

**1 OCTOBER 2002**



*Security*

**INFORMATION SECURITY PROGRAM  
MANAGEMENT**

**COMPLIANCE WITH THIS PUBLICATION IS MANDATORY**

---

**NOTICE:** This publication is available digitally on the AFDPO WWW site at:  
<http://www.e-publishing.af.mil>

---

OPR: 22 SFS/SFAI (SSgt Travis B. Greene)  
Supersedes MAFBI 31-401, 5 April 1996

Certified by: 22 SFS/CC (Major Robert H. Behrens)  
Pages: 24  
Distribution: F

---

This instruction establishes requirements/procedures for managing the information security program on McConnell Air Force Base (MAFB), Kansas, as required by Department of Defense (DOD) 5200.1-R, *Information Security Program*; Air Force Policy Directive (AFPD) 31-4, *Information Security*; and Air Force Instruction (AFI) 31-401, *Information Security Program Management*. It establishes policies and procedures for effective management of information security programs at the wing, group, and squadron level, and assigns specific responsibilities to commanders and unit security managers. Chapters 6 and 12 contain reference to the punitive provisions contained in AFI 31-401 and DOD 5200.1-R. This instruction applies to all personnel (active military, Department of the Air Force civilian, or reserve) assigned, attached, or visiting the 22d Air Refueling Wing or 931st Air Refueling Group (AFRES). Personnel who violate this instruction are subject to disciplinary action under Article 92 of the *Uniform Code of Military Justice (UCMJ)*, as prescribed in DOD 5200.1-R and AFI 31-401.

**SUMMARY OF REVISIONS**

Provides a detailed list of unit security manager's responsibilities (paragraph 1.5.); changes procedures for annual program reviews (paragraph 1.6.); changes requirements for unit self-inspections (paragraph 1.8.); lists procedures for marking and declassifying exercise data (paragraph 2.4.); changes secure room certification procedures (paragraph 5.1.); designates the Command Post as the primary point of contact for storage of all transient classified materials (paragraph 5.2.); changes the requirements for use of the Standard Form 702 (paragraph 5.3.2.); establishes new procedures for the storage of classified aboard aircraft (paragraph 5.5.); establishes and delegates responsibilities for the base Central Destruction Facility (CDF) (paragraph 5.7.); establishes an annual classified clean-out week (paragraph 5.9.3.); establishes subject areas for security education training AFI 31-401 (Chapter 8), and provides a sequence of events for security incident inquiries AFI 31-401 (Chapter 9). **A bar ( | ) indicates a change since the last edition.**

|    |                               |   |
|----|-------------------------------|---|
| 1. | Program Management. ....      | 3 |
| 2. | Classifying Information. .... | 5 |

|  |   |           |
|--|---|-----------|
| 3.   | Declassifying, Downgrading or Upgrading Information. ....                                       | 6         |
| 4.   | Marking. ....   | 7         |
| 5.   | Safekeeping and Storage. ....   | 7         |
| 6.   | Transmitting Classified Information. ....   | 12        |
| 7.   | Special Access Programs (SAPs). ....  | 12        |
| 8.   | Security Education and Training. ....   | 13        |
| 9.   | Compromise of Classified Information. ....  | 14        |
| 10.  | Access, Dissemination, and Accountability ....  | 15        |
| 11.  | Foreign Government Information – North Atlantic Treaty Organization (NATO)<br>Information: .... | 16        |
| 12.  | Administrative Sanctions. ....  | 17        |
| 13.  | Unclassified Controlled Nuclear Information (UCNI). ....  | 17        |
| 14.  | Industrial Security Program. ....   | 17        |
| <b>Attachment 1— GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION</b> |   | <b>19</b> |
| <b>Attachment 2— EMERGENCY PROTECTION/REMOVAL PLANS</b>                |   | <b>21</b> |
| <b>Attachment 3— (APPROPRIATE LETTERHEAD)</b>                          |   | <b>22</b> |
| <b>Attachment 4— COVER SHEET</b>                                       |   | <b>23</b> |
| <b>Attachment 5— INQUIRY OFFICIAL APPOINTMENT LETTER</b>               |   | <b>24</b> |

## 1. Program Management.

1.1. Commander, 22d Air Refueling Wing (22 ARW/CC). 22 ARW/CC retains overall responsibility for establishing and implementing the Information Security Program and designates the Chief, Security Forces (CSF) the Information Security Program Manager (ISPM) per AFI 31-401, paragraph 1.3.4.

1.2. Chief, Security Forces:

1.2.1. The CSF is directly responsible to the wing commander, in the capacity of the ISPM.

1.2.2. Appoints the Information Security Manager (ISM) for McConnell AFB.

1.2.3. Ensures viable unit security manager training, education, inspection/review, and information security programs are established.

1.2.4. Provides technical reviews and advice to unit commanders concerning security incident reports and their information security programs.

1.3. Installation Security Manager (ISM): The ISM is directly responsible to the CSF and will:

1.3.1. Develop and conduct unit security manager training, education, inspection/review, and information security programs.

1.3.2. Plan, coordinate, and conduct quarterly security managers' meetings.

1.3.3. Maintain appropriate training material and lesson plans and conduct indoctrination training for newly appointed security managers within 90 days of their appointment.

1.4. Unit Commanders:

1.4.1. Ensure a viable unit security program is in place by appointing a primary NCO and alternate (any rank) unit security manager. Provide the ISM a copy of the appointment letter.

1.4.2. Ensure unit security managers receive indoctrination training upon appointment and attend a formal training class within 90 days of appointment.

1.4.3. Appoint inquiry officials for security incidents in accordance with this instruction and AFI 31-401, as supplemented.

1.4.4. Close inquiry reports as prescribed in DOD 5200.1-R, AFI 31-401 (as supplemented), and this instruction.

1.5. Unit Security Managers:

1.5.1. Implement and manage the security program for their respective units.

1.5.2. Develop and update unit security operating instructions annually.

1.5.3. Advise the unit commander on security issues pertaining to the unit (i.e., security incidents, special information files, temporary suspensions, etc.)

