as required for all US Government classified documents as of October/2008. Respective commanders will certify unit shredders and disintegrators by signing an MFR indicating the date of inspection, make model, serial number and location of the shredder. The MFR templates for cross cut shredders and optical grinders are available on the 1 SOW Information Protection share-point page at [https://eis.afsoc.af.mil/sites/1SOW\\_IP/default.aspx](https://eis.afsoc.af.mil/sites/1SOW_IP/default.aspx). A copy of the MFR will be posted on the shredder, in the SM's Handbook and a copy sent to the 1 SOW/IPI. Additionally after inspection, conspicuously post a computer generated sign/decal, HFVA 9, *Not Authorized for Destruction of Classified Information*, or HFVA 8, *Authorized for Destruction of Classified Information Visual Aid*, on destruction equipment. Recertification is required for major repair, replacement of blades and cutting devices or decertification by drafting a new

letter. In the event of problems, recommend two cleared personnel be present during destruction of classified information. Use the base central destruction facility, (1 SOCS/SCDPR) 884-6279/3832, for large shredding task or material other than paper. The ISPM will verify all authorized shredders and disintegrators during program reviews.

6.1.7. (Added) After delivery to organizations by the Hurlburt Official Mail Center (OMC) or other courier means, protect all First Class marked “*Return Service Requested*”, Registered and Certified mail, Emory Air Freight, and FEDEX packages addressed to DoD organizations on base as classified until determined otherwise.

6.3.2. Procedures for receipting and safeguarding registered, certified, and first class mail and overnight delivery packages (FedEx, UPS etc..) will be included in unit and staff agency local OIs.

6.7.1.1. Commanders authorize couriers to hand carry classified material within CONUS on all modes of transportation.

6.7.1.1.1. (Added) Hand carrying or Escorting Classified Material Aboard Commercial Passenger Aircraft. Approval authority for escorting or hand carrying classified material outside the US, its territories, and Canada are listed in Table 6.7.1.

**Table 6.7.1. (Added) Approval Authorities.**

HQ AFSOC	1 SOW
Director of Staff	Installation Commander
Directorates	Group Commanders

6.8. Documentation. A Courier Authorization Letter (CAL) is required to hand carry classified in the local area (Escambia, Okaloosa, Walton, and Santa Rosa counties). A DD Form 2501, *Courier Authorization*, may be used in lieu of a CAL if a person hand carries classified regularly in the local area and must be returned to the security manager after each trip. A CAL is required to hand carry classified material beyond local limits, but within CONUS. Use of an Exemption Letter is required when traveling in areas which may require inspections. Authorization for contractors to hand carry classified material must be approved by the sponsoring unit commander. Classified material may be carried between offices on Hurlburt Field with supervisor’s permission. See [Attachment 16](#) and [Attachment 17](#) for CCL and Search Exemption Notice samples.

8.2. Methodology. At Hurlburt, the security manager is responsible for ensuring security training is conducted with all assigned personnel and documented. Accomplish initial security training prior to granting access to classified material (Indoctrination via JPAS is required for all unit personnel as well as contractors prior to access). Classified contractors must be provided the same level of training as well.

8.3.3.1. Security Managers must attend Security Manager Training Course within 90 days of appointment.

8.3.6.6. (Added) Organizations develop an annual training plan tailored to their unit needs. See [Attachment 17](#), [Attachment 18](#), [Attachment 19](#), and [Attachment 20](#) for sample training plan, required initial training subjects, refresher training and specialized training. Commanders or

staff agency chiefs approve the plan by January each year. Security training aids and sample lesson plans are available on the 1 SOW Information Protection share-point page at [https://eis.afsoc.af.mil/sites/1SOW\\_IP/default.aspx](https://eis.afsoc.af.mil/sites/1SOW_IP/default.aspx) as well as the web based training presentations. Security training topics/areas should be broken down quarterly to provide continuous security awareness for personnel who create, process, or handle classified information as well as those who do not routinely handling classified but have access. All cleared and uncleared personnel receive annual security refresher training on the basics of protection of classified material and other topics, as applicable, depending on the organizational mission. This applies to classified contractors as well. The training goal is to train 100% of those personnel who routinely handle and process classified.

8.4.1.1. Ensure a servicing relationship is established with all cleared classified contractors in JPAS during indoctrination.

8.4.1.2. Ensure the training requirements for both cleared and uncleared personnel outlined in this chapter and the AF Information Security Training Standard (available on 1 SOW Information Protection Information share-point page at [https://eis.afsoc.af.mil/sites/1SOW\\_IP/default.aspx](https://eis.afsoc.af.mil/sites/1SOW_IP/default.aspx)) are included in the organization's training plan as required. As a minimum, training documentation must include the trainee's name and grade, type of training (initial, refresher, or specialized), date of training, and a specific list of completed training subjects and tasks.

8.4.2. (Added) Unit and staff agency OIs will outline training responsibilities for supervisors and security managers.

8.6. Original Classification Authorities (OCAs). 1 SOW/IPI will provide training to Original Classification Authorities (OCAs) on request.

8.7. Derivative Classifiers, Security Personnel, and Others. 1 SOW/IPI will assist Security Managers in providing Derivative Classification and Classified Marking training on request. To maximize the training efforts a classroom setting with at least 10 students is required.

9.3.1. (Added) Classified Message Incidents (CMI) will be reported and processed within the following timelines:

9.3.1.1. (Added) The 1 SOW/IP will notify the base-level Network Control Center immediately by the end of the day of discovery of any CMIs.

9.3.1.2. (Added) Appointing Official will appoint an Inquiry Official within 2 days of notification.

9.3.1.3. (Added) Inquiry Official will complete the inquiry within 10 duty days of being briefed by 1 SOW/IPI.

9.3.1.4. (Added) On securing approval from the appointing authority the Inquiry Official will forward the Inquiry Report to 1 SOW/IP. 1 SOW/IPI will complete the technical review within 5 duty days of inquiry close out.

9.3.1.5. (Added) 1 SOW/JA will complete a legal review, if required, within 5 duty days.

9.3.1.6. (Added) The Appointing Official will close the inquiry and forward closing actions to 1 SOW/IPI within 5 duty days of receipt of the technical review.

9.3.1.6.1. (Added) The commander of the subject(s) of all CMI-related security incidents must acknowledge in writing on the Appointing Official's closing action report that a.) the commander has discussed with the subject(s) the findings of the investigation, and b.) appropriate corrective actions have been taken, for example, training and/or disciplinary action. All CMIs resulting in a compromise or possible compromise shall be forwarded to AFSOC/IP via fax or e-mail. Use secure means for classified reports.

9.3.2. (Added) The 1 SOW/IP will forward on going/open CMI security incident and inquiry updates to AFSOC/IP every Monday.

9.8.1. (Added) Non-CMI related security incidents will be processed under the same timelines as **paragraph(s) 9.3.1.2, 9.3.1.3, 9.3.1.4, 9.3.1.5 and 9.3.1.6**

9.8.1. 1 (Added) Unit security OIs will outline procedures to follow on discovery of a security incident. Procedures covered will include; securing the classified information, reporting the incident to the 1 SOW/IPI NLT the end of the discovery day, secure reporting procedures when classified information is unsecured and accessible to uncleared personnel, and appointment of inquiry/investigating officials.

