BY ORDER OF THE COMMANDER
70 INTELLIGENCE SURVEILLANCE
AND RECONNAISSANCE WING

70 INTELLIGENCE SURVEILLANCE
AND RECONNAISSANCE WING
INSTRUCTION 16-1404

4 JANUARY 2018

Operations Support

INFORMATION PROTECTION
PROGRAM MANAGEMENT

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

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

RELEASABILITY: There are no releasable restrictions on this publication

---

OPR: 70ISRW/IP

Certified by: 70ISRW/CC
(Matteo G. Martemucci)

Supersedes: 70ISRWI31-401, 26 August 2014

Pages: 35

This instruction establishes the policies, procedures, and responsibilities that will promote the proper training, classification, and safeguarding of information and personnel within 70 ISRW that are vital to national security and allows for the continuous evaluation of unit personnel for trustworthiness and reliability. All 70 ISRW personnel, to include Active Duty military, Reservists, civilians and contractors, must be familiar with and adhere to the policies listed in this instruction. Air Force units/organizations who are tenants to 70 ISRW must also be familiar with these policies. These policies implement and extend the requirements of the following DoD and Air Force Instructions: AFI 16-1404, Air Force Information Security Program; AFI 31-501, Personnel Security Program Management; AFI 16-1406, Air Force Industrial Security Program Management; AFI 10-701 Operations Security, AFI 16-1402, Insider Threat Program Management; DoDM 5200.01, Vol 1-4, DoD Information Security Program, DoDM 5200.02, Procedures for the DoD Personnel Security Program.

(Applicability) This publication outlines the internal security programs for the 70 ISR Wing and applies to all 70 ISRW units, assigned personnel to include civilians, contractors, attached ANG and Reserve units. This Instruction was designed to provide both local and Geographically Separated Units (GSU) the tools and guidance necessary to effectively manage and operate their organizations Personnel, Industrial and Information Security programs. NOTE: Due to the unique mission and operating locations of 70 ISR Wing units, all units must adhere to DoD, AF and SSA guidance and/or instruction and are subject to applicable inspection guidelines.

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 Forms 847 from the field through the appropriate functionals chain of command. 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/afrims/afrims/afrims/rims.cfm**. Additionally, if your publication generates a report(s), alert readers in a statement and cite all applicable Reports Control Numbers in accordance with AFI 33-324.

SUMMARY OF CHANGES

This document supersedes 70ISRWI31-401. This 70ISRW/IP Instruction contains updated references for the changed AFI 31-401 to designation AFI 16-1404, Air Force Information Security Program and AFI 31-601 designation to AFI 16-1406, Air Force Industrial Security Program.

Chapter 1

INFORMATION PROTECTION PROGRAM RESPONSIBILITIES

1.1. Commander. Uses the core security disciplines within Information Protection and coordinates with other program managers (e.g., COMSEC, OPSEC, etc.) to identify, promote information sharing, facilitate judicious use of resources, and simplify management of, employ maintain and enforce standards for safeguarding, storing, destroying, transmitting, and transporting; and mitigate the adverse effects of unauthorized access or disclosure, compromise or loss by investigating and acting upon reports of security violations involving classified information and CUI for the wing.

1.2. Chief, Information Protection. Manages and implements the execution of the Information Protection program (Information, Personnel, and Industrial Security) on behalf of the 70 ISRW/CC.

1.2.1. Conducts Information Protection Program reviews of all units within the local area.

1.2.2. Conducts staff assistance visits (SAVs), when requested.

1.2.3. Ensures security managers for units or staff agencies are trained to perform their duties IAW Chapter 5 of this Instruction.

1.2.4. Manages the information security training program and provides technical guidance to unit or staff agency security managers.

1.2.5. Conducts semiannual security manager meetings and prepares and distributes minutes of each meeting to all security managers and their commander or equivalent for use in their security programs.

1.2.6. Develops approval/recertification packages for open storage areas/secure rooms.

1.2.7. Provides assistance and guidance to commanders and directors in resolving unique security related issues.

1.2.8. Writes a wing instruction or leverage another directive that applies to all wing personnel.

1.3. Security Specialist, Information Protection. Implements the Information Protection core security disciplines on behalf of 70 ISRW/CC. The Information Protection duties include:

1.3.1. Provides guidance and direction to commanders and directors or designated security manager when requested on all aspects of the Air Force Information Security Program.

1.3.2. Provides oversight of the security incident inquiry/investigation process to include establishing a central tracking system.

1.3.3. Analyzes security violations and infractions to determine security impact.

1.3.4. Trains security managers on their duties and responsibilities in accordance with the Security, Education, Training and Awareness section of this Instruction.

1.3.5. Coordinate on security classification and declassification guides, Air Force Instructions, and other program related guidance resources as needed.

1.3.6. Advises commanders with collateral work spaces on types of emergency plans to develop based on local threats of hostile actions, foreign intelligence, natural disasters, or terrorist activity.

1.3.7. Provides derivative classifiers guidance, direction, and oversight for marking classified information and CUI.

1.3.8. Provides commanders and directors assistance in developing exception to policy staff packages to deviate from protection standards identified in DoDM 5200.01.

1.3.9. Integrate on-base contractor operations into the Wing Information Security Program.

1.3.10. Coordinate with Wing Cybersecurity Office to ensure full integration of information technology requirements to include: access, security, and response action to security incidents involving classified information and CUI on IT systems.

1.3.11. Assist the Chief, Information Protection with annual self-inspections.

1.4. Special Security Office. The SSO implements Sensitive Compartmented Information (SCI) programs and processes on behalf of the 70 ISRW/CC and coordinates with the Wing IP Office on security matters related to Information, Personnel, Industrial, and Physical Security. NOTE: Refer to local SSO OI or SOP for further information regarding SSO duties.

1.5. Unit Security Manager. The USM is the authority to establish and monitor the security policies and procedures necessary to assure the safeguarding of classified and controlled unclassified information. The USM will:

1.5.1. Establish a continuity binder/handbook and maintain pertinent program records. At a minimum the binder/handbook will include:

1.5.1.1. Primary and alternate USM Appointment Records.

1.5.1.2. Commander/USM Roles and Responsibilities

1.5.1.3. Regulations

1.5.1.4. Unit Security Instruction, Security Plan, or Standard Operating Procedures

1.5.1.5. Semiannual Wing IP USM Meeting Minutes

1.5.1.6. Annual Information Protection Program Review and/or Higher Headquarter inspections.

1.5.1.7. Annual MICT self-assessments (last 2 reports).

1.5.1.8. Security training documentation (minimum 2 years to include sign-in sheets, email receipts, etc.)

1.5.1.9. Miscellaneous items (Annual position code review, clean out day memo, safe custodian memo, classified container listing, SIPRNet Authorization memo, etc.)

1.5.2. Manage the Joint Personnel Adjudication System (JPAS) for the unit.

1.5.3. Attend 70 ISRW/IP semiannual USM meetings (primary, alternate or rep). For GSU's, slides and meeting minutes will be distributed accordingly.

