



Security

MANAGING THE INFORMATION AND PERSONNEL SECURITY PROGRAM

OPR: 920MSF/SF (TSgt Robert J. Cowart, Jr.)

Certified by: 920RQG/CC
(Col Bruce E. Davis)

Pages: 11

Distribution: F

This instruction implements *AFPD 31-4, Information Security, AFI 31-401/AFRC Supplement, Managing the Information Security Program, AFI 31-501, Personnel Security Management, DoD 5200.1-R, Information Security Program, and DoD 5200.1PH, DoD Guide to Marking Classified Documents*. It prescribes procedures and responsibilities of all 920 RQG personnel; specifically all staff agency chiefs, security managers (SM), and security monitors. The 45SFS/SFAI provides information security oversight and personnel security investigation (PSI) support to 920RQG and submits all PSIs to the Defense Security Service (DSS). Each commander, director, and staff agency chief is responsible for ensuring assigned personnel comply with AFPD 31-4, AFI 31-401/AFRC Supplement, DoD 5200.1-R, and this instruction.

1. Appointments and Responsibilities.

1.1. Commanders and Staff Agency Chiefs will:

1.1.1. As the responsible officer in charge of the Information Security Program, appoint in writing a Primary and Alternate Security Manager (SM), in the grade of GS-07 or E-6 or above to manage the Information and Personnel Security Programs. The primary or alternate SM will be full time personnel. Larger units/sections are encouraged to appoint security monitors at each section to assist the SM. Forward the original appointment letter to the 45SFS/SFAI and a copy to 920MSF/SF. Ensure SM receives training within 6 months of appointment. Training for SM is accomplished by 45SFS/SFAI.

1.1.2. Provide the SM with sufficient resources of time, staff, and funds to permit the accomplishment of their responsibilities.

1.1.3. Review self-inspections reports and provide a written endorsement of concurrence on corrective action to be taken.

1.1.4. Designate in writing, Safe and Classified Custodians and those who have access to safe combinations and personnel to perform end of day security checks utilizing **SF Form 701, Activity Security Checklist**.

1.1.5. Review security access requirements (SAR Codes) coded in the Unit Manpower Document (UMD), Automated Security Clearance Approval System (ASCAS) roster or by contacting 920MSF/SF to utilize SENTINEL KEY Clearance Access Verification System (CAVS) monthly to ensure clearance eligibility requirements are consistent with mission needs. Document this review and file in the SMs handbook. SAR codes should accurately reflect day-to-day access. Over inflating SAR codes may be construed as fraud, waste, and abuse.

1.1.6. Designate in writing, personnel authorized to receive classified material and forward the original letter to the 45CS/SCAAD and 45SW/CP. Designate in writing personnel authorized to open the inner wrappers of classified material and who can have access to NATO Secret material. Maintain file copies in the unit security manager's handbook.

1.1.7. Implement Security Education and Awareness Programs according to AFI 31-401, chapter 10, AFI 31-101, chapter 5, and AFH 31-103.

1.2. Security Manager (SM) will:

1.2.1. Provide oversight and management of the Information and Personnel Security Programs.

1.2.2. Maintain a Security Manager's handbook as outlined in the AFI 31-401.

1.2.3. Develop Internal Operating Instructions (OIs) and include them as part of the unit initial indoctrination and recurring training programs.

1.2.4. Brief individual(s) appointed to conduct semi-annual security self-inspections. Monitor the inspection and provide assistance to the inspector. 920MSF/SF will accomplish a report listing the discrepancies and recommended corrective actions to the commander. Ensure the commander reviews and endorses the report, and forward a copy of the report with identified corrective action to the 920MSF/SF. Maintain the last two self-inspections reports in the security manager's handbook. 920MSF/SF will conduct self-inspections on all 920RQG units. IAW AFI 31-401, chapter 1, para 1.4.3.1. SM will not conduct self-inspections.

1.2.5. Attend quarterly SM meetings sponsored by the 920MSF/SF and 45SFS/SFAI. Ensure the information is disseminated.

1.2.6. Manage the unit Personnel Security Program to include:

1.2.7. Manage the ASCAS roster for the unit to include identifying personnel who require personnel security investigations (PSI). SMs will acquire a new ASCAS roster before the 5th of each month. ASCAS can be obtained from PC-III or by contacting 920MSF/SF for ASCAS roster.