9.8.4. (Added) The 1 SOW/IP must submit the Security Incident Data Report to AFSOC/IP NLT 15 Jan and 15 Jul each year as outlined in AFD 31-4, *Information Security*, para. A2.1.

9.9.1. Contact 1 SOW/IPI for the case number (i.e., Case 09-H-01). 1 SOW/IPI will provide the inquiry official with a briefing, inquiry handbook and security incident tracking sheet. Stamp or mark reports "For Official Use Only." The appointing authorities for a formal investigation are: 1 SOW/CC, 1 SOW/CV or AFSOC/CC and AFSOC/CV. Inquiry officials must be, as a minimum, an impartial Commissioned or Senior Noncommissioned Officer equal to or senior to the person involved. The inquiry or investigation official may not be in the chain of command of any of the persons involved in the incident. The inquiry or investigation official may be appointed from another organization or AFSOC Directorate. Formal investigating officials must complete the investigation and submit a final report as soon as possible but no later than 30 duty days from appointment.

9.9.2. The inquiry official will also determine and document in the inquiry report if the "subject(s) of the inquiry or investigation" has completed all initial and recurring training requirements outlined in **Chapter 8**. Verification must include the date of initial training and all dates of recurring training.

9.10.1.1. (Added) The OCA, upon learning that a compromise or possible compromise of specific classified information has occurred and is reasonably expected to cause damage to national security, shall prepare a written damage assessment. While there are no time limits for completion of the damage assessment, initiate the assessment upon notification and complete without undue delay. The OCA must determine whether the damage assessment itself is classified and mark and process accordingly.

9.10.1.2. (Added) As a minimum, damage assessments contain the identification of the source, date and circumstances of the compromise; classification of the specific information lost or compromised; a description of the specific information lost or compromised; an analysis and statement of the known or probable damage to the national security; an assessment of the possible advantages to foreign powers; an assessment of the original classification decision

regarding the information involved; and an assessment of whether countermeasures are appropriate and feasible to negate or minimize the effect of the compromise.

9.10.2.4. (Added) OCAs must maintain records of damage assessments they prepare in a manner that facilitates their retrieval and use. Dispose of the records IAW the Air Force Records Disposition Schedule. OCAs provide a copy of damage assessments to the 1 SOW/IP for filing with the security incident.

9.12.5. (Added) The 1 SOW/IPI and unit security managers will maintain all security incident reports for two years IAW Air Force Records Disposition Schedule.

9.16. Prescribed and Adopted Forms.

9.16.1. Prescribed Forms. HURLBURTFIELD Form 2, *Classified Copying Equipment Approval*

9.16.2. Adopted Forms. DD Form 254, *Contract Security Classification Specification, Department of Defense*

DD Form 2024, *Security Classification Guide Data Element, DOD*

DD Form 2501, *Courier Authorization*

AF Form 143, *Top Secret Register Page*

AF Form 144, *Top Secret Access Record and Cover Sheet*

AF Form 847, *Recommendation for Change of Publication*

AF Form 1768, *Staff Summary Sheet*

AF Form 2587, *Security Termination Statement*

AFTO Form 36, *Maintenance Record for Security Type Equipment*

SF 311, *Agency Information Security Program Data*

SF 312, *Classified Information Nondisclosure Agreement*

SF 700, *Security Container Information*

SF 701, *Activity Security Checklist*

SF 702, *Security Container Checksheet*

SF 707, *Secret (Label)*

SF 708, *Confidential (Label)*

SF 710, *Unclassified (Label)*

SF 711, *Data Descriptor (Label)*

Hurlburt Field Form 191, *Discrepancy Report*

GREGORY J. LENGYEL, Colonel, USAF  
Commander

**Attachment 1****GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION*****References***

EO 12958, *Classified National Security Information*, April 17, 1995

DoD 5200.1-H, *Department of Defense Handbook for Writing Security Classification Guidance*, November 1999

DoD 5200.1-PH, *DoD Guide to Marking Classified Documents*, April 1997

DoD 5200.1-R, *Information Security Program*, January 14, 1997

AFPD 31-4, *Information Security*, 1 September 1998

AFI 10-245, *Antiterrorism (AT)*, 30 March 2009

AFI 10-701, *Operations Security (OPSEC)*, 18 October 2007

AFI 31-401, *Information Security Program Management*, 1 November 2005

AFI 31-401, AFSOC Sup 1, *Information Security Program Management*, 20 June 2008

AFI 31-501, *Personnel Security Program Management*, 27 January 2005

AFI 31-601, *Industrial Security Program Management*, 29 June 2005

AFMAN 33-363, *Management of Records*, 1 March 2008

AFSSI 8580, *Remanence Security*, 17 Nov 2008

TO 00-20F-2, *Inspection and Preventive Maintenance Procedures for Classified Open Storage*, 1 December 2006

AFI 31-401\_AFSOCSUP, *Information Security Program Management*, 20 June 2008

AFSOCI 33-202, *Portable Electronic Device (PED) Security*, 31 March 2004

HFVA 31-6, *Stop Classified Reproduction Not Authorized*, 31 August 2007

HFVA 8, *Authorized for Destruction of Classified Information Visual Aid*, 31 August 2007

HFVA 9, *Not Authorized for Destruction of Classified Information*, 31 August 2007

***Abbreviations and Acronyms***

**AFRIMS**—Air Force Records Information Management System

**AFRC**—Air Force Reserve Command

**AFRIMS**—Air Force Records Information Management System

**ANG**—Air National Guard

**CAL**—Courier Authorization Letter

**CMI**—Classified Message Incidents

**CNWDI**—Critical Nuclear Weapons Design Information

**DRMO**—Defense Reutilization Marketing Office  
**FDO**—Foreign Disclosure Office  
**EPP**—Emergency Protection Plan  
**GCCS**—Command and Control System  
**IDS**—Intrusion Detection Alarm System  
**ISPM**—Information Security Program Manager  
**ISPR**—Information Security Program Reviews  
**IS**—Information Systems  
**IAO**—Information Assurance Officer  
**NdA**—Nondisclosure Agreement  
**NATO**—North Atlantic Organization  
**NIC**—Noise Isolation Class  
**OCA**s—Original Classification Authorities  
**OMC**—Official Mail Center  
**OPR**—Office of Primary Responsibility  
**OSMs**—Office Security Managers  
**OSSAs**—Open Storage and Secure Areas  
**RDS**—Records Disposition Schedule  
**RF**—Radio Frequency  
**SCG**—Security Classification Guides  
**SIO**—Senior Intelligence Officer  
**STC**—Sound Transmission Class  
**STINFO**—Scientific and Technical Data  
**TL**—transmission loss  
**TSCO**—Top Secret Control Officer  
**TS**—Top Secret  
**UFC**—Unified Facilities Criteria

*Terms*

**Radio broadcast**—your radio is best tuned into.

## Attachment 8 (Added)

## SAMPLE APPOINTMENT LETTER

DATE:

MEMORANDUM FOR PERSON(S) BEING TASKED

TO: 1 SOW/IPI

FROM: Unit CC or AFSOC Directorates

SUBJECT: Appointment of Security Manager/Safe Custodian/Reproduction Official/Top Secret Control Officer/Self-Inspection Monitors/TS Annual Inventory Monitors (ONLY ONE APPOINTMENT PER LETTER)

1. In accordance with AFI 31-401, paragraph 1.3.5.1., the following personnel are appointed as (USE ABOVE TITLE) for the (USE SQUADRON NAME):

a. Primary:

b. Rank/Name/SSN: Duty Location: Duty Phone: E-Mail Address:

c. TSgt Jon Smith, Bldg 90210, Room 160, 884-2345, [smithj@hurlburt.af.mil](mailto:smithj@hurlburt.af.mil).

d. Alternate:

e. Rank/Name/SSN: Duty Location: Duty Phone: E-Mail Address:

f. SSgt Mary Jones, Bldg 90509, Room 123, 884-3456, [jonesm@hurlburt.af.mil](mailto:jonesm@hurlburt.af.mil). Note: (PLACE ADDITIONAL ALTERNATES STARTING HERE IF APPOINTED).