1.5.4. Attend the quarterly security managers meetings.

1.5.5. Plan and conduct annual security training for all personnel assigned to the unit.

1.5.6. Report ALL actual and suspected security incidents immediately to the ISM.

1.6. Program Reviews:

1.6.1. The ISPM shall determine the frequency of program reviews. A schedule shall be produced annually by the ISM, approved by the ISPM. The schedule will reflect an annual review of units that possess, process, control, transmit, or store classified information, and a biennial review of units that have no routine contact with classified materials.

1.6.2. Units on a biennial schedule will be issued a letter, from the ISPM, reflecting this change. The letter is to be placed within the unit security manager's handbook under the program reviews section. This letter will not be removed unless superseded.

1.6.3. The annual program review may serve as one of the required self-inspections. Annual program reviews will require a written response from the unit commander for any corrective actions implemented.

1.6.4. The ISM will maintain a six-part folder for each unit participating in the wing program. The six-part folder will contain designation letters, recent program review, designated secure area information, container listing, and Top Secret Control Officer letter. Mark the folder and its contents "For Official Use Only."

#### 1.7. Security Manager Meetings:

1.7.1. The ISM will plan, coordinate, and conduct meetings on a quarterly basis. The ISM shall chair and appoint a recorder for the meetings.

1.7.2. Distribute meeting minutes to the wing and group commanders and all attendees.

1.7.3. Attendance at quarterly security manager meetings is mandatory. The primary (or alternate) security manager will attend. The unit commander must ensure a unit representative attends the meeting if both the primary and alternate security managers are unable to. The ISPM will notify commanders in writing if their organization misses two consecutive meetings.

1.7.4. The meetings are open to anyone wishing to attend or address the unit security managers.

#### 1.8. Unit Security Program Management:

1.8.1. The unit security manager will maintain a security manager's handbook. The handbook will be formatted as outlined below:

1.8.1.1. Appointment/designation letters. These letters identify primary/alternate unit security managers, TSCOs, safe/vault/open/unattended storage area custodians along with locations of classified safes/shredders/copiers, etc.

1.8.1.2. Security Operating Instruction (OI). The OI should be designed to cover all security-related issues within the unit and be reviewed/updated annually.

1.8.1.3. Self-inspection Letters and Reports. Maintain inspection official appointment letters, inspection reports, and commander's review letters including approval/disapproval of corrective actions. Self-inspections will be conducted semi annually.

1.8.1.4. Information security program reviews conducted by the ISM. Maintain only the last report.

1.8.1.5. Quarterly meeting minutes. Maintain four consecutive quarterly minutes.

1.8.1.6. Training materials. The ISM or the unit may generate these materials.

1.8.1.7. Central Adjudication Verification System (CAVS) rosters (Military, IMA, and Civil-

ian). The roster may be kept for 90 days if it is updated with information received from the Personnel Data System or ISM. The roster is considered outdated and inaccurate if maintained longer than 90 days.

1.8.1.8. Self-inspection checklists.

1.8.1.9. Miscellaneous items. Periodic updates received from the ISM should be maintained in this section. Only retain items that are of value to the unit.

1.8.2. The unit security manager is responsible for monitoring the personnel security and industrial security programs for his/her commander. They shall maintain publications governing all security programs (Information, Industrial, Personnel, and Physical) and will have the following publications readily accessible:

1.8.2.1. DOD 5200.1-R, *Information Security Program*.

1.8.2.2. DOD 5200.2-R, *Personnel Security Program*.

1.8.2.3. AFD 31-4, *Information Security*.

1.8.2.4. AFD 31-5, *Investigations, Clearances, and Access Requirements*.

1.8.2.5. AFI 31-401, *Managing the Information Security Program*.

1.8.2.6. AFI 31-501, *Personnel Security Program Management*.

1.8.2.7. All applicable AMC supplements to the aforementioned publications.

1.8.2.8. Publications governing physical security programs, e.g., AFI 31-101, *The Air Force Physical Security Program*, MAFBI 31-101, Base Security Instruction, and MAFB OPlan 31-209, Base Resource Protection Plan (The Installation Security Plan is in Annex M).

1.8.3. The AFVA 205-11, *Your Security Manager Is*, will be posted conspicuously throughout the unit.

1.8.4. Unit security managers will maintain a sufficient supply of forms necessary to perform all facets of the security programs.

## 2. Classifying Information.

2.1. Original Classification Authority (OCA). There is no original classification authority on McConnell AFB.

2.2. Challenges to Classification:

2.2.1. Anyone may challenge information for the following reasons:

2.2.1.1. The information was incorrectly classified.

2.2.1.2. The information should no longer be classified.

2.2.1.3. The information should be classified, or classified at a higher level.

2.2.2. Unit security managers will process challenges through the ISM by obtaining views from personnel with technical knowledge of the subject matter or a functional interest in the information. Unit security managers will allow challengers to remain anonymous, if so desired. The request will be honored as long as practical.

2.2.3. Unit security managers shall follow paragraph 2.2.2. when derivative classification or information classified by compilation is challenged. They may also consult each OCA and office of primary responsibility (OPR) listed for the information under challenge.

2.2.4. Protect the material in question at the highest classification level, even if the holder believes the information to be over classified. The unit security manager or challenger must provide a recommendation on the disposition to the OCA or OPR if derivative or compilation classification.

### 2.3. Open Publication:

2.3.1. Anyone discovering classified information appearing in open publication, public domain, or otherwise unprotected format, will immediately notify the OCA, through the ISM, by the most expeditious method. The material will be protected commensurate to its highest classification level.

2.3.2. Notify the creator of a publication if the information appears in an Air Force publication.

2.3.3. Information revealing that classified information is in an unprotected format will be classified at the same level as the protected material.

2.3.4. Place notices and applicable markings on the unprotected document and any correspondence concerning the unprotected information until disposition and instructions are received.

### 2.4. Exercise Classified Information:

2.4.1. Place the following statement at the beginning on an exercise message "SECRET (or appropriate level of classified) UNCLASSIFIED – MARKED CLASSIFIED FOR TRAINING ONLY". Immediately below this include "Handling Instructions: (Unit) and its tenant units handle this message as (insert classification), all other addresses treat as unclassified." This line may be modified to meet user needs.