1.2.8. SM initiates tracer request through 45SFS/SFAP by either letterform or e-mail.

1.2.9. Notify personnel who have been identified for a periodic reinvestigation (PR) and assist them with completing PSI forms. Use the Electronic Personnel Security Questionnaire (EPSQ) to submit PSIs to the 45SFS/SFAP for processing. Contact 45SFS/SFAP to schedule an appointment when submitting PSIs. Ensure all PSI processing is completed within 30 days of initial notification. **NOTE:** Failure to submit required PSIs in a timely manner may jeopardize an individuals security clearance eligibility and result in establishment of a Special Information File (SIF).

1.2.10. Coordinate with respective supervisor, director, and/or commander for the establishment of SIF. Also provide initial notification and subsequent status report to 45SFS/SFAP through the 920MSF/SF concerning SIFs.

1.2.11. Manage the Security Education and Physical Security Awareness Programs for the unit according to AFI 31-401, chapter 10 and AFI 31-101, Chapter 5. Follow the annual training plan in Attachment 1. Document the training using sign-in sheets to document the training and maintain the sign-in sheets in the Security Managers Handbook.

1.2.12. Have access to required publications for administering the security program.

1.2.13. Establish and maintain an aggressive and recurring security-training program IAW AFI 31-401, para 9.4. The scope and depth of the security training should be geared toward the unit mission, needs, and the individual receiving the training. See attachment 1 for training requirements.

1.2.14. Ensure authorized personnel conduct Foreign Travel briefings.

1.2.15. Ensure computer security officers are assigned to the unit.

1.2.16. Coordinate restricted area badge **and AF Form 2586, Unescorted Entry Authorization Certificate**, issues with 45 SFS/SFA. For departing personnel, ensure each restricted area badge is turned in prior to departure.

1.2.17. Develop unit OIs and tailor them strictly to your unique security requirements.

1.2.18. Review all challenges to classifications and assist personnel in complying with classification markings and transmission procedures.

1.2.19. Ensure *AFVA 205-11, "Your Security Manager Is"*, is posted conspicuously throughout the unit to ensure assigned personnel are aware of SM appointments.

1.2.20. Conduct indoctrination and recurring training for assigned personnel.

2. Classification or declassification of classified material or information:

2.1. 45SW/CC has been designated as a Secret Original Classification Authority (OCA). The authority to originally classify information will be exercised sparingly and only when no promulgated classification guidance exists.

2.2. An action officer who develops information that is currently not classified under a security classification guide and believes the information warrants safeguarding, routes the information to the 45SFS/SFAI for classification evaluation. The action officer is responsible for advising 920MSF/SF of the OCA classification decision. The action officer will consult *DoD 5200.1PH*, prior to tentatively classifying the document.

2.3. The safe custodian will conduct quarterly reviews of classified material in their control to determine downgrading or declassification.

3. Classification challenges:

3.1. All personnel must challenge classification decisions, which they believe are improper. If information is received which is believed to be improperly classified, or an overly restricted period of continued classification has been assigned, the 920MSF/SF and security manager will be contacted.

3.2. The classified information being challenged will be safeguarded at the highest level of classification. If the information is SECRET and the challenge is for downgrading to CONFIDENTIAL, the information must still be safeguarded as SECRET until the challenge has been resolved.

3.3. The 920MSF/SF and security manager will ensure challenges are acted upon within thirty (30) days.

4. Marking Classified Information.

4.1. The originator of classified information is responsible for proper application of classification markings. This includes derivative classification decisions and working papers.

4.2. Those who prepare derivative classified documents are strongly encouraged to consult with their SM and review Executive Order 12958, chapter 4 in DoD 5200.1-R, AFI 31-401 and *DoD 5200.1PH*.

4.3. Marking Working Papers. Date and annotate all working papers with the OPR or action officer in ink, keep a record of all "DERIVED FROM" sources attached to the working paper, and properly mark the working paper with the highest overall classification and term "WORKING PAPERS" at the top and bottom of each page. Guidelines for working papers will be followed IAW DoD 5200.1R.

4.4. Refer complex marking issues to the SM for assistance.

5. Safekeeping and Storage.

5.1. Offices storing small numbers of classified documents that do not warrant an entire security container (GSA approved safe) may request courtesy storage from another office. In this case, a letter of agreement between the two offices is maintained in the safe with the documents. Additionally, the documents must be separated from the safe contents by placing them in a sealed envelope or container.