2. This supersedes all previous letters of the same subject. For additional information contact TSgt Smith at extension number:

a. Sample Letter. Where to locate appropriate guidance for appointments.

b. Security Managers: AFI 31-401, paragraph 1.3.5.1./CC Appointment.

c. Safe Custodian coming out in new AFI 31-401\_AFSOCSUP, *Information Security Program Management*, to /CC Appointment.

d. Reproduction Official: AFI 31-401, paragraph 5.25./CC Appointment.

e. Self Inspection Monitors coming out in new AFI 31-401\_AFSOCSUP to /CC Appointment.

f. Top Secret Control Officer: AFI 31-401, paragraph 5.8.1.1./CC Appointment.

g. Top Secret Annual Inventory Monitors: AFI 31-401, paragraph 5.8.1.3.1./CC Appointment.

CC SIGNATURE BLOCK

**Attachment 9 (Added)****SECURITY MANAGER (SM) DUTIES AND RESPONSIBILITIES**

**A9.1. (Added) Unit focal point for security program with primary focus being in:** Information, industrial, and personnel security. Includes ensuring through aggressive, oversight, training and hands-on assistance; classified material is protected according to Department of Defense, Air Force, MAJCOM and local directives and guidelines.

**A9.2. (Added) Function as security container and lock combination changing focal point when:** Container custodians are not appointed. This includes maintaining a list of all security containers within the organization. Report all changes affecting integrity of containers, to include secure rooms and vaults.

**A9.3. (Added) Conduct and manage initial security and education training.** Ensure refresher training is conducted and documented. Develop an internal system to ensure all unit personnel (including contractors) receive required training on a recurring basis.

**A9.4. (Added) Conduct or provide supervisors with:** Material for initial security education indoctrinations.

**A9.5. (Added) Provide office security managers (OSMs) with:** Material for recurring security and education training.

**A9.6. (Added) During program reviews organizations will:** Provide reports indicating the number of assigned personnel and specific training accomplished to 1 SOW/IPI.

**A9.7. (Added) Review and track challenges to classification decisions.**

**Attachment 10 (Added)****SAMPLE LETTER FOR NOTIFICATION OF IMPROPERLY MARKED CLASSIFIED DOCUMENT**

MEMORANDUM FOR (Originator of Classified Document).

TO: Office of Responsibility (as listed in applicable classification guide).

FROM: (Classified Custodian).

SUBJECT: Notification of Improperly Marked Classified.

Document (Unclassified Title).

1. The following discrepancies exist on the subject document:

- a. \_\_\_ Overall classification is not shown on the front cover, top and bottom.
- b. \_\_\_ Overall classification is not the same as the highest classification of information contained in the document.
- c. \_\_\_ Internal pages are not marked on the top and bottom with the overall classification of the page or marked unclassified.
- d. \_\_\_ Date originated is not marked on the document.
- e. \_\_\_ Agency, office of origin or office of primary responsibility is not identified on the face of the document.
- f. \_\_\_ Classification authority, "Classified By" line, is missing.
- g. \_\_\_ Declassification instructions, "Declassify On" lines missing.
- h. \_\_\_ Subject or title is not marked with appropriate classification symbol (e.g., TS, S, C, or U).
- i. \_\_\_ Paragraphs or subparagraphs do not contain appropriate classification symbols (e.g., TS, S, C, U).
- j. \_\_\_ Other discrepancies: \_\_\_\_\_

2. Please notify our office and other holders of this document of the corrective actions to be taken. A copy of this notification will be filed with our copy of the affected document until corrective actions are complete.

SIGNATURE BLOCK

**Attachment 11 (Added)****SECURITY CLASSIFICATION GUIDANCE (SCG)**

**A11.1. (Added) Program managers having primary management responsibility for:** A classified weapon system, plan, project, program (including a special access program), operation, equipment, or item (herein referred to as a system) must publish a formal SCG for each system they manage, if not peculiar to and previously published in another SCG. When issuing changes for a SCG, you must review the entire guide. At a minimum, disseminate a change letter to all parties on the SCG distribution list. Coordinate administrative change letters with the necessary system wing authorities. The signature authority for administrative change letters may not be delegated lower than the system senior security functional. Identify the next review date no longer than 5 years from the date of the change. Submit DD Form 2024, *Security Classification Guide Data Element*, DoD RCS: DD-C3I(B&AR)1418, IAW DoD 5200.1-R, Section C2.5.3.5.

**A11.2. (Added) ISOW/IPI will monitor the review of:** ISOW/IPI will send a suspense notice to the OPR 90 days before the review date. The OPR then issues changes as necessary. When major revisions to guides **SCGs issued by activities on Hurlburt Field** occur, the OPR must review for any change of performance and cost involved for the contractor in relationship to the current DD Form 254, *Contract Security Classification Specification, Department of Defense*. Issue a revised DD Form 254 after publication of a new/revised SCG or letter change to a SCG. When changes to the basic SCG occur, the country-unique document OPR must evaluate them in order to update the existing document.

**A11.3. (Added) For SCGs sent to organizations or activities of other Air Force commands :** Provide an electronic copy to the 1 SOW/IPI and AFSOC/IPI office and to SAF/AA.

**A11.4. (Added) Country-unique security classification documents (guides) developed in support of foreign governments or foreign contractor work performance and approved for release under National Disclosure Policy must contain a statement prohibiting release or disclosure of contents to third countries and their nationals.** They must be maintained IAW applicable Executive Orders governing the classification of information.

**A11.5. (Added) SCGs are not releasable to foreign nationals or governments except as stated in paragraph A11.4.** Use a DD Form 254 to convey contractual security classification guidance to foreign contractors. For procurement actions with complex security classification considerations, attach only those extracted portions of an approved SCG applicable to the foreign contractual performance to the DD Form 254, provided they are releasable to the foreign government under National Disclosure Policy.

**A11.6. (Added) Contractor participation in preparation of SCGs is encouraged.** However, if more than one contractor is involved in performance of a contract, ensure all have the opportunity to comment and make recommendations for SCG changes.

**A11.7. (Added) Coordinate all SCGs, changes or revisions with the 1 SOW/IPI before publication, except for guides containing SCI.** Also, as appropriate, coordinate guides with the senior intelligence officer (SIO), Public Affairs, Foreign Disclosure, OPSEC and COMSEC officers.

**A11.8. (Added) Use one classification designation, e.g., U, C, S, or TS under the classification column.** Do not use U-TS, C-S etc. This forces the reader to make an original classification decision. Explain any differences in classification in the remarks column. The remarks column clarifies classification guidance when required.

**A11.9. (Added) The servicing 1 SOW/IPI keeps on file:**

A11.9.1. **(Added)** A current DoD 5200.1-R and DoD 5200.1-H, *Department of Defense Handbook for Writing Security Classification Guidance*.