1.5.4. Notify unit members whenever a PSI action is required (initiation of PR in eQIP, etc.).

1.5.5. Coordinate the annual position code review each May.

1.5.6. Conduct an annual clean-out day (either self-initiated or when directed by the IP Office) to remove classified material no longer valid to the mission.

1.5.7. Notify the Wing IP Office, in writing, when a secure room or vault is no longer used for classified storage.

1.5.8. Provide the following documentation (when requested) to the 70 ISRW/IP Office:

1.5.8.1. Appointment memorandums for USM, Top-Secret Control Officers (if applicable), Safe Custodians, etc.

1.5.8.2. Copy of the last annual Higher Headquarters (HHQ) program review or unit self-inspection reports.

1.5.8.3. Copy of all secure room, vault and secure room approval/recertification memorandums.

1.5.8.4. USM training documentation.

1.5.8.5. Security Incident Reports.

1.5.8.6. Other items as determined by the Wing CIP.

1.6. All Personnel. Protect classified and controlled unclassified information in his or her custody or which is found not properly protected.

1.6.1. Report any discovery of classified or controlled unclassified information not properly controlled/protected to the USM, immediate supervisor, unit chief, or higher authority. Protect the classified information until it is conveyed to the appropriate custodian.

1.6.2. Know their level of security clearance and any approved special access authorization.

1.6.3. Be alert to the presence of classified or CUI information in the work area.

1.6.4. Challenge strangers in the work area; find out who they are and what business they have there.

1.6.5. DO NOT discuss classified information in the work area without insuring conversation cannot be overheard by unauthorized personnel.

1.6.6. DO NOT discuss classified information over a non-secured telephone or in a room where someone is using the telephone.

1.6.7. Be familiar with the prerequisites required prior to allowing an individual access to classified information:

1.6.7.1. Individual has the appropriate security clearance eligibility;

1.6.7.2. Individual has signed an SF 312, Classified Information Nondisclosure Agreement.

1.6.7.3. Individual has a need-to-know.

1.6.8. NOTE: Refer to Industrial Security for granting a contractor access to classified information.

1.6.9. Report derogatory and/or significant life issues to their supervisor and USM

1.6.10. Report to their USM all contacts with individuals of any nationality, whether within or outside the scope of the employee's official activities, when unauthorized access to classified or sensitive information is sought or the employee believes he or she is a possible target for exploitation by a foreign and/or domestic entity.

Chapter 2

PERSONNEL SECURITY

2.1. Personnel Security Actions. Members are responsible for completing clearance paperwork by the assigned suspense date.

2.2. Position Code. AFI 31-501 requires commanders to determine the level of access necessary for each military and civilian position based on mission needs.

2.2.1. Each position is coded with the appropriate security access requirement (SAR) and identified on the UMD.

2.2.2. Commanders are required to conduct an annual review of the UMD, determine the accuracy of position coding and adjust SAR codes appropriately.

2.3. Initial Security Investigations. When notified by the USM or Security Specialist of a requirement for a Personnel Security Investigation (PSI) the individual will follow directions provided by the USM or Security Specialist to accomplish the Electronic Questionnaires for Investigations Processing (eQIP).

2.3.1. It is the individual's responsibility to obtain the information required to complete all forms associated with the PSI.

2.3.2. Failure or refusal to complete the PSI could result in Unfavorable Administrative Actions as outlined in AFI 31-501.

2.4. Reinvestigations. Reinvestigations are required:

2.4.1. Every 5 years for Top Secret/SCI eligibility.

2.4.2. Every 10 years for Secret eligibility.

2.4.3. When notified by the USM or Security Specialist of a need for a reinvestigation, the individual will complete their eQIP package.

2.5. Continuing Evaluation Program (CEP). This is a program used to continuously monitor a cleared individual's eligibility for access to classified information based on any derogatory information that may arise between investigations.

2.5.1. USMs are there to provide assistance, advice, and recommendations to supervisors and the commander on the Continuing Evaluation Program whenever a members continued access to classified information becomes questionable.

2.5.2. Supervisors and coworkers are responsible for reporting derogatory or adverse information in accordance with the Continuing Evaluation Program as outlined in DoD 5200.2-R and AFI 31-501.

2.5.3. Personnel who are experiencing problems in their personal lives (i.e., financial, medical, emotional, etc.) must immediately inform their supervisor/someone in their chain of command and USM. Failure to comply with reporting requirements may adversely affect an individual's continuing access to classified information. NOTE: Certain reporting situations (i.e. Sexual Assault) may preclude official notifications.

2.5.4. USMs will provide reported changes in personnel status to the SSO.

2.6. Security Information File (SIF). The USM is to be notified immediately when unfavorable information is revealed that could have a direct impact upon an individual's security clearance.

2.6.1. A SIF is established upon receipt of derogatory information that places an individual's loyalty, reliability, judgment, or trustworthiness into question.

2.6.2. The USM will be responsible for briefing their commander or appointed designee of the requirement to review and evaluate derogatory information IAW adjudicative guidelines outlined in DoD 5200.2-R.

2.6.3. All unfavorable or derogatory information developed and/or received from outside agencies will be protected IAW Privacy Act laws. NOTE: Any derogatory information involving an SCI indoctrinated member will be reported to the SSO.

2.7. Denied or Revoked Clearance Eligibility. If an adjudicative decision is made to deny or revoke clearance eligibility, the individual will immediately be denied all access to classified information and facilities.

2.8. Joint Personnel Adjudication System (JPAS). JPAS is the authorized system of record for clearance eligibility and access for DoD military, civilian and contractor personnel.

2.8.1. Primary and alternate USM will obtain a JPAS account.

2.8.2. The USM will utilize JPAS to verify clearance eligibility for all personnel, to include visitors, prior to granting access to classified information. See Industrial Security for granting a contractor access to classified information.

2.8.3. The USM must in-process all members assigned to the unit upon arrival and out-process upon PCA, PCS or separation from service. NOTE: All members must be owned in JPAS (SCI, non-SCI) unless otherwise directed by higher authority.

Chapter 3

INDUSTRIAL SECURITY

3.1. General. Due to the unique environment of the 70 ISRW and subordinate units (to include GSU's), the management of industrial security contracts (DD Form 254, Statements of Work, etc.) is performed by the 25 AF/A2S. Other, non-AF, contracts will be managed by their respective organization. EXCEPTION: GSUs will comply with Host Wing IP/Servicing Security Activity directives/guidelines.

3.2. In-processing. If a contractor is assigned to a unit, they must in-process with the USM within the first week of duty.

3.3. Investigations. USM will verify investigation eligibility in the Joint Personnel Adjudication System (JPAS). When necessary, the contractor will contact the agency owning their SCI to fulfill investigation requirements.

3.4. Continuing Evaluation Program (CEP). Contractors will participate in the CEP and reporting requirements.

3.5. Security Training. All contractor personnel are required to complete initial and recurring security training in accordance with local unit requirements.