2.4.2. When portion markings are needed, for confidential use C-TNG, for Secret use S-TNG.

2.4.3. Declassify on the last day of the inspection, or the termination date of the training period and destroy when no longer needed or in use.

## 3. Declassifying, Downgrading or Upgrading Information.

### 3.1. Declassification:

3.1.1. Units will ensure that all declassification instructions listed on the front of classified information are followed.

3.1.2. Any person who feels that information should not be declassified as directed in the declassification instructions may challenge those instructions IAW Chapter 2 of this instruction.

### 3.2. Downgrading or Upgrading Classification:

3.2.1. When instructions are received concerning a change in classification, all referenced material will be remarked as follows:

3.2.2. Previous markings will be blacked out completely with permanent black ink and the new markings will be placed in all areas, to include portion markings.

3.2.3. The person making the change will place his/her initials on the cover of the document, with the date of the change, and a reference for authority. **NOTE:** If the instructions affect an excessive

number of documents it is permissible to post the notice on the safe and remark the material through its use. The instructions in paragraphs 3.1.1. through 3.1.2. apply.

3.2.4. When the document itself is the source for the change, per instructions included on the cover of the document, the person making the change will affix his/her initials and date only.

#### **4. Marking.**

##### 4.1. Remarking:

4.1.1. Instructions for changing classification markings are contained in Chapter 3 of this instruction.

4.1.2. Consult AFI 33-211, *Communications Security (COMSEC) User Requirements*, or contact the base COMSEC Manager for guidance on marking Communications Security (COMSEC) media.

4.1.3. Consult AFI 16-701, *Special Access Programs*, for guidance on marking Special Access Program material.

##### 4.2. Working Papers:

4.2.1. Working papers are classified documents and materials, drafts, notes, and other items created in the development and preparation of a finished document.

4.2.2. Working papers will display the overall classification, date of origination, originator's name, rank, and office symbol when they are initiated.

4.2.3. Working papers will reflect all markings prescribed in DOD 5200.1-R, Chapter 4, and DOD 5200.1PH and have the appropriate cover sheets placed on the front and back.

4.2.4. Working papers will be safeguarded commensurate with their assigned classification. Accountability and control will be established according to the overall classification level.

4.2.5. Working papers containing classified information will be handled the same as a finished document, to include all required markings i.e., classified by, declassify by, and appropriate portion markings, if they are released outside the originating office or are retained more than 180 days for the date of origin.

4.2.6. Destroy working papers when no longer needed.

##### 4.3. McConnell AFB Publications:

4.3.1. All publications, checklists, OPlans, base instructions, etc., that are derivatively classified will contain all markings specified in DOD 5200.1-R, Chapter 4.

4.3.2. When checklists or slides are developed and derivatively classified they will be sequentially numbered (i.e., 1 of 10, 2 of 10, etc.), as will each set (Set 1 of 20, Set 2 of 20, etc.). Maintain a list of sources and a record of distribution with the original file copy.

4.3.3. Maintain a list of sources and record of distribution with the original file copy when Oplans and base instructions are developed. This paragraph also applies when changes to publications are issued.

#### **5. Safekeeping and Storage.**

### 5.1. Designated Secure Areas:

5.1.1. Units will provide a written request for establishment of a secure area to the ISM.

5.1.2. The ISM, a civil engineer representative and a base COMSEC representative, Emission Security (EMSEC), Computer Security (COMPUSEC) (as needed) shall survey areas upon receipt of the unit's request. The survey will determine whether the area provides adequate security for classified information.

5.1.3. The ISPM is the approval authority for all designated secure areas; i.e., open and/or unattended secure areas, vaults, and secure conference rooms.

5.1.4. Unit security managers will maintain all documentation reflecting the survey(s) and approval of secure rooms. They will maintain a list of security containers (safes, vaults, storage areas, etc.) to include the container number, location, and custodian information. Forward a copy of this letter to the ISM (SFAI). The unit will develop operating instructions covering use of the area and end-of-day checks.

5.1.5. A facility loses certification anytime construction or modification of the facility i.e., new doors, repair of the ceiling or walls, etc. is started. Notify the ISM immediately to begin the recertification process.

### 5.2. Overnight Repository:

5.2.1. There is no accredited Sensitive Compartmented Information Facility (SCIF) on McConnell AFB. If SCI material is brought to McConnell, advise the courier there is no accredited SCIF or transient storage area to store SCI materials.

5.2.2. The command post (22 ARW/CP) will provide transient storage for up to and including "Top Secret" material during normal duty hours, after duty hours, or on weekends/holidays.

5.2.3. This transient facility will not be used unless the visited activity does not have the capability to safeguard the material.

5.2.4. The transient facility will develop procedures for documenting the transferring of custody. The AF Form 12, **Accountable Container Receipt**, is suitable for this purpose. The form shall reflect an inventory of the material and signatures of all parties involved in handling and storage of the information.

5.2.5. Each repository will develop an OI and ensure personnel understand how to secure transient material. Personnel accepting material will document the courier's name, rank, agency to be visited, location of his/her stay, and a phone number. In addition, the receiving person will verify the courier's authority to transport the material.

5.2.6. Installation entry controllers, visitor center technicians, airfield management personnel, and billeting personnel will know the locations of all repositories. The commanders of these agencies will ensure appropriate notices are posted for the benefit of visiting couriers.

### 5.3. Emergency Protection/Removal:

5.3.1. Emergency protection/removal plans will be developed and posted on all security containers, vaults, and open/unattended storage areas. These plans will include information on how to protect and where to store the material for the duration of the emergency. Utilize [Attachment 2](#) as the guide.

5.3.1.1. The plan will be tailored to limit the loss of life. Protection of the material is paramount, but not at the expense of human life.

5.3.1.2. Plans will address natural disasters and civil disturbances.

5.3.2. The Standard Form 702, **Security Container Check Sheet**, will be posted on each container, vault, or open/unattended secure area, and annotated each time the container is opened. On days when the container, vault, or open/unattended secure area is not used, "NOT OPENED" will be placed on the form at the end of the day.