A11.9.2. **(Added)** One copy of classification guides (and changes/revisions) issued by activities they service.

A11.9.3. **(Added)** Related DD Form 2024.

A11.9.4. **(Added)** Other SCGs necessary to support activities serviced.

**A11.10. (Added) Review distribution list upon revisions to SCGs to ensure only activities requiring SCGs are identified.** To the extent possible, distribute the SCG electronically or via computer media.

**A11.11. (Added) Revised SCGs and changes must contain a summary of changes, to include the topic or item changed.** An OCA must approve and sign changes to guides involving classification decisions.

**Attachment 12 (Added)****CLASSIFIED MEETING/BRIEFING SLIDE**

- A12.1. (Added) THIS BRIEFING CONTAINS CLASSIFIED INFORMATION.**
- A12.2. (Added) This briefing is classified: (LEVEL).**
- A12.3. (Added) PEDs/PDAs are not permitted IAW, AFSOCI 33-202, Portable Electronic Device (PED) Security, para. 7.6.4.**
- A12.4. (Added) Turn off LMRs.**
- A12.5. (Added) No recording devices permitted.**
- A12.6. (Added) Secure all entrances.**
- A12.7. (Added) If you do not possess a (LEVEL) security clearance identify yourself at this time.**

**Attachment 13 (Added)****CONSTRUCTION GUIDELINES FOR SECURE CONFERENCE FACILITIES****A13.1.**

**A13.2. (Added) Secure Conference Facility.** For the purpose of this instruction, a secure conference facility is defined as an area provided special acoustical, technical, and physical security protection, and designated for the discussion and handling of classified defense information on a continuous basis. Due to the high costs of building a secure conference facility, the number of secure conference facilities will be kept to the absolute minimum consistent with mission accomplishment.

**A13.3. (Added) General Approach.** The achievement of adequate security for conference facilities so as to protect all classified information therein requires a blend of acoustical, technical, and physical security measures. This blend is obtained through the coordination of acoustical, electronics, 1 SOCES and security personnel from the initial planning stage through construction and inspection phases. The installation 1 SOCES or Construction Agent is responsible for the design and construction of secure conference facilities. Qualified persons should be consulted for solutions to acoustical problems. The 1 SOCES, Installation Construction Agent, or a qualified consultant should be able to help in the solution of acoustical problems. All elements comprising the physical boundaries of the facility must have a uniformly low transmission of sound through the exterior envelope (walls, ceiling, floor, and doors) of the secure space. No utilities should serve as a fortuitous probe to electronic or audio signals emanating from the secure facility. Physical access to the area must be controlled. Secure conference facilities will not be constructed adjacent to facilities not under U.S. control. After architectural plans are complete and before a contract is let, physical and technical security specialists will review the plans for potential security weaknesses. If uncleared personnel accomplish the construction, it is recommended that appropriately cleared owner/user personnel periodically check the facility, with particular emphasis on monitoring the installation of security items and to preclude the installation of clandestine surveillance devices.

**A13.4. (Added) Acoustical Security.** Acoustical security deals with all measures necessary to minimize the loss of intelligible information acoustically radiated within an area through proper construction techniques.

A13.4.1. **(Added)** Acoustical security treatment. The following facets of acoustical treatment are provided as a general guide to achieve adequate acoustical security:

A13.4.1.1. **(Added)** Doors & Frames. Commercially available doors acoustically rated with a proper Sound Transmission Class (STC) Laboratory rating shall be used. This rating should be 5 - 7 STC Points higher than the Noise Isolation Class (NIC) objective. One concept employs the use of a double door system. In this system two doors are mounted back-to-back with wider doorjamb's used. This gives the added advantage of a relatively dead air space between the inner and outer area and overcomes the direct link from the outside to interior via the door hardware assemblies, such as locks. Fire rated doors will not be used, as they cannot be made to meet the required STC rating. Lead sheets on the inner surface of both doors, helps to increase the sound transmission loss. Any items of hardware installed on such doors should not in themselves create a sound leakage path. The weakest link of a secure room is the doors because they have moving

parts, they must be maintained on a scheduled basis. Doors must be acoustically tested biennially to ensure continuing compliance with required NIC standards.

A13.4.1.2. **(Added)** Doorjamb. Only factory supplied, acoustically rated STC doors that are delivered in factory-supplied doorframes and that have been STC rated, as a functional unit, shall be used. The doorframe shall be installed per manufacturer's instruction.

A13.4.1.3. **(Added)** Door thresholds. Wooden thresholds are preferred over metal because of their lower sound conductivity rating. All thresholds will be sealed at all points of contact with the floor and doorframe.

A13.4.1.4. **(Added)** Expansion joints. Conference facilities should not be located where building expansion joints will form a part of or be immediately against any portion of the facility perimeters. Such joints cannot be effectively soundproofed on a continuing basis, since the joints are always subject to gap changes resulting from ambient temperature variations or building movements.

A13.4.1.5. **(Added)** Holes or crevices. Holes or crevices in all exterior boundaries should be completely sealed with elastomeric caulking cement or equivalent mortar of such sufficiency as to prevent sound leakage and maintain the overall uniformity of sound transmission loss.

A13.4.1.6. **(Added)** Pipes, ducts, and conduits. Holes or crevices around pipes, ducts, and conduit passing into any part of the facility should be well sealed as discussed above. All pipes, ducts, or conduits, must contain a dielectric break (nonmetallic coupling) where passing through the perimeter wall, or be treated with structural masking. Those pipes remaining inside the facility, which are surface mounted, should be covered with an effective insulating material to attenuate the coupling of sound vibrations to the pipe (a possible transmission link from the facility). However, clean metal-to-metal contact is required where ducts or pipes pass through electrical shielding. Likewise, all service boxes connected to pipes and conduits should be covered. When necessary, a short length of pipe leaving a service box should be filled with fiberglass to attenuate airborne sound transmitted within the pipe.

A13.4.1.7. **(Added)** Metal beams or posts. The presence of metal beams and posts within the conference facility should be avoided wherever possible, since they both minimize the utility of a facility and require acoustical treatment in essentially the same manner as pipes and conduits mentioned above.

A13.4.1.8. **(Added)** Radiators. Hot water or steam radiators will not be installed, as they are difficult to make acoustically secure. The best heating system for security is an electrical heater within each room, since the electrical power circuits can be more easily made secure.

A13.4.1.9. **(Added)** Air conditioners. If possible, secure conference facilities should be equipped with an air conditioning system independent of the master building system. Master building systems, with all their air supply and return ducts, are more difficult to make secure. A dedicated air conditioning system should be installed in TOP SECRET areas. The background noise contribution of the heating, ventilation and air conditioning systems should not exceed 42 dB as measured inside the secure area.

A13.4.1.10. **(Added)** Air ducts and ventilation grills. Air ducts and ventilation grills create severe security problems in that they provide a ready path for the transmission of both airborne and structure-borne sound energy. All duct penetrations shall be fitted with commercially available duct silencers having a Dynamic Insertion Loss equal to the specified STC rating of the secure perimeter itself. The sides of the duct silencer shall have the same STC rating as the perimeter. A steel screen with ½ inch square mesh will be installed to preclude the introduction of a clandestine listening device. An approved duct silencer manufactured of non-sound conductive materials will be used to decouple duct sections where any part of air duct passes through an exterior boundary of the facility. As an alternative, the ducts may be treated with structural sound masking at the inside point of penetration.