3.6. Granting Contractors Access to Classified Information . The individual controlling the classified will verify the level and type of information being released to the contractor.

3.6.1. Verify the level of access the individual requires is on contract via the DD Form 254, DoD Contract Security Classification Specification.

3.6.2. Verify through the Joint Personnel Adjudication System (JPAS) the individual's record is "owned" by the current employer, as identified by CAGE code.

3.6.3. Verify the individual possesses the correct security clearance eligibility and their US Access is recorded up to the level of the classified information be disclosed (i.e., TS, Secret, NATO, CNWDI).

3.6.4. Ensure a signed SF 312, Classified Information Nondisclosure Agreement is recorded.

3.6.5. Verify the individual's need-to-know prior to access. If one of these elements is missing access will not be granted.

3.7. Identification and Badges . Contractors will identify themselves as such in accordance with the local site contractor badge policy.

3.8. Out-processing: All contract personnel must out-process with the USM and SSO.

3.9. Contract Termination/Extension. Program Managers/Quality Assurance Personnel (PM/QAP) will notify the USM, SSO, Industrial Security Specialist or IP Office when a contractor's effort has ended or the period of performance has been extended. If period of performance has been extended, the PM or QAP will provide a copy of the contract modification to the USM, SSO, Industrial Security Specialist, or IP Office.

3.10. Security Incidents

3.10.1. Program Managers and Contracting Officer Representative will notify USM when issues concerning a contractor (such as incorrect or incomplete background investigation, conduct, personnel issues, security incidents, etc.) would prevent the contractor from accessing classified information or performing security-related responsibilities outlined in the contract or VGSA. USM will contact the SSO for guidance for SCI indoctrinated contractors. NOTE: For Non-SCI indoctrinated contractors, contact the IP Office.

3.10.2. Security incidents involving contractors will be reported in accordance with the VGSA, AFI 16-1404, and paragraph 3.8.1. As a minimum, violations will be immediately reported to the USM, Program Manager, and the COR.

3.10.3. USM must record, and notify the SSO and/or IP Office immediately upon notification of any incidents of espionage, sabotage, subversive activities, deliberate compromises of classified information, and leaks of classified information to the media, involving contractors assigned to their unit.

3.10.4. USM must ensure the following information is gathered and provided upon request:

3.10.4.1. Identify the contractor involved. Identify the person(s) involved, including the full name, date and place of birth, social security number, local address, present location, position with the contractor, security clearance (including past or present participation in any special access programs (SAPs), and a description of any plans or action and any recommendations to suspend or revoke the individual's personnel security clearance (PCL).

3.10.4.2. Establish the known circumstances of the incident, including the identity of the classified material involved; any subsequent activities or circumstances (including whether and which news media know about the incident); and culpable individuals, where known.

3.10.5. The SSO and/or IP Office will report and provide detailed information from the incident to local AFOSI for further investigation.

Chapter 4

INFORMATION SECURITY

4.1. Safeguarding of Classified and Controlled Unclassified Information

4.1.1. The individual having possession of classified material or information is responsible for safeguarding it to prevent the loss or unauthorized disclosure.

4.1.2. While outside its approved storage container, all classified material will be maintained under the immediate control of the authorized person using the material. SF Form 704, Secret (Cover Sheet), or SF Form 705, Confidential (Cover Sheet) will be attached to the material while outside the storage container.

4.1.3. Classified material will never be left unattended. It will be returned to the approved storage container when not being used or when not under the direct control of the user. All classified material will be returned to the authorized storage container at the end of the duty day for proper storage and accountability.

4.1.4. Access and Dissemination of Classified Information

4.1.4.1. Classified information will not be discussed with or under conditions where unauthorized persons could monitor the conversation. The individual controlling the classified information will verify the security clearance, the individual's need-to- know, and ensure a signed SF Form 312, Classified Information Nondisclosure Agreement, is on file before allowing access. See Chapter 3, Industrial Security, for granting access to classified information to contractors.

4.1.4.2. During the handling of classified material, when unidentified persons approach whose security clearance is unknown and their need-to-know is uncertain, cover the classified material and any notes or papers to prevent possible unauthorized disclosure.

4.1.4.3. Access to North Atlantic Treaty Organization (NATO) classified information will be granted on an as-needed basis. Prior to access, the USM will provide the NATO briefing and document the authorization on an AF IMT 2583, Request for Personnel Security Action, and annotate Joint Personnel Adjudication System (JPAS).

4.1.4.4. Access to Critical Nuclear Weapon Design Information (CNWDI) is limited to personnel according to job assignment. Individuals must have final Top Secret or Secret clearance. Access is recorded on AF IMT 2583 and documented in JPAS.

4.1.5. Marking Classified Material

4.1.5.1. All classified information shall be identified clearly by electronic labeling, designation or marking IAW AFI 16-1404 and DoDM 5200.01, Vol 2.

4.1.5.2. ISOO has issued a Marking Booklet to reflect updates in marking procedures for classified national security information resulting from the issuance of Executive Order 13526 and 32 CFR Parts 2001 and 2003. The USM will be able to provide guidance to all personnel.

4.1.5.3. The 70 ISRW does not have any Original Classification Authority (OCA).

4.1.5.4. Derivative classification is the process of determining whether information that is to be included in a document or material has been classified and, if it has, ensuring that it is identified as classified information by marking or similar means. Information is derivatively classified whenever it is extracted, paraphrased, restated, or generated in a new form. Application of classification markings to a document or other material as directed by a security classification guide or other source material is derivative classification. Simply photocopying or otherwise mechanically reproducing classified material is not derivative classification.

4.1.5.5. All cleared personnel who generate or create material that should be derivatively classified are responsible for ensuring that the derivative classification is accomplished IAW DoDM 5200.01, Vol 2.

4.1.6. Reproduction of Classified Material

4.1.6.1. All machines capable of producing copies, to include facsimile machines and digital senders, may be designated for unclassified or classified use. Machines must be authorized (as applicable), labeled for the level of material authorized to be reproduced and obvious to the individual using the copier. Copiers that have the capability of storing images must be properly accredited. Consult the local servicing SSO or IP Office for local procedures governing reproduction and/or use of facsimile and digital sender machines.

4.1.6.2. Stop Do Not Use This Machine for Collateral or SCI Classified Reproduction (or other similar identification), is posted near each machine that cannot be used to reproduce classified material.

4.1.6.3. Use ACCVA 31-1, Authorized to Process Classified Label & ACCVA 31-3, MFD Authorized to Process Classified Poster for machines that are authorized for classified reproduction (or other similar identification).

4.1.7. Storage of Classified Material

4.1.7.1. Store collateral classified information not under the personal control and observation of an authorized person, in a GSA-approved security container, vault, or open storage area meeting the requirements as specified in DoDM 5200.01, Vol 3. NOTE: Storage of SCI will conform to the construction standards in ICS 705-1 and procedures, as dictated, in DoDM 5105.21-V2.