5.3.2.1. If a container has more than one lock, a separate SF 702 is required for each lock.

5.3.2.2. Annotate the SF 702 every day of the week or days when personnel are in the office to reflect the container, vault, or open/unattended secure area was checked prior to leaving the office or facility.

#### 5.4. Secure Conferences or Meetings:

5.4.1. Areas designated as secure conference rooms will be surveyed and approved per paragraph **5.1.** of this instruction.

5.4.2. Each agency hosting a classified conference or meeting will ensure all attendees have the commensurate security eligibility and have signed a Standard Form 312, **Nondisclosure Agreement** (NdA). If a certified secure conference room is unavailable, the hosting unit will ensure sufficient personnel are posted at all entrances and exits outside of the room. Security forces personnel will not be used for this function. Personnel posted will ensure the exterior of the facility or hallways surrounding the room are kept clear for the duration of the meeting.

5.4.3. Hosting agencies will obtain the information in para **5.4.2.** on attendees from the attendee's assigned unit. This information will be in written form and provided to the host prior to the meeting. Attendees may handcarry verification of eligibility and a NdA only when there is less than 24 hours advance notification of the meeting. The personnel security section will not be called upon to furnish this information unless the attendee is not listed on the unit CAVS roster or other means have failed.

5.4.3.1. Group executive officers (or their designee) will check the CAVS roster for those personnel scheduled to attend wing standup.

5.4.3.2. Personnel tasked with identifying meeting attendees will place themselves outside the entrance to the meeting and identify (through use of a DD Form 2 or personnel recognition) each of the attendees.

5.4.3.3. Personnel coordinating secure meetings/briefings must determine the level of security clearance required and ensure all attendees have appropriate security clearances.

5.5. Protection of Classified Aboard Aircraft: Aircraft commanders (owners/users) are responsible for the protection of classified material aboard their aircraft whether on a DOD facility, at a civilian airfield, or when stopping in foreign countries in accordance with DOD 5200.1R, paragraph 6-300. Aircraft commanders should consult with the local ISPM or the senior security forces representative for assistance in complying with these requirements.

5.5.1. General Requirements (Normal Day-to-Day Operations): The following minimum standards are established to provide cost effective security of classified material and detect unauthorized access.

5.5.1.1. Park USAF aircraft in established restricted areas or equivalent and lock the aircraft, if possible, to provide security-in-depth for classified components and material onboard the aircraft. Host nation restricted areas in non-U.S controlled locations may be used only if material and components aboard the aircraft have been approved for release to the host nation by a cognizant foreign disclosure authority.

5.5.1.2. If the above requirements cannot be met:

5.5.1.2.1. Place classified material (e.g. classified mission folder) in a storage container secured with a GSA approved lock. Lock all aircraft egress points or secure them from the inside. Seal the aircraft with tamper proof seals such as numerically accountable metal or plastic seals. The storage container is a seamless metal (or similar construction) box or one with welded seams and a lockable hinged top secured to the aircraft. Hinges must be either internally mounted or welded. Containers installed for storage of weapons may also be used to store classified information even if weapons/ammunition are present, provided the criteria listed above have been met.

5.5.1.2.2. If the aircraft can be locked and sealed but there is no storage container, remove classified material (e.g. classified mission folder) and store it in an approved security container in an authorized U.S. facility.

5.5.1.2.3. If the aircraft cannot be locked and sealed and no storage container is available, offload all classified material and components to an approved security container in an authorized U.S. facility.

5.5.1.2.4. U.S. cleared personnel must provide continuous surveillance if none of the above criteria can be met.

5.5.1.2.5. Initiate a security investigation IAW AFI 31-401, Chapter 9 if evidence exists of unauthorized entry.

5.5.2. Generations: Classified material may be stored on alert aircraft during generations only under the following conditions:

5.5.2.1. The material remains in the original packaging with a GSA approved lock and a seal affixed to the opening apparatus.

5.5.2.2. The restricted area is established and security forces personnel are posted within the area. Security forces personnel will not be posted on individual aircraft; however, they will control entry, provide mobile patrols, and perform close boundary duties.

5.5.2.3. Each unit will provide the Security Forces Control Center (SFCC) with an AMC Form 41, Flight Authorization, as required by 22 ARW OPlan 31-209, Annex M, per each aircraft.

5.5.2.4. The command post will notify SFCC when an aircraft has classified on board and considered on alert.

5.5.2.5. When the area is disestablished and security forces personnel are relieved, a member

of the aircrew must stay with the aircraft until the classified is removed.

5.5.3. When an aircraft possesses “Top Secret” material or equipment, the aircraft will be considered a force protection level II asset and protected in accordance with AFI 31-101, as supplemented, and all applicable local directives. Use the posting considerations prescribed in paragraph [5.5.2.](#), with the exception that security forces will control entry into the affected aircraft exclusion area. Entry Authority Lists (EALs) or crew orders will be used by the entry controller.

5.5.4. When an aircraft possesses “Secret” or “Confidential” material or equipment, comply with paragraph [5.5.1.](#) and protection will be as follows:

5.5.4.1. Take no further action if the owner/user of a transient aircraft stay with it. If they don't stay with the aircraft they must contact SFCC to ensure the aircraft receives periodic checks.

5.5.4.2. For aircraft assigned to McConnell AFB, during normal operating periods the responsible unit will ensure the aircraft receives continuous coverage, to include avenues of approach. At other times, the responsible unit will arrange duty schedules to provide the necessary continuous coverage. The unit owning the aircraft is ultimately responsible for the security of the classified. SFCC will be notified of the presence of classified material or equipment. This notification will include the level of classification, type (installed equipment, briefcase, folder, etc.), and location within the aircraft. When unit personnel cannot provide the continuous coverage, security patrols will conduct checks periodically.

5.5.4.3. All aircraft containing classified equipment or material will be parked within an established restricted area, when possible. If this is not possible, a temporary restricted area will be established around the aircraft as a last resort. Procedures prescribed above still apply.