A13.4.1.11. **(Added)** Sound system speakers. Speakers should be located as far as practicable from all air return inlets and, under no circumstances, mounted on perimeter surfaces. They should be mounted at a point where the sound transmission loss is the greatest (i.e., on a pillar) and likewise, the greatest levels of sound energy must be directed inward, away from any exterior walls. A sound level or volume-unit (VU) meter should be installed as part of the sound system to assure sound levels of 75 dB or below are maintained to avoid nullifying the acoustical security treatment provided the area. Once the 75 dB is achieved, the volume control should be set/secured. Amplified sound shall utilize a well-distributed speaker system (such as speakers suspended from the ceiling) so that the sound pressure level does not exceed more than 75 dB at any place within the room (certain work areas may require a higher speaker dB).

A13.4.1.12. **(Added)** Communications devices. Telephones, intercoms, or any other communications devices that transmit clear text audio from an area should be kept to an absolute minimum, consistent with essential operational requirements. Each such device and its planned location should be considered carefully, for when in use they transmit from the area all conversations conducted within proximity of the device. No cell phones, camera cell phones, cordless telephones, or wireless microphones, keyboards, or mice, wireless or Infrared Local Area Networks (LANs), or devices are allowed in areas where classified information is discussed, briefed, or processed. "Area" refers to a room and/or to a space the size of a 3-meter radius sphere, centering on the classified source. In areas where classified information is discussed, briefed, or processed, wireless pointer/mice devices are allowed for presentations only. All other wireless portable/personal electronic devices (PEDs) not specifically addressed above, that are used for storing, processing, and/or transmitting information shall not be operated in areas where classified information is electronically stored, processed, or transmitted. Classified information could unintentionally be transmitted from an area over unsecured communications systems because of poor planning. Care as to the quantity and location of communications devices, along with acoustical shells or booths about various work centers, can greatly reduce undesired sound transmissions via unsecured communication links. During planning stages, the use of secure communication devices must be considered, i.e. STU III, push to talk, etc.

A13.4.1.13. **(Added)** Alcoves or sound locks. A small room of suitable size can be provided at the main entrance door for both access control and the prevention of inadvertent overhearing whenever the outer door is opened. As an alternative measure, to

identify visitors before opening a single door, either a closed circuit television system or a miniature, wide-angle optical lens (with a suitable hinged, lockable cover over the inside portion) may be installed in the entrance door.

A13.4.1.14. **(Added)** Windows. Windows will not be installed in new secure facilities. When present in existing construction, windows will be removed or sealed and covered to provide an NIC rating equal to the encompassing wall area. Where windows must exist, venetian blinds and masking sound are required in the window area. Installation of man bars outside the windows should be considered. Completely eliminating the windows and replacing them with similar construction, as the surrounding wall is preferable. Where windows must exist, venetian blinds and flameproof heavy drapes (11 oz/sq yd or better) are encouraged to cover such windows inside the area.

A13.4.1.15. **(Added)** Ceilings, Walls, and Floors. True walls (structural floor to ceiling) will be installed in all new construction. For existing structures that do not meet the above requirement, a cap must be installed providing an NIC rating equal to the walls of the room. The presence of false ceilings, walls, and floors in new or old construction must be carefully compared against the total transmission loss afforded.

A13.4.1.16. **(Added)** Floor trenches. Service or utility trenches of any type under the floor should be filled, if possible, with concrete. If this cannot be done, masking sound is required.

A13.4.2. **(Added)** Sound Transmission Class: STC is a numerical rating system for laboratory determined transmission loss. In this rating system, acoustical security is determined solely by the attenuation (transmission loss) of airborne speech between the source and a potential listener outside the perimeter of the facility. The sound transmission loss (TL) of a partition is measured in 16 third-octave bands between 125 Hertz and 4000 Hertz, with each specific TL figure plotted in decibels on a graph. The resulting curve should be normalized against a standard curve, with the overall sound transmission loss expressed as a single figure value called STC (reference: ASTM E90, E-336, and E-413). The NICs provided in [Table 1.5](#) are recommended minimums for secure conference facilities, depending on the level of classification discussed therein, the sound power level of speech within the area, and the ambient noise level in outside adjacent areas. Noise reduction tests in accordance with the ASTM E-413 in-to-out test procedures shall be performed after construction is completed and when modifications are made to the perimeter surface. The test data should be plotted per ASTM E-413 and expressed in a single number NIC. NIC is the same as STC except that an STC test is performed on partitions in an acoustical laboratory, and a NIC test is of a completed structure such as a finished secure facility. Thus, STC ratings are used to select the wall construction, doors, etc., and NIC is what you get when the facility is fully assembled. AN ASTM E-336 test procedure shall be conducted on each wall, floor, ceiling, and perimeter door within the facility. The lowest NIC among the test points shall be that of the entire facility. Because ambient noise outside an area is a variable, i.e., day vs. night, duty hours vs. non-duty hours, etc; it may be necessary to employ sound masking techniques. Such units consist of electronically controlled noise systems or vibration transmitters installed within the perimeter. The employment of such noise generators in wall voids, doors, windows, and overhead ducts is a more economical technique to achieve acceptable transmission losses.

**A13.5. (Added) Technical Security.** Technical security encompasses those measures necessary to deny the use of existing technical equipment that may have compromising emanations or the installation of clandestine technical surveillance devices to collect intelligence from within an area. The servicing communications activity and Office of Special Investigations should be contacted for guidance regarding technical security issues during the initial planning stages of the secure facility. Some guidelines for technical security treatment are as follows:

A13.5.1. **(Added)** Electrical services. All electrical wiring should, if at all possible, be run from a common distribution panel located within the secure discussion area. A single feeder circuit entering the area should service the panel. Radio frequency filters should be included if any equipment is located within the secure conference facility that may have possible compromising emanations. Final determinations of the requirement (or lack thereof) for filters will be made by the Air Force Communications Agency Certified Technical TEMPEST Authority (AFCA/CTTA).

A13.5.2. **(Added)** Communications services. All wires or cables that transmit information to or from a secure conference facility should be routed to a common distribution frame from which a single multi-pair cable leaves the area. All obsolete wires should be removed. Unused wires required for future expansion should be electrically grounded at the distribution frame within the secure area. All communications systems installed should be the minimum necessary consistent with essential and efficient operations. All voice systems, incoming or outgoing, secure or unsecured, should be designed such that when not in use (turned "on") they do not transmit clear text conversation from the area. Line disconnect jacks on outgoing circuits and isolation amplifiers on incoming circuits are an effective means to render such systems secure when not in use. Radio frequency filters should be included if any equipment is located within the secure conference facility that may have possible compromising emanations.

A13.5.3. **(Added)** Telephones. All telephones should be equipped with an automatic disconnect device or a manual plug-type disconnect to disconnect the telephone from the outgoing line. When disconnects are employed nonresonant external ringers are required. See [paragraph A13.4.1.12](#). for further guidance.

A13.5.4. **(Added)** Shielding. If equipment that unintentionally radiates clear text intelligence is used in a secure conference facility to process classified information, consideration must be given to Radio Frequency (RF) shielding the equipment or the facility to contain the compromising emanations. Although technical security surveys do provide a determination if any clandestine technical surveillance devices were or currently are in place, they do not provide protection against future installations or unwitting carriers unless very stringent physical security and access controls are in effect. One countermeasure, which commanders may consider to combat clandestine RF transmitters, is the utilization of RF shielding about sensitive conference sites.