4.1.7.2. Safe combinations will be managed and changed by the safe custodian, who shall be designated in writing by the unit commander.

4.1.7.3. Combinations shall be changed when the container is placed in service whenever an individual knowing the combination to the container no longer requires access, when compromise of the combination is suspected, or when the container is taken out of service or is no longer used to store classified information. Reset the combination lock to the standard combination 50-25-50 and post a sign stating “Not in Service”.

4.1.7.4. After each combination change, complete a new SF 700, Security Container Information form.

4.1.7.4.1. SF 700 Part 1 will be completed and placed in an opaque envelope and marked "Security Container Information". The envelope will be placed inside the safe.

4.1.7.4.2. SF 700 Part 2, will be used. The classification authority block will be marked "Derived From: 32 CFR 2001.80(d) (3)). Declassification upon change of combination." Seal Part 2 and mark at the highest level of classification authorized for the storage container. Part 2 will be stored in a different container of equal to the highest level of classification authorized.

4.1.7.5. The safes will be secured at all times except when material is being placed in or removed from them. SF 702, Security Container Check Sheet, will be annotated each time the safe is opened and closed. The person securing the safe may also verify the locking mechanism. An end-of-day security check to ensure the containers are locked must be completed and annotated on the SF 701, Activity Security Checklist.

4.1.7.6. The safe custodian and USM's will ensure no weapons, funds, drugs or high value items, are stored in the approved containers.

4.1.7.7. Update the Safe Custodian letter and notify the USM when a change of custodian occurs.

4.1.8. Transmission and Transportation

4.1.8.1. Secret and Confidential material can arrive by mail pouch with DD Form 2825 (Accountable Container Receipt) attached. A copy of the receipt will be maintained for file. Controlled mail is considered the following: 1st class, registered, certified and express mail. Controlled mail will be protected as classified and stored in a GSA approved security container until a determination has been made that it does not contain classified.

4.1.8.2. Once the mail recipient determines whom the mail is for, they will make every attempt to contact the individual for notification of immediate pick up. If the individual is not immediately available, the mail recipient will maintain physical control over the mail until it is receipted for. The mail recipient is to determine if classified material is inside, and will open controlled mail, which has not been picked up by the addressee by the end of the day. If classified is present, the USM or assistant USM will be contacted and the material will be placed in a security container.

4.1.8.3. The mail recipient will inspect the envelope seal for tampering.

4.1.9. Courier

4.1.9.1. To transport classified material out of the office area without exiting an installation gate, the individual will obtain the verbal permission of the supervisor. Classified material, which is to be transported from one building to another, is required to be "double" wrapped (or locking courier bag); annotate the inner wrapper with the appropriate classification markings (or cover sheet). There will be no markings denoting classification on the outer wrapper. For further guidance refer to AFI 16-1404, Information Security Program Management, Chap 5 (extract) and DoDM 5200.01, Vol 3, DoD Information Security Program: Enclosure 4, Chap 9-13 (extract).

4.1.9.2. To transport classified material out of the office area where the individual will exit a base gate, the individual must have in their possession a valid DD Form 2501, Courier Authorization issued or authorization letter issued by IP Office, SSO, USM, or alternate USM. Before personnel transport classified material they must receive a briefing from a Security Specialist. The material will be wrapped in the same manner prescribed in AFI 16-1404.

4.1.9.3. While in-transit status (i.e., overnight stops), individuals must make arrangements for secure storage of classified material at a U.S. military facility (i.e., Command Post, Wing Operation Centers), embassy or cleared U.S. contractor facility. Classified material will never be stored in hotel safes.

4.1.9.4. For transmission and transportation of SCI material, contact local the SSO.

4.1.10. Processing Classified Material

4.1.10.1. All classified information will be processed inside of an authorized facility and/or space (i.e., SCIF, Vault, Secure Room or Secure Working Area).

4.1.10.2. Secret Internet Protocol Router Network (SIPRNet) will be used for Secret processing. ***NOTE:*** Prior to installation and utilization of SIPRNet in collateral areas, approval to operate must be obtained by the Wing IP Office and Wing Cybersecurity Office.

4.1.10.3. All personnel must have signed authorization [via DD Form 2875, System Authorization Access Request (SAAR)] for access to the SIPRNet.

4.1.10.4. Authorized users must follow specific instructions for the use of the SIPRNet as outlined in the SIPRNet Standard Operating Procedures.

4.1.10.5. The Joint Worldwide Intelligence Communications (JWICS) or an agency equivalent AIS will be used for Top Secret processing

4.1.11. Open Storage Area

4.1.11.1. Requests for open storage of classified information or recertification of previous areas will be approved, in writing, by Wing CIP. These areas must meet the physical security requirements as outlined in DoDM 5200-01, Vol 3, Appendix to Enclosure 3. NOTE: For SCI, consult with the Host SSO or SSA.

4.1.11.2. The following offices will be contacted prior to construction and/or utilization in order to conduct a site review and grant approval to proceed; IP Office, Civil Engineering, Comm Squadron (EMSEC), Cybersecurity Office (as required), SSO (as required). NOTE: Approval documentation will be kept on file by the USM and a copy provided to the Wing IP Office and any other offices as required.

4.1.11.3. Non-approved electronic devices (cell phones, blackberries, Fitbits, cameras, etc.) are NOT permitted inside the SIPRNet room or any other open storage area or secure room during processing.

4.1.11.4. The door to the SIPRNet room or any secure area will remain secured at all times with appropriate signage posted.

4.1.11.5. Modifications to approved Secure Rooms (i.e. door change, lock change, etc.) will not be made unless authorization has been granted by the IP Office.

4.1.12. Controlled Unclassified Information (CUI). Care should also be taken when destroying CUI. This information includes For Official Use Only; Personal Identification Information; Law Enforcement Sensitive etc. At a minimum, the material will be torn into small pieces to preclude easy reconstitution. The preferred method for destroying CUI is shredding, using the Central Destruction Facility or using the special CUI blue bins controlled by the base recycling program. Reference DoD Manual 5200.01-Volume 4, DoD Information Security Program: Controlled Unclassified Information, for specifics to manage CUI.

4.1.12.1. During working hours, reasonable steps shall be taken to minimize the risk of access by unauthorized personnel (e.g., not reading, discussing, or leaving CUI information unattended where unauthorized personnel are present).

4.1.12.2. After working hours, CUI information may be stored in unlocked containers, desks, or cabinets if Government or Government-contract building security is provided.

4.1.12.3. If such building security is not provided or is deemed inadequate, the information shall be stored in locked desks, file cabinets, bookcases, locked rooms, etc.