#### 5.6. Inspection Procedures and Identification:

5.6.1. There are no special provisions for handcarrying classified material from one building to another on McConnell AFB because inspection points for unauthorized removal of classified material are the installation entry/exit gates.

5.6.2. Personnel authorized to handcarry classified material off the installation will be identified in writing by their unit commander. The unit security manager will maintain this authorization. The individual must sign and maintain a DD Form 2501, **Courier Authorization**. The unit security manager will keep photocopies of this completed form with the designation letter. **NOTE:** The 22 SFS/SFAI section maintains blank forms. However, if DD Fm 2501 is unavailable, use a memorandum letter as shown in [Attachment 3](#). Use [Attachment 4](#) as the outer coversheet for the document.

#### 5.7. Central Destruction Facility (CDF):

5.7.1. 22 CS/IM is the office of primary responsibility regarding the operation of the CDF.

5.7.2. Central destruction capability is subject to change. IM will keep custodians informed of any change in CDF status.

5.7.3. IM will establish procedures in the form of an operating instruction for the CDF to include training, maintenance, and routine usage.

5.7.4. IM shall conduct monthly inspections of the CDF to ensure proper operation and safety of the facility.

5.7.5. Notify the Installation Security Program Manager (22 SFS/CC) if the CDF is to experience significant downtime due to impact on the Information Security Program.

5.7.6. Unit custodians shall incorporate a system to ensure retention of mission essential classified materials only. Custodians will routinely examine holdings for extraneous classified material and destroy them as soon as possible using the CDF or other unit destruction means.

5.8. Unit Owned/Operated Equipment:

5.8.1. Unit security managers will ensure the equipment meets the specifications listed in Table of Allowances (TA) 006, Organizational and Administrative Equipment. In addition, unit security managers will post the appropriate visual aid on or near the equipment. Use a locally generated visual aid, Not Authorized for Destruction of Classified, or Authorized for Destruction of Classified.

5.8.2. The operation of the equipment will be included in the OI. These procedures will include the number of personnel that are needed to destroy the material, how destruction records will be kept, and who is responsible for securing maintenance and materials for the equipment.

5.9. Destruction Records:

5.9.1. Use the AF Form 310, AF Form 1565, or AF Form 145, **Certificate of Destruction**, to record the disposition of classified material. Although "Secret" and "Confidential" do not require records if two personnel are involved in the entire destruction process, it is advisable to use the existing receipt form to record the disposition and file it in an in-active file for two years.

5.9.2. Destruction records for "Top Secret" materials will be completed and maintained IAW DOD 5200.1-R, Chapter IX, and AFI 31-401, Chapter 9.

5.9.3. Classified waste will be destroyed as prescribed in DOD 5200.1-R, Chapter IX. The first week of June will be the annual classified clean-out week.

## 6. Transmitting Classified Information.

6.1. Handcarrying Classified:

6.1.1. IAW AFI 31-401, the unit commander, orders approving official, unit security manager or supervisor have the authority to approve the escort and/or handcarrying of classified material aboard commercial passenger aircraft, outside the United States, its territories, and Canada.

6.1.2. The unit commander is the exclusive authorizing official and will sign the courier designation letter and all exemption notices. This authority will not be delegated.

6.1.3. Refer to AFI 31-401, paragraph 6.7., for authorizations and procedures regarding handcarrying/escorting classified materials aboard commercial passenger aircraft, within the United States, its territories, and Canada.

6.1.4. Refer to paragraph 5.6., of this instruction, for escorting and/or handcarrying materials on-base.

6.1.5. Instructions found in DOD 5200.1-R, Chapter 7, will be used to package classified material for any mode of transmission.

## 7. Special Access Programs (SAPs).

7.1. There are no specific issues at McConnell AFB. All instructions pertaining to SAPs can be found in:

7.1.1. DOD 5200.1-R, Chapter XII.

7.1.2. AFI 31-401, Chapter 12 and AMC Sup 1, paragraph 12.2. through 12.4.

7.1.3. AFPD 16-7 and other specific program directives.

7.2. Units that require SAP access and routinely receipt for SAP material will ensure compliance with DOD 5200.1R and AMCI 16-701. In addition, units will notify the ISM via memorandum of the existence of SAP materials within the organization.

7.3. There are no McConnell supplements regarding the safekeeping, storage, reproduction, transmission, access, and dissemination of SAP materials for McConnell AFB.

## **8. Security Education and Training.**

### **8.1. Initial Training.**

8.1.1. Unit security managers will be included on the unit in-processing checklist as a mandatory stop. They should use the unit OI to brief newly arrived personnel on all security programs and issues within the unit. Verify a person's security eligibility, investigation, and NDA status during initial training.

8.1.2. Address physical security issues found in AFI 31-101, MAFBI 31-101, and the Installation Security Plan for personnel requiring a restricted area badge or who will work under escort within a restricted area.

8.1.3. Ancillary security disciplines will be included in initial unit training. This training will include the basic principles and application of Operations Security (OPSEC), Computer Security (COMPUSEC), Security Awareness Training and Education (SATE), Communications Security (COMSEC).

### **8.2. Recurring Training:**

8.2.1. Units will develop an annual training plan. The plan will address items listed in AFI 31-401 Attachment 7 (see IC 2000-1 to AFI 31-401) and DOD 5200.1-R, paragraph 10-101, for all personnel. In addition, physical security issues will be covered. Escorting and basic restricted area procedures should be covered in depth. The following are examples of areas to be covered. This list is not all-inclusive but used as an example. Each unit should tailor its training needs to their unit mission.

8.2.1.1. Policy and Program Management

8.2.1.2. Original Classification

8.2.1.3. Derivative Classification

8.2.1.4. Declassification/Change of Classification

8.2.1.5. Foreign Government Information

8.2.1.6. Marking

8.2.1.7. Safeguarding

8.2.1.8. Transmission and Transportation

8.2.1.9. Special Access Programs

8.2.1.10. Actual/Potential Compromise of Classified Information

8.2.2. The method of presentation, topics, and when they will be addressed included in the unit OI.

8.2.3. Recurring training covering OPSEC, COMSEC, COMPUSEC, SATE, and SECURITY NOW is available from the respective installation program manager. The ISM maintains a list of these managers and will coordinate training sessions upon request.