**A13.6. (Added) Physical Security.** Physical security encompasses those measures necessary to deny the physical access of unauthorized personnel to a designated area. Physical security can be achieved through the employment of physical barriers, locking devices, and IDS, or combinations thereof. Since secure conference facilities are located on Air Force installations and are not used to store classified information, secure construction requirements IAW DoD 5200.1-R, Appendix 7, are not mandated. However, if 1 SOW/IP determines the local threat and

security environment dictates more stringent construction requirements, they may use DoD 5200.1-R, Appendix 7, as a guide for constructing the secure conference facility. Some physical security guidelines that can be followed for normal threat environments are as follows:

A13.6.1. **(Added)** Facility Structure. The floor, walls, and roof must be of permanent construction materials offering resistance to, and evidence of unauthorized entry into the area. Walls shall be extended to the true ceiling and attached with permanent construction materials. Windows should not be installed in new secure conference facility construction. Follow the guidance in [paragraph A13.4.1.14](#) for windows in existing construction. Clean, straightforward construction techniques should be employed. Whenever possible, all utility pipes, conduits, and related components should be run exposed on interior wall or ceiling surfaces to minimize exploitation, while facilitating their periodic examination. Likewise, access ports or doors should be provided to permit the periodic examination within concealed areas, i.e., above false ceilings, under stages, etc. In general, the secure conference facility should be kept orderly, with only furniture necessary to minimize concealment locations.

A13.6.2. **(Added)** Locking Devices. Entrances to the secure conference facility should be kept to an absolute minimum commensurate with local fire and safety codes. Doors will be substantially constructed of wood or metal. Doors will be equipped with a locking mechanism to prevent unauthorized entry into the facility when not in use. Built-in, manipulation-proof, three position combination locks with an interior safety release turn knob that conforms to GSA Federal Specifications, FF-L-2740, will be used on entry doors to provide maximum security. Panic hardware will be installed on the inner side of all emergency doors. Emergency doors will not have any hardware on the outside of the doors.

A13.6.3. **(Added)** Door hinges. Door hinges should be installed to deny access to the pivot pin, as its removal often makes an otherwise very secure door highly susceptible to being opened. If the hinge pin must be exposed, then it should be fixed to preclude its removal or the door additionally secured on the hinge side from within.

A13.6.4. **(Added)** Openings. All openings large enough to permit a person to gain unauthorized access into an area, 96 square inches or greater, should be appropriately sealed. Either physical security bars or complete and permanent blockage of the opening is desirable. Special care is necessary to ensure all utility areas such as steam tunnels, air ducts, air shafts, utility shafts, are secure, as is the area above a false ceiling. All windows and other openings which exist in boundary surfaces of a secure conference facility and which adjoin areas of lesser security must be covered or sealed to deny optical and audio surveillance of classified information therein. Optical surveillance techniques include the unaided and aided human eye (binoculars, etc.), photographic and TV cameras, infrared scanners, etc. Audio surveillance techniques include lip reading, infrared pick-off devices, etc. Protective coverings over all openings should include glass opaque to infrared or ultraviolet band energy, venetian blinds, and flameproof heavy drapes (11 oz/sq yd or heavier).

A13.6.5. **(Added)** Intrusion Detection Alarm System (IDS). Since classified information is not stored in secure conference room facilities, Intrusion Detection Alarm Systems are not required. The inclusion of IDS is only recommended when the local threat and security environment dictates more stringent security requirements to prevent the installation of clandestine technical surveillance devices. The system should include volume, perimeter, and point sensors. Proximity and motion detectors provide protection for unique problems.

All intrusion alarm systems should include electrical line supervision between the protected area and monitoring location. Further, all systems should be capable of sustaining normal operation for 24 hours after a commercial power loss. All sensors employed must detect an intrusion and be immune to normal bypass techniques. When used, all intrusion detection alarm systems should be of the type, and so installed, that they do not transmit intelligence from an area.

**A13.7. (Added) Masking Sound Applied to Speech Security.** In order to make it impossible to understand speech outside the secure area, the system design goal must be to reduce speech intelligibility in all situations, whether it is the result of human listening or listening with detection devices. Technically, the purpose of masking sound is to reduce the signal-to-noise ratio of a sound to zero at all pertinent frequencies. In this context, the signal is the speech and the noise is the masking sound. When the speech intelligibility is zero, the privacy is total and the signal to noise ratio is zero. This is adequate for direct human listening, but when detection devices are used and signal-processing techniques are used on the derived signal, it is possible to improve the signal-to-noise ratio and recover meaning. To keep speech intelligibility at zero, the masking should be amenable to signal processing techniques that could reduce its effectiveness. This can be achieved with a masking signal that is the result of a stationary random process. The masking signal becomes not only unknowable but cannot be processed with statistical techniques. Standard masking generators are digital using components in which the signal repeats itself after one minute. They are called pseudo random controlled noise generators. The sound created by them may appear random to the listener, but is in fact a deterministic process. Sophisticated techniques can make use of this deterministic property to increase the speech intelligibility and thus recover speech. Analog masking generators are somewhat better in that they create a truly random signal, but suffer from the fact that the signal is Gaussian and stationary, statistical properties that make signal processing easier. This aspect of the problem is handled in the equipment generating the masking sound. The most effective method for structural masking is when random signal vibrations are introduced directly to the perimeter barrier surface to control background sound levels at potential listening points. The sound masking system and all wires and transducers shall be located within the perimeter of the facility. Speakers can be located outside the facility and directed outward as close as practicable to the facility's perimeter where the sound transmission loss is the greatest (i.e. doors, windows, HVAC ducts, electrical and plumbing conduit, etc.) to achieve the required/desired STC rating. The sound masking system should only be utilized when the required/desired STC rating is not achievable through physical security means. See Unified Facilities Criteria (UFCs) 3-450-01, Noise and Vibration, 4-021-02NF, Security Engineering and 4-610-01, Administrative Facilities for planning, design, construction, restoration and modernization applicable specifics.

**Table A13.1. (Added) Noise Isolation Class (NIC).**

RULE	Area Approved for Discussion of:	If Area Has:	
		Normal Speech	Amplified Speech
1	Secret	45	50
2	Top Secret	50	55



Attachment 15 (Added)

CLASSIFIED COPIER CHECKLIST

CLASSIFIED COPIER CHECKLIST

ALL PURPOSE CHECKLIST		PAGE 1 OF 1 PAGES			
TITLE/SUBJECT/ACTIVITY/FUNCTIONAL AREA		OPR	1 Sep 09		
CLASSIFIED COPIER APPROVAL CHECKLIST(Added)		SFAI	YES	NO	N/A
NO	ITEM				
1	Is the equipment to be used for classified reproduction an Automated Information System (AIS)? (Ref: DOD 5200.1-R, 6-309 and AFI 31-401, 5.17.1)				
2	If AIS, has the equipment been accredited by Information Assurance?				
3	Has the Commander designated the equipment to be used for classified reproduction in writing? Use HF Form 2 to document. (Ref: AFI 31-401, para 5.24.1.)				
4.	Has the Commander designated a unit Reproduction Official in writing to exercise reproduction authority for classified material in their activities? Document on HF 2 and include in unit security operating instruction. (Ref: AFI 31-401, para 5.25)				
5.	Have the user organizations Information Assurance Official (IAO) approved the equipment to be used for classified reproduction? (Ref: AFI 31-401, para 5.24.2)				
6.	Have the IM personnel issued procedures for clearing copier equipment of latent images? (Ref: AFI 31-401, para 5.24.2)				
7.	Has the unit security manager posted equipment approval (HF Form 2). (Ref: AFI 31-401, HF Sup 1, para 5.24.3.1)				
8.	Has the security manager developed procedures that ensure control of classified? (Ref: DOD 5200.1-R, 6-502 and AFI 31-401, para 5.24.3.2)				
9.	Are these procedures included in the unit security operating instruction OI?				
10.	Has the security manager taken steps to ensure all organizational personnel understand their security responsibilities and that they follow procedures? (Ref: AFI 31-401, para 5.24.3.3)				
11.	Has a completed copy of HF 2 been submitted to 1 SOW/IPI for each copier used for reproduction of classified?				