4.1.13. Classification Advisory Officer (CAO)

4.1.13.1. Commanders/directors will ensure the following documents receive a classification review by a subject matter expert prior to publishing and/or forwarding to the next appropriate level; Awards Packages, EPR/OPR, Decoration Packages, and unit papers, articles, reports, briefings, resumes, etc. that are planned for public release

4.2. Disposal and Destruction

4.2.1. Form Requirements. For SECRET and CONFIDENTIAL material, no receipt is required to certify destruction.

4.2.2. Destruction Requirements. Classified documents and material identified for destruction shall be destroyed completely, to prevent anyone from reconstructing the classified information.

4.2.2.1. The SSA has a burn bag policy requirement. Classified paper material will be placed in a burn bag and sealed. Mark the bag with the highest classification of the material being destroyed and annotate office symbol and phone number. The burn bag must be stored and protected as classified pending destruction.

4.2.2.2. Other methods and equipment used to routinely destroy classified information include crosscut shredding, wet pulping, mutilation, chemical decomposition or pulverizing. Methods used for clearing, sanitization or destruction of classified IT equipment and media include overwriting, degaussing, sanding, and physical destruction of components or media.

4.2.2.3. The Evaluated Products List (EPL) contains high security destruction devices evaluated by the SSA that meet the performance requirements of High Security Crosscut Paper Shredder Specifications. The table on page two identifies High Security Crosscut Combination Optical and Paper Shredders; additional tables are High Security Crosscut Paper Shredders only. Inclusion of a product in the EPL is not an endorsement by SSA or the U.S. Government. Contact the IP Office or SSO/SSA for most current approved listing.

4.3. End of Day Security Checks

4.3.1. End-of-day security checks are required in areas where classified is processed or stored. End-of-day security checks will be documented on the SF 701, Activity Security Checklist. Security container openings, closings and after-hour checks will be documented on the SF 702. NOTE: For co-located units that operate within an SCI environment, local SSA policy and procedures will be followed.

4.3.2. All personnel within their respective sections will check their area of operations for secure close-out procedures and annotate the SF 701, Activity Security Checklist. Double check to ensure the container is locked and annotate on SF Form 702, Security Container Check Sheet. The last member out will conduct an end-of-day security sweep of their entire area, and then enter time and initials on the SF 701. The using office will maintain completed SF Forms 701 and 702 until the forms are filled; then destroyed after 90 days.

4.3.3. All personnel are responsible to check their areas prior to departing for the day. Ensure all lights are turned off; doors and windows are to be secured, including restrooms if applicable. Ensure all computers are shut down (if stand-alone systems). Make sure CUI (including PII, FOUO etc.) is protected properly IAW DoDM 5200.01, Vol 4. Make sure CAC cards are not left in workstations and any otherwise compromising situation is not left unattended. First Class mail will be secured.

4.4. Emergency Procedures. Personnel will provide protection for classified material in a manner that will minimize the risk of injury or loss of life. In the case of fire or natural disaster, persons in the immediate vicinity of the safe will verify the safe is locked before leaving the area if possible. Personnel having classified material in their possession when an alarm sounds will:

4.4.1. Secure the material in the security container if time permits without personal risk.

4.4.2. Hand carry and provide personal security for classified documents when leaving the building and at the assembly area.

4.4.3. Retain possession of the documents until you return to the work area. After returning, normal operating procedures for safety and security of classified documents apply.

4.4.4. In the event you cannot return to the work area, secure the material in another container.

4.4.5. In accordance with the Emergency Action Plan, if an emergency arises requiring destruction of the classified holdings, the priority of destruction shall be: Top Secret first, Secret second, and Confidential last.

Chapter 5

SECURITY EDUCATION, TRAINING AND AWARENESS (SETA)

5.1. Initial Training. Supervisors will ensure every newly assigned person in-processes with the USM and receives initial security training, in accordance with DoDM 5200.01, Vol 1 and AFI 16-1404. This can be accomplished by having members complete the DoD Initial Orientation and Awareness Training (**https://securityawareness.usalearning.gov/**). NOTE: This training covers the training listed in paragraph 5.2.2.-5.2.4.

5.2. Mandatory Training. The training listed below is required within 60 days of signing into the unit. NOTE: Some training may be locally produced (PowerPoint), completed via CDSE website or SSA Computer Based Training (CBT) so long as it meets the requirements listed in section 5.1. Refer to Chapter 10 for mandatory Insider Threat training.

5.2.1. DoD IAA Cyber Awareness Challenge

5.2.2. Access to Classified Training

5.2.3. Marking Classified Training

5.2.4. Derivative Classified Training

5.2.5. Unauthorized Disclosure Training (required for personnel indoctrinated into SCI)

5.3. Annual Refresher Training. The USM will ensure refresher training is completed annually for all unit personnel as listed below:

5.3.1. DoD IAA Cyber Awareness Challenge

5.3.2. Derivative Classification Training

5.3.3. Unauthorized Disclosure Training

5.3.4. Local threat and techniques used by foreign intelligence activities, penalties for engaging in espionage and other unauthorized disclosures, relevant changes in information security policy or procedures, and issues/concerns identified during Wing IP program reviews.

5.4. Tracking of Training. USMs will have a tracking mechanism documenting completion of initial and annual training (i.e. ADLS certificates, read receipt, sign-in log, or spreadsheet) to show the type of training, name of individual, and date the training was completed.

5.5. USM Training. USMs must complete the DSS Air Force Security Manager Curriculum training within 90 days of assuming duties. The following set of courses are mandatory and provides an introduction to common DoD security disciplines encountered while performing duties as a security manager, assistant security manager, or security assistant.

5.5.1. Block I – All training identified in section 5.2. of this Operational Instruction.

5.5.2. Block II – (AF Security Manager Curriculum) **http://www.cdse.edu/stepp/index.html**

5.5.2.1. Introduction to Industrial Security IS011.06 and Exam IS011.16

5.5.2.2. Introduction to Information Security IF011.06 and Exam IF011.16

5.5.2.3. Introduction to Personnel Security PS113.06 and Exam IF113.16

5.5.2.4. Marking Classified Information IF105.06 and Exam IF105.16

5.5.2.5. Storage Containers and Facilities PY105.06 and Exam PY105.16

5.5.3. Block III - **http://www.cdse.edu/stepp/index.html**

5.5.3.1. JCAVS User Levels 2-6: PS183.16

5.5.3.2. Identifying/Safeguarding Personally Identifiable Information DS-IF101.06

5.5.4. Block IV – Localized hands-on training for JPAS, e-QIP and local security procedures.

Chapter 6

SECURITY INCIDENTS

6.1. Personnel Reporting Procedures . If an individual suspects a security incident has occurred, they must immediately safeguard the material involved and notify their Commander, supervisor, USM and/or SSO/SSR using secure communication when making the notification if possible. Only provide the basic details necessary until more detailed briefing can be accomplished.

6.2. USM Reporting Procedures. The USM will notify the SSO and/or IP Office by the end of the first duty day using the "Security Incident Data Reporting Template" (see Attachment 4). The USM will report the incident to appropriate Cybersecurity Liaison (CL) by the end of the first duty day.

6.3. USM/CAO Review. The USM must verify via Classified Advisory Officer (CAO) verify information is classified prior to appointing an inquiry official.