5.2. Safe Custodians. The first person listed on the **Standard Form 700, Security Container Information**, is considered the primary safe custodian. Safe custodian responsibilities are as follows:

5.2.1. Ensure safe combinations are changed at required intervals.

5.2.2. Combinations are changed when placed in use; whenever an individual knowing the combination no longer requires access; when the combination has been subject to compromise; or when taken out of service.

5.2.3. Report container malfunctions to 920MSF/SF who will contact appropriate personnel to correct the malfunction. Do not perform any maintenance on security containers.

5.2.4. Ensure all documents placed in the safe are properly marked. Refer to DoD 5200.1-PH for proper marking of classified information.

5.2.5. Ensure safe contents are identified in unit office file plans.

5.2.6. Ensure the security container is properly marked with an easily identifiable number permanently attached to the exterior so it can be identified after natural disasters. If your security container is not properly marked, contact 920MSF/SF.

5.3. The possibility of fire, civil disturbance, terrorist activity, natural disaster, or enemy action at Patrick AFB, FL requires development and possible implementation of special procedures for safeguarding and emergency removal of classified material to preclude the material from falling into unauthorized hands. A situation may develop that requires higher headquarters or a designated representative to direct implementation of this plan. The senior individual present in the office containing classified material may deviate from this plan when circumstances warrant.

5.3.1. Emergency Protection procedures of classified documents in the event of a fire or natural disaster:

5.3.1.1. If evacuation becomes necessary the senior member evacuates all personnel according to the evacuation plan. Secure all classified materials in its approved container and insure the container is secure. If time does not permit to secure the classified, leave the classified where it is if your life is in jeopardy and evacuate the building. When the emergency has been terminated and it

has been declared safe to re-enter the facility, inspect the safe for signs of forced entry or tampering and report discrepancies to 920MSF/SF and/or 45SFS/SFAI.

5.3.2. Emergency Protection procedures of classified documents in the event of a civil disturbance/implementation of THREATCONS:

5.3.2.1. When notified of a civil disturbance secure all classified in a security container.

5.3.2.2. During THREATCON implementation minimize usage of classified information.

5.4. Holding Classified Meetings:

5.4.1. Prior to scheduling classified meetings, contact 920MSF/SF to ensure all security precautions are completed.

5.4.2. Appoint a security OPR for the meeting.

5.4.3. Comply with all security guidelines IAW DoD 5200.1R, chapter 6, section 6-307 and AFI 31-401, chapter 5, section 5.15.

5.4.4. Ensure all personnel have the appropriate level of clearance eligibility prior to starting the meeting. ASCAS rosters, visit request letters, and TDY orders are acceptable for this purpose.

6. Destruction of classified material:

6.1. Destruction of classified material must be approved by the unit commander, security manager, or classified custodian. Classified material belonging to 920RQG can be destroyed by using the unit's approved shredding machine located in the 920OSF/IN or by taking the material to 45CS/SCBG for large volume shredding. 45CS/SCBG is also the alternate location for the destruction of classified material. Classified will be destroyed when it has served its purpose and is no longer needed.

6.2. Annual Cleanout Day. The annual cleanout day for 920RQG is the first Tuesday of September. Each commander/staff agency responsible for maintaining and storing classified will ensure the safe custodians review all classified documents for destruction. Provide a written response to 920MSF/SF in reference to how many pages of classified need to be destroyed.

6.3. All shredders utilized within 920RQG will be properly labeled. Shredders approved for destruction of classified will be marked with *920RQGV A 31-104, "This Shredder Is Authorized For The Destruction Of Classified Material"*. Shredders not approved for the destruction of classified will be marked with *920RQGV A 31-101, "ATTENTION, This Shredder Is Not Authorized for the Destruction Of Classified Material, ATTENTION"*.

7. Access, Dissemination, and Accountability:

7.1. No one will be allowed access to classified until the following requirements are met: verify security clearance eligibility, establish the need-to-know, and verify the individual requesting access has signed an SF 312. Contact the unit SM or 920MSF/SF to verify clearance eligibility and a SF 312 has been executed.

7.1.1. SMs are authorized to accept SF 312s on behalf of the United States. Any 920RQG employee may witness execution of the SF 312.

7.1.1.1. Once the SF 312 is complete, do a pen-and-ink change to your unit ASCAS roster under the NdA column by annotating a "1". Keep a copy of the SF 312 on file, send a copy of the SF 312 to 920MSF/SF, and mail the original to the appropriate location:

7.1.1.2 For military members, send SF 312 to HQ AFMPC/DPMDOMIA, 550 C Street, West, Suite 21, Randolph AFB TX, 78150-6001.