AF FORM 2519, NOV 91(EF)

PREVIOUS EDITION WILL BE USED

**Attachment 16 (Added)****SAMPLE COURIER LETTER**

DATE:

MEMORANDUM FOR WHOM IT MAY CONCERN

FROM: 1 XXX/CC

SUBJECT: Designation of Official Courier

1. Master Sergeant John A. Doe, FR000-11-2222, 1st Special Operations Flight Support Squadron, (Unit), Hurlburt Field, Florida, is designated an official courier for the United States Government. Upon request, he will present his official identification card bearing the number X-XXXXXXX (or other appropriate identification media).
2. Master Sergeant Doe is hand-carrying three sealed packages, size 9" x 8" x 24 " addressed from "1 SOXX/XX, Hurlburt Field, FL 32544-5716," and addressed to "HQ USAF/IG, Wash DC 20330-5001." Each package is identified on the outside of the package by the marking "OFFICIAL BUSINESS--MATERIAL EXEMPTED FROM EXAMINATION" bearing the signature of the undersigned.
3. Master Sergeant Doe is departing Ft. Walton Beach Regional Airport with a final destination to Washington National Airport, District of Columbia. He has a transfer point at Atlanta International Airport.
4. This courier designation can be confirmed by contacting the undersigned at 1 SOXXX, Area Code 904, 884-XXXX, or DSN 579-XXXX. This letter expires 1 July 20XX.

CC SIGNATURE BLOCK

**Attachment 17 (Added)**  
**SAMPLE EXEMPTION NOTICE**

**SAMPLE EXEMPTION NOTICE**

Department of the Air Force

*Office Symbol*

Hurlburt Field Florida, 32544

---

OFFICIAL BUSINESS

---

MATERIAL EXEMPT FROM EXAMINATION

{Signature Required}  
JANE B. AGOODGUY, Colonel, USAF  
Commander

**Attachment 18 (Added)****MODEL (ORGANIZATION NAME) ANNUAL TRAINING PLAN****A18.1. (Added) References:** DoD 5200.1-R and AFI 31-401.

A18.1.1. **(Added)** AFI 31-501, *Personnel Security Program Management*.

A18.1.2. **(Added)** AFI 31-601, *Industrial Security Program Management*.

A18.1.3. **(Added)** AFI 10-245, *Antiterrorism (AT)*,

A18.1.4. **(Added)** AFI 10-701, *Operations Security (OPSEC)*.

A18.1.5. **(Added)** DoD 5200.1-PH.

A18.1.6. **(Added)** Executive Order 12958, Classified National Security Information as Amended.

A18.1.7. **(Added)** General. Commanders and staff agency chiefs must ensure personnel understand the compelling need to protect classified and sensitive resources. To accomplish this, supervisors or unit security managers provides an initial security briefing during indoctrination to all personnel on basic security policies, principles and practices. Cleared personnel must have this training prior to being granted access to classified information as soon as possible (normally within two weeks) of a person's assignment using "Initial Briefing Training Standards" **Attachment 19**. Do this in a one-to-one setting or as group discussion using training aids. Thereafter, security managers provide at least quarterly refresher training to all cleared personnel who create process or handle classified information. Refresher training must be accomplished at least annually to reinforce the policies, principles and procedures covered in initial and specialized training using "Refresher Security Education and Training Standards" at **Attachment 20**. More detailed specialized security education and training should be given to original classifiers, authorized declassification authorities, individuals specifically designated as responsible for derivative classification, classification management officers, security managers, security specialists, and all other personnel whose duties significantly involve the creation or handling of classified information. This training should be provided before or concurrent with the date the person assumes any of the positions listed herein, using "Specialized Security Education and Training Standards" on **Attachment 21**. The 1 SOW Information Protection share-point page at [https://eis.afsoc.af.mil/sites/1SOW\\_IP/default.aspx](https://eis.afsoc.af.mil/sites/1SOW_IP/default.aspx) provides training aides, presentations and training documentation. **Note:** All security training requirements vary depending on activity, size, mission, location, type/amount of classified holdings, etc. Tailor depth of subject coverage to the organizational/personnel missions.

**A18.2. (Added) Method.** Conduct individual, group training by verbal briefing, films, videotapes, slides, handouts, publications, and other media means: First session (Jan-Mar).

A18.2.1. **(Added)** Executive Order 12958, as amended responsibilities.

A18.2.1.1. **(Added)** Classification, identification and markings, self-inspections, declassification, transmitting, destruction, reproduction, storage, mailing (U.S. Postal or FEDEX).

A18.2.1.2. **(Added)** HUMINT/local threat. **Note:** AFOSI may do it, but if they cannot support, security manager should do.

A18.2.1.3. **(Added)** Base security OPLAN.

A18.2.1.4. **(Added)** Unescorted entry procedures.

A18.2.1.5. **(Added)** Local security operating instructions and practices.

A18.2.1.6. **(Added)** Security violation reporting and requirements (through unit and 1 SOW/IPI).

A18.2.1.7. **(Added)** Results of local inspections/reviews, IG evaluations, and recent security violations, as applicable.

A18.2.1.8. **(Added)** Selected topics from security managers' meeting (QSMM).

A18.2.1.9. **(Added)** Updates to the Personnel Security Program.

A18.2.1.10. **(Added)** NATO briefing.

**A18.3. (Added) Method.** Film, handouts, computer presentations, video, and guest speaker: Second session (Apr-Jun).

A18.3.1. **(Added)** Classification challenges and procedures.

A18.3.2. **(Added)** Security classification guides.

A18.3.3. **(Added)** Security violations and their adverse impact on national security, espionage and penalties.

A18.3.4. **(Added)** Protection of classified and end-of-day security checks.

A18.3.5. **(Added)** Protecting unclassified technical data including Scientific and Technical Data (STINFO).

A18.3.6. **(Added)** Physical security of AIS assets.

A18.3.7. **(Added)** Results of local inspections/reviews, IG evaluations, and recent security violations, as applicable.

A18.3.8. **(Added)** Selected topics from Quarterly Security Managers Meetings (OSMM).

A18.3.9. **(Added)** Protecting controlled unclassified information (FOUO etc.).

**A18.4. (Added) Method.** Film, handouts, computer presentations, videos and guest speaker: Third session (Jul-Sep).

A18.4.1. **(Added)** OPSEC.

A18.4.2. **(Added)** Protection of government/personal property.

A18.4.3. **(Added)** Foreign travel.