6.4. Appointing an Inquiry Official . Commanders shall appoint an inquiry official, in writing within two duty days from the discovery of the security incident. These individuals will be a minimum of E-7 or GS-09 equivalent or above or commissioned officer. The USM, members assigned to the IP Office or the SSO/SSR cannot perform IO duties. The USM will obtain a security incident number from the IP Office. The USM will then create a memorandum for the Unit Commander to appoint an inquiry official. Inquiry official shall:

6.4.1. Consult and receive guidance from the IP Office (Collateral) or SSO (SCI)

6.4.2. Complete inquiry within 10 duty days or ask for an extension from Commander

6.4.3. Determine and report facts

6.4.4. Make conclusion whether or not classified information was actually compromised, potentially compromised, suspected loss, no compromise

6.4.5. Characterize incident as a Security Infraction or Violation

6.4.6. Recommend actions to prevent future incidents

6.4.7. Answer all questions listed in DoDM 5200.01, Vol 3, Enclosure 6

6.5. Commander Responsibility. Commanders approve, endorse, and close inquiry reports after review by the IP Office. In approvals, endorsements, and closures to reports Commanders address: Concurrence in whole or part with findings, if an actual, potential or suspected loss or compromise occurred or did not occur and whether or not further investigation is needed. Commanders must indorse corrective actions to prevent further occurrences and if administrative, disciplinary or punitive actions taken against individual(s) responsible for the violation are warranted to include establishing a Security Information File (SIF).

Chapter 7

SELF-ASSESSMENTS

7.1. General. As a minimum, an annual self-assessment of the unit security program will be conducted by the USM. This may be further supplemented (quarterly, semiannually) as directed by the unit commander, Wing IP Office, or SSA.

7.1.1. Upon request, ensure copies of all completed self-assessments, to include HHQ inspections and annual program reviews, are forwarded to the Wing IP Office.

7.1.2. Utilize the self-assessment checklists provided in the Management Internal Control Toolset (MICT) to complete the self-inspection. At a minimum, USMs will complete the Information Security Program (for units that create, store, or handle classified information) and Personnel Security Program checklists. The Industrial Security Program checklist will be used when contractors are assigned to the unit.

7.1.3. Designated SSO/SSR's will complete the AFMAN 14-304, The Security, Use, and Dissemination of Sensitive Compartmented Information and Personnel Security Program checklists. NOTE: The Information Security Program checklist will be completed if there are applicable collateral security areas.

7.2. Local Information Protection Program Reviews. The Wing Chief, Information Protection (CIP) will conduct an annual local inspection of unit security programs IAW AFI 90-201, The Air Force Inspection System and Air Combat Command Supplement (ACCSUP) to AFI 16-1404, Chapter 10, using MICT and applicable DoD/AFI/SSA program guidance. A copy of this report will be provided to the inspected organization commander and USM. If the organization has received a HHQ inspection during the current fiscal year, an annual review will not be conducted. NOTE: GSUs are subject to their host base MOA or IP Office guidelines.

7.3. Staff Assistance Visits. The Wing CIP will conduct staff assistance visits when requested.

Chapter 8

PHYSICAL SECURITY

8.1. Visitor Control. For visitors who require access to classified information or facilities, verify the individual's clearance eligibility, need-to-know, and identification card (preferably a driver's license or identification (ID) with a photograph and SF 312 in JPAS, or visitor access request (VAR). NOTE: The USM or Security Specialist are the authorized authenticating officials and will determine the need for escort(s).

8.2. Access Control. Entry to all SCIFs, Controlled and Restricted Areas will be monitored. Individuals without the required level of clearance will be escorted at all times while in the area. Contact your servicing SSO for local procedures and further guidance.

8.3. Badge Control.

8.3.1. Intelligence Community (IC) badges must be worn and visibly displayed at all times within SSA facilities and/or controlled areas. When departing these areas, badges will be secured out of view.

8.3.2. Badges will be used for official purposes only. DO NOT use badges as personal identifiers for government employment or similar purposes.

8.3.3. Badges will not be left in vehicles or any other location where it may be vulnerable to loss, damage, or theft.

8.3.4. For 70 ISRW affiliated units within the Air Force District of Washington (AFDW) locale: Badges are not authorized to be utilized at other IC locations outside of AFDW (Exception: IC Staff Badges). Members MUST report to the Visitor Center and drop off their badge where it will be secured while they are TDY.

8.3.4.1. If visiting other IC locations, ensure you are sponsored and have the appropriate VAR submitted.

8.3.4.2. GSUs: Contact your local SSO, SSA, or USM for guidance.

8.3.5. If you lose your IC badge, notify your SSO/USM and report to the nearest Visitor Center and complete any local forms.

8.4. Classified Meetings and Conferences . Meetings and conferences involving classified information in non-secure areas (not inside of a SCIF, Vault or Secure Room) present special vulnerabilities to unauthorized access and/or disclosure. To aid and assist commanders, DoDM 5200.01, Vol 3, Enclosure 2 and AFI 16-1404, Attachment 4, Classified Meeting, Briefing, Conference Checklist will be utilized for reference. Security managers are responsible for accomplishing the checklist unless the commander or director has delegated the responsibility to another individual.

Chapter 9

FOREIGN TRAVEL

9.1. General. All official government and/or personal foreign travel must be reported to the Security Specialist and USM at least 30 days prior to your departure, unless circumstances dictate otherwise. This includes travel to Mexico, Canada, or Bahamas.

9.2. Contractors. Contractors shall contact their Facility Security Officer (FSO) to meet National Industrial Security Program (NISPOM) reporting requirements. As a courtesy it is recommended contractors notify their USM and/or commander.

9.3. SCI/SAP Briefed. Anyone who is Sensitive Compartmented Information (SCI) and/or Special Access Program (SAP)-briefed must also report their foreign travel at least 30 days in advance to the SSO and SSA per Intelligence Community Standard (ICS) 703. NOTE: Failure to report foreign travel to the appropriate offices may result in reevaluation of eligibility for continued SCI access.

Chapter 10

INSIDER THREAT PROGRAM

10.1. General. An insider threat is anyone with authorized access to the information or things an organization values most, and who uses that access -- either wittingly or unwittingly -- to inflict harm to the organization or national security. When an insider becomes a threat, it can have far-reaching consequences on both the Wing and national security.

10.1.1. The WikiLeaks case represented one of the major catalysts for the insider threat national policy.

10.1.2. While some insiders volunteer, others are targeted and recruited by adversary groups. For this reason, it is each member's responsibility to be aware of common signs someone is being recruited. Not all of the following indicators will be evident in every insider threat and not everyone who exhibits these behaviors is doing something wrong. However, most of the insider threats discovered displayed at least some of the indicators below. It is important for each member to be aware of these behaviors so we can combat the insider threat and protect our organization and the country.