7.1.1.3. For reservist, send SF 312 to HQ ARPC/DSMM, 6760 E. Irvington PL #3000, Denver CO, 80280-3000.

7.1.1.4. For Air Force Civilians, send the SF 312 to 45MSS/DPCC.

7.1.1.5. For Air Reserve Technicians, send the original SF 312 to the address in paragraph 7.1.1.4. and an original to the address in paragraph 7.1.1.3. ART personnel will need to sign two NdAs.

7.1.2. The responsibility for access to classified information rests with the individual having custody of the classified information.

7.2. Reproduction Authority and Persons Designated to Copy Classified Information:

7.2.1. Each unit establishes procedures for the reproduction of classified materials. This will be included as one of the unit operating instructions.

7.2.1.1. Each commander appoints in writing, who within the unit is authorized to reproduce classified documents. Keep appointments to a minimum.

7.2.2. All copiers utilized within 920RQG will be properly labeled. Copiers approved for the reproduction of classified will be marked with 920RQGVA 31-103, *"This Copier Is Authorized For The Reproduction Of Classified Material"*. Copiers not approved for the reproduction of classified will be marked with 920RQGVA 31-102, *STOP This Copier Is Not Authorized For The Reproduction Of Classified Material"*.

8. Transmitting Classified Materials:

8.1. All classified distribution will be sent to 920MSF/SCB.

8.2. All first class, registered, certified, and FED EX mail will be handled as classified information until opened.

8.3. All outgoing classified distribution will be sent IAW DoD 5200.1R, chapter 7 and AFI 31-401, chapter 6.

8.4. Removal of Classified Documents from units within 920RQG (On Base):

8.4.1. Commanders or supervisors approve appropriately cleared personnel to remove classified information from the work area for the following purposes:

8.4.1.1. Routine destruction at the designated areas.

8.4.1.2. For official duties on Patrick AFB or for handcarrying classified documents to off-base areas under the control of the installation commander. Accomplish the following when handcarrying classified to off-base areas under the control of the installation commander: obtain supervisor's permission to remove/pick-up the classified material from the workplace, attach the appropriate cover sheet, and enclose the material in an outer container such as a sealed envelope, folder (closed with a lock, tie, or velcro), briefcase, zippered bag, etc. NOTE: Classified markings must not appear on the outer container. Individuals must possess written authorization, such as **DD Form 2501, Courier Authorization**, or courier authorization letter.

8.5. Removal of Classified Documents from units within 920RQG (Off Base): NOTE: Removing classified documents/equipment from designated work areas to work at home is strictly prohibited.

8.5.1. For transmission off the installation see DoD 5200.1R and AFI 31-401.

8.5.2. Personnel authorized to remove classified information must be briefed on their responsibilities for protection of classified by their SM. This briefing can be annotated on the **DD Form 2501** or letter.

8.5.3. When travel by commercial aircraft, follow guidelines established in DoD 5200.1R, section 7-302.

9. Reporting a security incident:

9.1. The section commander and unit security manager will be notified immediately (by close of business on the day the incident was discovered) when classified material is compromised, suspected of being compromised, loss, unauthorized disclosure, or administratively mishandled. SM will immediately (by close of business on the day the incident was discovered) notify the 920MSF/SF for action. 920MSF/SF will immediately notify 45SFS/SFAI.

9.2. The unit commander will appoint, in writing, a disinterested Noncommissioned Officer (E-7 or above), a commissioned officer or a civilian employee (GS-7 or above) to conduct inquiries or investigations into the events surrounding the violation per AFI 31-401. Provide a copy of the

appointment letter to 45SFS/SFAI and 920MSF/SF. The inquiry/investigation report will be completed within 10 working days and forwarded to 45SFS/SFAI and 920MSF/SF. If the investigating official needs more time, they will, in writing, request additional time from the unit commander and forward this request to 45SFS/SFAI and 920MSF/SF.

9.2.1. The inquiry official will be relieved of all duties until the inquiry has been completed.

9.2.2. Upon notification of being appointed as an inquiry official, the inquiry official will contact 45SFS/SFAI to receive instructions.

9.3. Security Violation Involving Electronic Mail (e-mail).

9.3.1. Once there is suspected security violation involving e-mail, contact the network system administrator, network control center, and the 920MSF/SF.