A18.4.4. **(Added)** The threat, techniques employed by foreign intelligence activities attempting to obtain classified information, and penalties for engaging in espionage activities.

A18.4.5. **(Added)** Results of local inspections and reviews, IG evaluations, and recent security violations, as applicable.

A18.4.6. **(Added)** Select QSMM topics.

**A18.5. (Added) Method.** Film/handouts, computer presentations, videos and guest speaker. Fourth session (Oct-Dec).

A18.5.1. **(Added)** Personnel security clearance/need-to-know, Special Information File, initial investigations and periodic reinvestigations.

A18.5.2. **(Added)** Bomb threats.

A18.5.3. **(Added)** Special access programs Critical Nuclear Weapons Design Information (CNWDI) requirements.

A18.5.4. **(Added)** Industrial Security-National Industrial Security Program Operations Manual (NISPOM), DD Fm 254 and Visitor Group Security Agreements (VGSA).

A18.5.5. **(Added)** JPAS Visit request procedures.

A18.5.6. **(Added)** Security violation reporting and requirements (through unit and 1 SOW/IPI).

A18.5.7. **(Added)** Results of local inspections and reviews, Inspector General evaluations, and recent security violations.

A18.5.8. **(Added)** Select QSMM topics.

APPROVED:

COMMANDER OR DIRECTOR, (DATE)

**Attachment 19 (Added)****INITIAL TRAINING BRIEFING STANDARDS**

**A19.1. (Added) This initial briefing training standard should be used to:** Brief all newly assigned personnel as soon as possible (normally within 2 weeks). Cleared personnel must have this training prior to being granted access to classified information.

A19.1.1. (Added) These standards are not intended to be all-inclusive. Security managers should expand or modify the depth of briefing according to applicability and the organization's mission, program and policy needs.

A19.1.2. (Added) Consider the following areas, as applicable.

A19.1.3. (Added) Roles and responsibility.

A19.1.4. (Added) What are the responsibilities of the senior unit/agency official, classification management officers, and the security manager/specialist?

A19.1.5. (Added) What are the responsibilities of agency/unit members who create or handle classified information?

A19.1.6. (Added) Who should be contacted in case of questions or concerns about classification matters?

A19.1.7. (Added) Elements of classifying and declassifying information.

A19.1.8. (Added) What is classified information and why it is important to protect?

A19.1.9. (Added) What are the levels of classified information and the damage criteria associated with each level?

A19.1.10. (Added) What are the prescribed classification markings and why is it important to have classified information fully and properly marked?

A19.1.11. (Added) What are the general requirements for declassifying information?

A19.1.12. (Added) What are the procedures for challenging the classification status of information?

A19.1.13. (Added) Elements of Safeguarding.

A19.1.14. (Added) What are the proper procedures for safeguarding classified information?

A19.1.15. (Added) What constitutes an unauthorized disclosure and what are the penalties associated with these disclosures?

A19.1.16. (Added) What should an individual do when he or she believes safeguarding standards may have been violated?

**A19.2. (Added) The following areas are the mandatory subject areas :** From the **AIR FORCE INFORMATION SECURITY PROGRAM TRAINING STANDARD** available on the 1 SOW Information Protection share-point page at [https://eis.afsoc.af.mil/sites/1SOW\\_IP/default.aspx](https://eis.afsoc.af.mil/sites/1SOW_IP/default.aspx) (see the training standard for breakdown by subject area and technical references). These areas are mandatory for all cleared personnel during initial, indoctrination/orientation and annual refresher information security training.

**Attachment 20 (Added)****REFRESHER SECURITY EDUCATION AND TRAINING STANDARDS**

**A20.1. (Added) This refresher security education and training standard will be used to provide:** Refresher training to those personnel who create, process or handle classified information. Refresher training should reinforce the applicable policies, principles and procedures covered in initial and specialized training. As a minimum, personnel shall receive annual refresher training that reinforces the policies, principles and procedures covered in initial and specialized training. Refresher training should also address the threat and the techniques employed by foreign intelligence activities attempting to obtain classified information, and advise personnel of penalties for engaging in espionage activities. Refresher training should also address issues or concerns identified during unit self-inspections.

**A20.2. (Added) Refresher training should:** Address issues or concerns identified during agency self-inspections and ISPRs. When other methods are impractical, units or agencies may satisfy the requirement for refresher training by means of audiovisual products or written materials.

**A20.3. (Added) Refresher training may also be required when:** Personnel violate established security procedures or are identified as the subject of a security incident.

**Attachment 21 (Added)****SPECIALIZED SECURITY EDUCATION AND TRAINING**

**A21.1. (Added) This detailed specialized security education and training should :** Be given to original classifiers, authorized declassification authorities, individuals specifically designated as responsible for derivative classification, classification management officers, security managers and all personnel whose duties significantly involve the creation or handling of classified information. This training is to be provided before or concurrent with the date the person assumes any positions above, but in any event no later than 6 months from that date. Training materials for OCAs and Derivative classifiers are available on the 1 SOW Information Protection share-point page at [https://eis.afsoc.af.mil/sites/1SOW\\_IP/default.aspx](https://eis.afsoc.af.mil/sites/1SOW_IP/default.aspx).

**A21.2. (Added))** Coverage considerations should include:

A21.2.1. **(Added)** Original Classifiers.

A21.2.2. **(Added)** What is the difference between original and derivative classification?

A21.2.3. **(Added)** Who can classify information originally?

A21.2.4. **(Added)** What are the standards that a designated classifier must meet to classify information?

A21.2.5. **(Added)** What is the process for determining duration of classification?

A21.2.6. **(Added)** What are the prohibitions and limitations on classifying information?

A21.2.7. **(Added)** What are the basic markings that must appear on classified information?

A21.2.8. **(Added)** What are the general standards and procedures for declassification?

**A21.3. (Added) Declassification authorities other than original classifiers:**

A21.3.1. **(Added)** What are the standards, methods and procedures for declassifying information under E.O.12958 as amended?

A21.3.2. **(Added)** What is contained in the unit/agency's automatic declassification plan?

A21.3.3. **(Added)** What are the unit/agency responsibilities for the establishment and maintenance of a declassification database?

**A21.4. (Added) Individuals specifically designated as responsible for derivative classification :** Security managers, classification management officers, security specialists or any other personnel whose duties significantly involve the management and oversight of classified information.

A21.4.1. **(Added)** What are the original and derivative classification processes and the standards applicable to each?

A21.4.2. **(Added)** What are the proper and complete classification markings, as described in Identification and Marking Section of the Executive Order 12958 as amended?

A21.4.3. **(Added)** What are the authorities, methods and processes for downgrading and declassifying information?

A21.4.4. **(Added)** What are the methods for the proper use, storage, reproduction, transmission, dissemination and destruction of classified information?

A21.4.5. **(Added)** What are the requirements for creating and updating classification and declassification guides? What are the requirements for controlling access to classified information?

A21.4.6. **(Added)** What are the procedures for investigating and reporting instances of security violations, and the penalties associated with such violations?

A21.4.7. **(Added)** What are the requirements for creating, maintaining, and terminating special access programs, and the mechanisms for monitoring such programs?

A21.4.8. **(Added)** What are the procedures for secure use, certification and accreditation of automated information systems and networks which use, process, store, reproduce or transmit classified information?

A21.4.9. **(Added)** What are the requirements for oversight of the security classification program, including unit/agency self-inspections?