10.2. Recruitment Indicators. Reportable indicators of recruitment include, but are not limited to:

10.2.1. Unreported request for critical assets outside official channels

10.2.2. Unreported or frequent foreign travel

10.2.3. Suspicious foreign contacts

10.2.4. Contact with an individual who is known to be, or is suspected of being, associated with foreign intelligence, security, or terrorism

10.2.5. Unreported offer of financial assistance, gifts, or favors by a foreign national or stranger: Beware of those bearing gifts

10.2.6. Suspected recruitment by foreign or domestic competitive companies to convince employee to work for another company

10.3. Information Collection Indicators. Reportable indicators of information collection include, but are not limited to:

10.3.1. Unauthorized downloads or copying of files, especially for employees who have given notice of termination of employment

10.3.2. Keeping critical assets at home or any other unauthorized place

10.3.3. Acquiring access to automated information systems without authorization

10.3.4. Operating unauthorized cameras, recording devices, computers, or modems in areas where critical assets are stored, discussed, or processed

10.3.5. Asking you or anyone else to obtain critical assets to which the person does not have authorized access

10.3.6. Seeking to obtain access to critical assets inconsistent with present duty requirements

10.4. Information Transmittal Indicators . Reportable indicators of information transmittal include, but are not limited to:

10.4.1. Removing critical assets from the work area without appropriate authorization

10.4.2. Using USB storage devices to remove information from Automated Information Systems

10.4.3. Extensive use of copy, facsimile, or computer equipment to reproduce or transmit critical asset-related information that may exceed job requirements

10.4.4. Discussing critical asset-related information in public or on a non-secure telephone

10.4.5. Actions/behaviors specific to classified information:

10.4.5.1. Using an unauthorized fax or computer to transmit classified information

10.4.5.2. Attempting to conceal any work-related foreign travel and any personal foreign travel while having a Top Secret/Sensitive Compartmented Information clearance or being a contractor with a reporting requirement

10.4.5.3. Improperly removing the classification markings from documents

10.5. General Suspicious Behaviors. Reportable indicators of other suspicious behavior include, but are not limited to:

10.5.1. Attempts to expand access:

10.5.1.1. Attempting to expand access to critical assets by repeatedly volunteering for assignments or duties beyond the normal scope of responsibilities

10.5.1.2. Performing repeated or unrequired work outside of normal duty hours, especially unaccompanied

10.5.2. Questionable behavior:

10.5.2.1. Exhibiting behavior that results in repeated security violations

10.5.2.2. Engaging in illegal activity or asking you to engage in any illegal activity

10.5.3. Changes in financial circumstances:

10.5.3.1. Unexplained affluence not explained by situations such as an inheritance, luck in gambling, a successful business venture, etc.

10.5.3.2. Displaying sudden reversal of financial situation or sudden repayment of large debts

10.5.4. Attempts to compromise individuals:

10.5.4.1. Attempting to entice personnel with access to critical assets into situations that could place them in a compromising position

10.5.4.2. Attempting to place personnel with access to critical assets under obligation through special treatment, favors, gifts, money, or other means

10.5.5. Questionable national loyalty:

10.5.5.1. Displaying questionable loyalty to U.S. government or company

10.5.5.2. Making anti-U.S. comments

10.5.6. Exhibits actions or behaviors associated with disgruntled employees:

10.5.6.1. Conflicts with supervisors and coworkers

10.5.6.2. Decline in work performance

10.5.6.3. Tardiness

10.5.6.4. Unexplained absenteeism

10.6. Reporting Procedures . If you suspect a possible insider threat, recruitment by a foreign entity, or espionage, you must report it to your local security office, AFOSI, FBI or counterintelligence officials.

10.7. Required Training. Insider threat program personnel will receive training to ensure adherence to privacy, whistleblower, records retention, civil liberties, and information sharing requirements. Additionally, commanders and supervisors will ensure insider threat training is provided to assigned personnel within 30 days of assignment or hire and annually thereafter. **NOTE:** This may be conducted via briefings, PowerPoint, or the CDSE website.

MATTEO G. MARTEMUCCI, Colonel, USAF
Commander

Attachment 1

GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

References

ACC SUPPLEMENT to AFI 16-1404, Information Security Program Management, 20 Nov 2015

AFI 16-1402, Insider Threat Program Management, 5 August 2014

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

AFI 31-501 (Changing to AFI 16-1405), Personnel Security Program Management, 27 January 2005, Incorporating through Change 2, November 29, 2012

AFI 16-1406, Air Force Industrial Security Program Management, 25 August 2015

DoDM 5105.21-V2, Sensitive Compartmented Information (SCI) Administrative Security Manual: Administration of Physical Security, Visitor Control, and Technical Security, 19 October 2012

DoDM 5200.01-V1, DoD Information Security Program: Overview, Classification, and Declassification, 24 February 2012

DoDM 5200.01-V2, DoD Information Security Program: Protection of Classified Information,

24 February 2012

DoDM 5200.01-V3, DoD Information Security Program: Marking of Classified Information, 24 February 2012

DoDM 5200.01-V4, DoD Information Security Program: Controlled Unclassified Information (CUI), 24 February 2012

DoDM 5200.02, DoD Procedures for the Personnel Security Program, 3 April 2017

ICS 705-1, Physical and Technical Security Standards for Sensitive Compartmented Information Facilities, 17 September 2010

Adopted Forms

AF IMT 310, Document Receipt and Destruction Certificate, 1 November 1995

AF IMT 1109, Visitor Register Log, 1 May 1999

AF IMT 2583, Request for Personnel Security Action, 04 April 2014

AF IMT 2587, Security Termination Statement, 1 September 1981

AF Form 847, Recommendation for Change of Publication, 22 September 2009

DD Form 254, DoD Contract Security Classification Specification, December 1999

DD Form 2501, Courier Authorization, March 1988

DD Form 2825, Internal Receipt, June 2000

DD Form 2875, System Authorization Access Request (SAAR), August 2009

SF Form 311, Agency Security Classification Management Program Data, February 2015

SF Form 312, Classified Information Nondisclosure Agreement, July 2013

SF Form 701, Activity Security Checklist, November 2010

SF Form 702, Security Container Check Sheet, November 2010

SF Form 704, Secret (Cover Sheet), August 1985

SF Form 705, Confidential (Cover Sheet), August 1985

Abbreviations and Acronyms

AFDW—Air Force District of Washington

AFI—Air Force Instruction

AFOSI—Air Force Office of Special Investigations

CEP—Continuing Evaluation Program

CIP—Chief, Information Protection

COR—Contracting Officer Representative

CUI—Controlled Unclassified Information

DoD—Department of Defense

FBI—Federal Bureau of Investigations

IC—Intelligence Community

JPAS—Joint Personnel Adjudication System

PSO—Personnel Security Office

USM—Unit Security Manager

SCI—Sensitive Compartmented Information

SSA—Security Service Activity

SSR—Special Security Rep

SSO—Special Security Office(r)

STE—Secure Terminal Equipment

WCO—Wing Cybersecurity Office

Attachment 2

SECURITY INCIDENT DATA REPORTING TEMPLATE

Figure A2.1. Security Incident Data Reporting Template.