8.3. Unit Security Manager Indoctrination/Formal Education:

8.3.1. The ISM will conduct a formal education class every 90 days. The training will include basic instruction on OPSEC, COMSEC, COMPUSEC, SATE, Physical Security (Security NOW), and detailed instruction on Personnel, Information, and Industrial Security.

8.3.2. The ISM will provide indoctrination training, at the earliest convenience, for newly appointed unit security managers.

## 9. Compromise of Classified Information.

9.1. Appointing Authorities:

9.1.1. The commander of the responsible unit will appoint the inquiry official as prescribed by AFI 31-401. Utilize [Attachment 5](#) as an example.

9.1.2. The group commander will appoint the inquiry official in cases involving two or more units from within the same group,

9.1.3. The wing commander will appoint or determine which group commander appoints the inquiry official when two or more units from different groups are involved.

9.1.4. Inquiry officials should be an impartial competent individual in a grade equal to, or higher than, the person involved in the incident. The inquiry may not be assigned to the same flight or section as any of the people involved in the incident. The inquiry official cannot be in the chain of command for any of the persons involved in the incident. The inquiry official must be one (or more) of the following:

9.1.4.1. Any commissioned officer.

9.1.4.2. Any senior noncommissioned officer (E-7, E-8, or E-9).

9.1.4.3. Any DOD civilian (GS-9 and above).

9.2. Incident Processing:

9.2.1. When receiving material that has been transmitted incorrectly, the receiving unit will notify the ISM and the sending unit immediately. The receiving unit shall take statements from personnel receiving or handling the material. Gather all statements and forward them to the sending unit for their inquiry. Reminder emails/letters will be forwarded to the inquiry official and unit security manager at the 10-day and 20-day mark to comply with AFI 31-401, paragraph 9.6.2.

9.2.2. When the inquiry official has completed the report, he/she will have the ISM perform a technical review. The ISM will provide the ISPM with a written technical review. Once this letter is signed, the ISM will forward the entire inquiry and technical review to 22 ARW/SJA for a legal review. Upon receipt of the SJA technical review, the unit security manager will provide the entire package to the appointing authority. The appointing authority will close the inquiry and take the appropriate action recommended, or initiate a formal investigation.

9.2.3. All original documentation will be provided to the ISM. The ISM will provide a complete copy to affected unit security manager for filing. Inquiries will be filed:

9.2.3.1. Two years for incidents involving classified other than NATO.

9.2.3.2. Four years for incidents involving NATO information.

## 10. Access, Dissemination, and Accountability

### 10.1. Visit Requests:

10.1.1. Visitors will not handcarry the request. Requests shall be received, prior to the visitor's arrival, by mail, fax, electronic mail, etc., and shall include at a minimum:

10.1.1.1. Full name, date and place of birth, social security account number, and rank or grade.

10.1.1.2. Clearance eligibility and investigation date.

10.1.1.3. Employer's name, address, and phone number.

10.1.1.4. Purpose, date, and duration of visit.

10.1.1.5. Activity and specific person being visited.

10.1.2. The ISM will be contacted immediately upon receipt of a visit request. The ISM will authenticate the visit request prior to the visit, no exceptions. Activities will not approve a visit request without the authentication from the ISM.

10.2. Nondisclosure Agreement Address: After completion, unit security managers will update this information in the Sentinel Key Computer program and forward the original signed Standard Form 312, **Nondisclosure Agreement (NdA)**, for all active duty, reserve, guard, and civilian personnel to:

HQ AFMPC/DPMDOM3  
550 C STREET WEST SUITE 21  
RANDOLPH AFB, TX 78150-4723

10.2.1. Unit security managers who do not have access to Sentinel Key will forward the original document to 22 SFS/SFAP.

### 10.3. Reproduction:

10.3.1. Unit commanders or unit security managers will designate personnel, in writing, that are authorized to approve the reproduction of classified material. Unit security managers shall:

10.3.1.1. Train personnel on the limitations and procedures.

10.3.1.2. Ensure the appropriate visual aids are posted.

10.3.1.3. Ensure the equipment is approved by 22 SFS/SFAI, 22 CS and the approval is posted.

10.3.1.4. Ensure the equipment is positioned to allow constant surveillance.

10.3.2. "Top Secret" will only be reproduced when consent is granted from the originator. Copies will be numbered and accountability will be established on the authorization and distribution of local copies.

10.3.3. Procedures for classified reproduction will be included in the unit OI. Each person reproducing classified will, after reproducing classified materials, run at least two blank sheets through the equipment to clear any latent images. These blank sheets will be destroyed as classified waste.

10.3.4. Locally generated visual aids, Classified Reproduction Authorized, or STOP, Do Not Use..., will be posted on or near all reproduction equipment.

#### 10.4. Inventory/Accountability.

##### 10.4.1. Top Secret:

10.4.1.1. Unit commanders controlling or possessing "Top Secret" materials will appoint a Top Secret Control Officer (TSCO), with sufficient alternates, in writing. Forward a copy of this memorandum to the ISM.

10.4.1.2. Conduct inventories IAW AFI 31-401, paragraph 7.8.4.

10.4.1.3. Select inventory officials based on their reliability, maturity, and trustworthiness. Inventory officials shall possess a "Top Secret" eligibility and may be assigned as a TSCO or alternate.

##### 10.4.2. Secret and/or Confidential:

10.4.2.1. Annual inventories are not required.

10.4.2.2. Each unit possessing or controlling "Secret" or "Confidential" materials will develop a positive accountability and control system. This system will be outlined within the OI; include procedures on receiving and accounting for, to include transmitting and destruction.