9.3.2. Comply with the network system administrator, network control center and 920MSF/SF and assist the inquiry official during their investigation.

10. Automated Information Systems (AIS) :

10.1. Computer systems must be approved by the designated approving authority prior to processing classified.

10.2. All removable AIS and word processing media are marked externally with the highest overall classification contained therein via **SF 706, Top Secret ADP Media Classification Label; SF 707, Secret ADP Media Classification Label; or SF 708, Confidential ADP Media Classification Label.**

10.3. Sections using Global Command Control Systems to produce classified documents are required to record all printed documents to ensure accountability on an AF Form 3137. All documents will be protected and destroyed IAW DoD 5200.1-R. Once documents are no longer required, ensure their disposition is recorded on the accountability log.

10. Security Awareness:

10.1. All personnel are responsible for reporting suspicious individuals or acts and unexplained influence.

10.2. SMs and supervisors are responsible for implementing a security awareness program.

11. Program Management:

11.1. 920RQG/CC is the Information, Personnel, and Physical Security Program Manager for all units within the 920RQG and delegates those duties to 920MSF/SF.

11.1.1. 920MSF/SF provides oversight and assistance to all commanders/directors/staff agency chiefs and SMs.

12.1.2. 920MSF/SF in conjunction with 45SFS conducts Information and Personnel Security Program Oversight Visits (ISPOV) on an annual basis. No notice inspections can and will be conducted as needed by 920MSF/SF and/or 45SFS. ISPOVs are conducted on all units within the 920RQG.

12.1.2.1. ISPOV reports are provided to each commander/director and are broken down by findings, observations, and recommendations. Correct findings immediately. Serious or repeat findings will be identified and will require a 30-day follow-up visit by 920MSF/SF to ensure findings have been corrected. ISPOV reports will be signed by the commander/director and filled in the SM Handbook. All findings will be corrected immediately.

12.2. Commanders, directors, and staff agency chiefs are responsible for implementation of the Information Security Program within their respective area of responsibility. The SM manages the ISP for the commander or director.

12.3. End-of-day Checks:

12.3.1. Each commander or director responsible for storing classified material establishes a system of end-of-day (duty day) security checks conducted within their area of responsibility. This ensures all classified material is stored in security containers and the security container is locked for the day.

12.3.2. Ensure a primary and alternate is designated to conduct the end-of-day check for the unit/directorate.

12.3.3. End-of-day checks will be annotated on the SF 701,. The SF 701 should be tailored to unit needs.

12.3.4. If the designated person conducting the checks finds classified unattended they will report it immediately to the SM. Secure the classified in the safe or 45SW Command Post when the security container cannot be accessed.

BRUCE E. DAVIS, Col, USAFR
Commander

Attachment 1 (Added)

GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

References

AFPD 31-4, Information Security

AFI 31-401/AFRC Supplement, Managing the Information Security Program

AFI 31-501, Personnel Security Management

DoD 5200.1-R, Information Security Program

DoD 5200.1PH, DoD Guide to Marking Classified Documents

AF Form 2586, Unescorted Entry Authorization Certificate

DD Form 2501, Courier Authorization

SF 312, Classified Information Nondisclosure Agreement

SF 700, Security Container Information

SF 701, Activity Security Checklist

SF 706, Top Secret ADP Media Classification Label

SF 707, Secret ADP Media Classification Label

SF 708, Confidential ADP Media Classification Label

920 RQG VA 31-101, ATTENTION, This Shredder Is Not Authorized For the Destruction Of Classified Material ATTENTION

920 RQG VA 31-102, This Copier Is Not Authorized For The Reproduction Of Classified Material

920 RQG VA 31-103, This Copier Is Authorized For The Reproduction Of Classified Material.

920 RQG VA 31-104, This Shredder Is Authorized For The Destruction Of Classified Material

920 RQG VA 31-105, Your Unit Security Manager Is

Attachment 2 (Added)

Annual Security Training Plan, Security Education and Motivation

First Quarter

Access and Access Requirements
Elements of Safeguarding
Protecting AIS Classified
Transmission and Transportation

Second Quarter

Physical Security
Storage of Classified
Dissemination of Classified
Destruction of Classified
Continuing Evaluation

Third Quarter

Marking Classified
Original and Derivative Classification
Safe Custodian Responsibilities
End-of-Day Checks
Protection of the President

Fourth Quarter

Personnel Security
Reporting Security Violations
Sanctions for Violating Security
Foreign Travel
OPSEC and HUMINT