NOTE: Once filled in, classify the report according to the information contained herein and handle/distribute accordingly.

1. Date/Time Incident Reported:

2. Name/Rank or Grade of Individual Reporting Incident:

3. Organization/Office Symbol of Individual Reporting Incident:

4. Type of Incident: (Unauthorized Access, Information Technology Data Spillage, IT Classified Message Incidents (CMI), Improper Classification Action, Improper Storage, Improper Transmission, Unauthorized Reproduction, Other)

5. Level of Classified Involved: (Confidential, Secret, Top Secret, SCI)

6. Synopsis of Incident:

a. WHO:

b. WHEN:

c. WHERE:

d. WHAT:

e. WHY:

7. Commander Notified:

8. Actions Taken:

Attachment 3

SAMPLE MEMORANDUM FOR APPOINTMENT OF SAFE CUSTODIANS

Figure A3.1. Sample Memorandum for Appointment of Safe Custodians.

MEMORANDUM FOR [Security Office] [Date]

FROM: [Unit]

SUBJECT: Appointment of Classified Storage Container Custodians

1. IAW AFI 16-1404, Information Security Program Management, para. 2.7.11., and TO 00-20F-2, Procedures For Classified Storage Containers, the following individuals have been appointed as the primary and alternate Classified Storage Container Custodians for the security container ([Container #]) belonging to [Unit].

Rank	Name	Pri/Alt	Phone

2. In addition to the custodians identified above, the following individuals are granted to the classified storage container and meet the security clearance requirements to include possessing a valid need to know and have executed a SF312, as verified in the Joint Personnel Adjudication System (JPAS).

Rank	Name	Phone

3. Only the personnel listed on this letter are authorized unescorted access to the classified storage container. Security clearances and the need to know will be verified prior to access being granted to anyone without the combination to the security container.
4. This letter supersedes all previous memorandums, same subject.

SIGNATURE BLOCK
[Unit/CC]

Attachment 4

MEMORANDUM FOR CONTAINER LISTING

Figure A4.1. Memorandum for Container Listing.

MEMORANDUM FOR [Security Office] [Date]

FROM: [Unit]

SUBJECT: Classified Container Listing

1. IAW DoDM 5200.01, DoD Information Security Program: Protection of Classified Information, Vol. 3, Enclosure 3, para. 10., a record must be maintained for each container, or vault or secure room door, used to storing classified information. [Unit name] is responsible for the following security container(s):

UNIT	MODEL STYLE	TYPE OF CONTAINER	BRAND NAME	SERIAL NUMBER	EXACT LOCATION	CUSTODIAN NAME ALTERNATE CUSTODIAN NAME	LAST COMBO CHANGE
Unit	GSA	2 Drawer	Hamilton	4565G	Bldg 9805	XXX XXX	13 Aug 16

SIGNATURE BLOCK
[Unit/CC or USM]

Attachment 5

COURIER BRIEFING FOR HAND-CARRYING CLASSIFIED MATERIAL

Figure A5.1. Courier Briefing For Hand-Carrying Classified Material.

1. Directive:

a. Per AFI 16-1404, Information Security Program Management, Chap 5, para 5.3.2 Commanders and Directors determine the need and proper method to be used by each individual authorized to escort, courier, or hand-carry classified material on or off the installation, and establish procedures to ensure hand-carrying classified material is minimized to the greatest extend possible and does not pose unacceptable risk to the information. (T-0) Refer to DoDM 5200.01, Vol 3, Enclosure 4, for additional guidance on Escort, Courier, or Hand-Carry of Classified Material authority, packaging requirements, and responsibilities, arrangements with customs, police and/or immigration officials, disclosure authorization, authorizations statements, and transporting classified information on commercial aircraft.

b. Please ensure you read this briefing and the AFI/DoDM extracts very carefully to ensure you fully understand your role, responsibilities, and requirements for transporting classified materials both on and off-base.

c. When required to transport classified materials off the installation please ensure you contact a USM prior to departing to ensure required forms, inventories, and authorizations are completed.

2. Couriers of classified material will:

a. Conduct themselves throughout the shipment operation in such a manner that security of classified material entrusted to them will not be jeopardized through carelessness or lack of vigilance.

b. Accept custody of classified material by signing a valid receipt and release custody of the material to consignee at the destination, after obtaining a receipt from a properly cleared and identified individual.

c. Ensure all classified material is properly packaged (double wrapped) or otherwise protected from viewing in accordance with DoDM 5200.01/AFI 16-1404 prior to transportation outside the facility or government property

d. Carry the classified material on their person or in approved containers until delivered to designated addressee.

e. Keep the material under constant surveillance and continually be in a physical position to exercise direct control over the material at all times.

f. Maintain continuous alertness for the presence of conditions or situations that might jeopardize the security of the material.

g. In the event of an emergency which immobilizes their vehicle, request assistance from the nearest government installation or cleared facility with storage capability to provide storage and protection.

h. In the event an overnight stop is required, ensure the classified material is kept under the constant surveillance of another cleared individual or placed in secure storage at the nearest government installation or cleared facility.

i. Ensure that when classified material is carried in any private, public or government conveyance, the material is not placed in any detachable compartment.

3. Couriers of classified material will NOT:

a. Use intoxicants or drugs (controlled or prescription) that may impair their judgment or physical ability to maintain constant alertness.

b. Engage in any activity that may distract their attention from their primary responsibility of protection of the classified material.

c. Read, study or display in any manner, classified material in public conveyances or places.

d. Make any unnecessary stops along the route of travel.

CLASSIFIED MATERIAL COURIER CERTIFICATION

I certify that I have read or been briefed, understand and agree to abide by the information contained in this Classified Material Courier Briefing to include Attach 1 and Attach 2. I fully understand that the classified material in my possession is my responsibility until released to a properly cleared and authorized individual either at my end destination or return to my work center and that any willful violation of these procedures may result in disciplinary action. I understand that my duties as courier will expire one year from the date below.

SIGNATURE OF COURIER DATE

Attachment 6

SAMPLE COURIER LETTER

Figure A6.1. Sample Courier Letter.

MEMORANDUM FOR WHOM IT MAY CONCERN [Date]

FROM: [Unit]

SUBJECT: Designation of Official Courier: (XXX-XX-XXXX)

1. The above member(s), XXth Intelligence Squadron, Location, is designated an official courier for the United States Government. Upon request, he will present his official identification card (License or State ID) bearing the number XXX (or other appropriate identification media).

2. The above member(s) is hand-carrying classified material that should not leave their person.

3. This courier designation can be confirmed by contacting the undersigned at contact number(s). This letter expires one year from date of issuance.

_____ _____

SIGNATURE OF SECURITY SPECIALIST DATE

_____

PRINTED NAME OF SECURITY SPECIALST

If additional information is required, please contact the [Unit] at commercial contact number