10.4.2.3. The AF Form 310, **Document Receipt and Destruction Certificate**, or AF Form 1565, **Entry, Receipt, and Destruction Certificate**, may be used for accountability. When the AF Form 310 is used, establish a file as follows:

10.4.2.3.1. An active accountability section.

10.4.2.3.2. An on-loan suspense section.

10.4.2.3.3. An in-active/destruction record.

## 11. Foreign Government Information – North Atlantic Treaty Organization (NATO) Information:

11.1. The 22d Air Refueling Wing Director of Staff (22 ARW/DS) is the NATO control point for McConnell AFB. 22 ARW/DS is responsible for authoring operating instructions in accordance with DOD 5100.55 and AMCI 31-401. Administrative requirements will be coordinated through 22 SFS/SFAI to HQ AMC/SFOI when personnel changes occur. In addition, SFAI will perform a review of the control point during the 22 MSS program review and process the results accordingly.

11.2. Units that require NATO access and routinely receipt for NATO material will ensure compliance with DOD 5100.55 and AMCI 31-401. Units will notify SFAI via memorandum of the existence of NATO materials within the organization.

11.3. Refer to AFI 31-406 regarding the safekeeping, storage, reproduction, transmission, access, and dissemination of NATO materials for McConnell AFB. Also refer to DOD 5200.1-R, Chapter 5, DODD 5100.55, or AMCI 31-401, for instructions regarding NATO and other foreign government information.

**12. Administrative Sanctions.** Administrative sanctions will be processed according to instructions in DOD 5200.1-R and AFI 31-401. There are no additional procedures within this instruction.

**13. Unclassified Controlled Nuclear Information (UCNI).**

13.1. DODD 5210.83 contains guidance on policy, assigns responsibilities, and prescribes procedures for identifying, controlling, and limiting the dissemination of unclassified information pertaining to the physical protection of special nuclear material, equipment, and facilities.

13.2. The wing commander and ISPM are authorized to identify and deny release of UCNI.

13.3. The ISPM and wing commander will review all requests for release of UCNI material. Information leading to and the final decision will be reported through HQ AMC/SF to HQ USAF/SFI.

13.4. The wing commander or ISPM review and approve/disapprove special access requests to this material.

**14. Industrial Security Program.**

14.1. The Industrial Security Program will be administered using the following guidelines:

14.1.1. *DOD 5220.22-R, Industrial Security Regulation.*

14.1.2. *DOD 5220.22-M, National Industrial Security Program Operating Manual.*

14.1.3. *AFPD 31-6, Industrial Security.*

14.1.4. *AFI 31-601, Industrial Security Program Management.*

14.1.5. *AFH 31-602, Industrial Security Program*

14.1.6. All applicable AMC supplements to the aforementioned publications.

14.2. 22 SFS has oversight responsibilities for all aspects of the Industrial Security Program at McConnell AFB. This includes, but is not limited to, annual program reviews, secure room certification, and visit requests approval.

14.3. The ISM will initiate a Visitor Group Support Agreement between the contractor and the U.S. Government upon receipt of DD Form 254, **Department of Defense Contract Security Classification Specification**, specifically listing the responsibilities of the contractor, the unit, and 22 SFS for the receipt, access, storage, reproduction, accountability and destruction of classified, administrative and oversight responsibilities.

14.4. Unit Responsibilities: Unit security managers are responsible for ensuring that the ISM is notified anytime they receive or issue a DD Form 254, or a contractor requires access to classified information.

14.4.1. Unit security managers with industrial security contracts listed on a DD Form 254 shall provide the contractor with adequate storage containers and associated forms if the contractor is authorized to maintain classified material.

14.4.2. Unit security managers will perform the same functions for the contractor as they do for the military and Department of the Air Force civilian personnel assigned to their unit.

14.4.3. Unit security managers will review and abide by the Long Term Visitor Group Security Agreement.

RONALD R. LADNIER, Colonel, USAF  
Commander, 22d Air Refueling Wing

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

DODD 5100.55, *United States Security Authority for North Atlantic Treaty Organization Affairs*

DOD 5200.1-R, *Information Security Program*

DOD 5200.1-PH, *DOD Guide to Marking Classified Documents*

DOD 5200.1-PH-1, *Classified Information Nondisclosure Agreement (Standard Form 312)*

DODD 5210.2, *Access to and Dissemination of Restricted Data*

DODD 5210.83, *Unclassified Controlled Nuclear Information (UCNI)*

DOD 5220.22-M, *National Industrial Security Manual (NISPOM)*

DOD 5220.22-R, *Industrial Security Regulation*

AFI 14-302, *Control, Protection and Dissemination of Sensitive Compartmented Information*

AFMAN 14-304, *The Security, Use and Dissemination of Sensitive Compartmented Information*

AFPD 16-2, *Disclosure of Military Information to Foreign Governments and International Organizations*

AFI 16-201, *Foreign Disclosure of Classified and Unclassified Military Information to Foreign Governments and International Organizations*

AFPD 16-7, *Special Access Programs*

AFI 16-701, *Special Access Programs*

AFI 31-101, Volume 1, *Air Force Physical Security Program*

AFPD 31-4, *Information Security*

AFI 31-401, *Information Security Program Management*

***Abbreviations and Acronyms***

**AFI**—Air Force Instruction

**AFMAN**—Air Force Manual

**AFOSI**—Air Force Office of Special Investigations

**AFPD**—Air Force Policy Directive

**ASCAS**—Automated Security Clearance Approval System

**CAVS**—Central Adjudication Verification System

**CNWDI**—Critical Nuclear Weapons Design Information

**CSF**—Chief, Security Forces

**DOD**—Department of Defense

**DODD**—Department of Defense Directive  
**DODI**—Department of Defense Instruction  
**EO**—Executive Order  
**FOUO**—For Official Use Only  
**FRD**—Formerly Restricted Data  
**GSA**—General Services Administration  
**IDS**—Intrusion Detection System  
**IO**—Inquiry Official  
**ISM**—Information Security Manager  
**ISPM**—Information Security Program Manager  
**MDR**—Mandatory Declassification review  
**NAC**—National Agency Check  
**NATO**—North Atlantic Treaty Organization  
**NdA**—Nondisclosure Agreement  
**OCA**—Original Classification Authority  
**RD**—Restricted Data  
**SAP**—Special Access Program  
**SATE**—Security Awareness, Training and Education  
**SCI**—Sensitive Compartmented Information  
**SCG**—Security Classification Guide  
**SIF**—Special Information File  
**TSCA**—Top Secret Control Account  
**TSCO**—Top Secret Control Officer  
**UCNI**—Unclassified Controlled Nuclear Information

**Attachment 2****EMERGENCY PROTECTION/REMOVAL PLANS**

Date

MEMORANDUM FOR 22 SFS

FROM: 22 SFS/SFAI (Unit Security Manager)

SUBJECT: Emergency Protection/Removal

1. Emergency Protection/Removal of Classified Material: When directed/required by the situation, personnel entrusted to safeguard and protect classified material will:

1.1. Protect classified material at all times. When removal of the material is necessary to provide a higher degree of protection, the last individual to account for the material removes the material and transports/transfers it to the classified account custodian for immediate storage in container CSF#2. The applicable classified accountability form(s) for the information is also given to the custodian.

1.1.1. Classified material removed from SFCC must be secured and hand carried to storage container CSF#2 and maintained there until termination of the situation or when directed by higher authority to return the classified material to SFCC. Document the transfer in the Security Forces blotter.

1.1.2. Handcarry the material and accountability form(s) back to the original location upon receipt of termination from competent authority. Upon return, the controller accounts for all classified material using the accountability form(s) and completes an entry in the Security Forces blotter.

1.2. On-duty personnel will fulfill guard requirements when emergency protection is implemented during duty hours within the designated area where classified material is located and until the order is given to remove classified material to the Operations Branch (SFO). Personnel do not have to be armed, but must have the appropriate clearance to perform guard duties. Notify, and recall if necessary, the classified account custodian and unit security manager during non-duty hours. SFO personnel will prepare for emergency protection of classified material and determine if/when documents are to be transferred to an area for security reasons.

1.2.1. In the event of a fire, bomb threat, or natural disaster, classified material may be secured in an authorized container or removed as the situation dictates. An authorized/cleared individual may be placed outside the affected area and briefed he/she must prevent unauthorized removal of classified material in the event the building is destroyed. This is an acceptable means of protecting classified material and reduces the risk of casualty.

1.2.2. Any discrepancies noted during emergency removal/storage of classified material is recorded and the individual removing or storing the classified must brief the classified account custodian and unit security manager.

1.3. SFO must prepare a suitable container(s), as specified by DOD 5200.1-R, chapter 6-400, for holding classified material when classified has been gathered and directions have been received to transfer all classified to a central storage/protection area.

JOHN Q. PUBLIC, MSgt, USAF

Chief, Information Protection Branch

**Attachment 3****(APPROPRIATE LETTERHEAD)**

Date

MEMORANDUM FOR WHOM IT MAY CONCERN

FROM: (UNIT/CC)

SUBJECT: Designation of Official Courier

1. Master Sergeant Joe Q. Public, FR123-45-6789, 22d Security Forces Squadron, Administration and Reports Flight, McConnell AFB, Kansas 67221-3716, is designated an official courier for the United States Government. Upon request, he will present his official identification card bearing his name, rank, social security number, and date of birth.
2. Sergeant Public is handcarrying/escorting four sealed packages, each package measures 9" x 8" x 24" and addressed from "22d Security Forces Squadron/CCQ, 53403 Kansas Suite 147, McConnell AFB, Kansas 67221-3716," and addressed to "HQ AMC/SPI, 102 E. Martin Street Room 110, Scott AFB, IL 62225-5318." Each package is identified on the outside of the package by the marking "OFFICIAL BUSINESS - MATERIAL EXEMPT FROM EXAMINATION" bearing the signature of the undersigned.
3. Sergeant Public is departing Wichita International Airport with a final destination of Lambert Field, Saint Louis Missouri. There are no transfer points or authorized delays enroute, unless there is a state of emergency.
4. This courier designation can be confirmed by contacting the undersigned at 22d Security Forces Squadron, Area Code 316, 759-xxxx, or Defense Switching Network 743-xxxx. This letter expires 30 Oct xx.

JOHN L. DOE, Lt. Col, USAF  
Commander, 22d Security Forces Squadron

**Attachment 4  
COVER SHEET**

**DEPARTMENT OF THE AIR FORCE**

**22d SECURITY FORCES SQUADRON (AMC)**

**MCCONNELL AFB KANSAS 67221-3716**

---

**OFFICIAL BUSINESS**

---

**MATERIAL EXEMPT FROM EXAMINATION**

**JOHN L. DOE, Lt. Col, USAF  
Commander, 22d Security Forces Squadron**

## Attachment 5

## INQUIRY OFFICIAL APPOINTMENT LETTER

Date

MEMORANDUM FOR 22 SFS/SFAI

FROM: 22 SFS/CC

SUBJECT: Appointment of Inquiry Official

1. Under the provisions of AFI 31-401, paragraph 6.3.1, MSgt James L. Potter 22 SFS/SFTT is appointed to conduct a preliminary inquiry into security incident MCC 00-00.
2. The purpose of this inquiry is to determine whether a compromise occurred and to categorize this security incident. The categories are: compromise, possible compromise or security deviation. MSgt Potter is authorized to interview those persons necessary to complete his findings. He is also authorized to access all records and files, to include those classified up to and including Top Secret, which are pertinent to this inquiry.
3. MSgt Potter must contact the 22 ARW Information Security Manager (22 SFS/SFAI) for a briefing on his responsibilities. His written report will be forwarded to me within 10 days from receipt of this letter. As a minimum, the report must contain the following:
  - a. A statement that a compromise or possible compromise did or did not occur
  - b. Category of the security incident
  - c. Cause factors and responsible person(s)
  - d. Recommended corrective action
4. Notify 22 SFS/SFAI immediately if it is determined that a compromise has occurred.
5. If you have any questions, contact SSgt Greene at 4651 or SSgt Smith at 3954.

JOHN L. DOE, Lt Col, USAF  
Commander, 22d Security Forces Squadron