



**INFORMATION SECURITY PROGRAM
MANAGEMENT**

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

NOTICE: This publication is available digitally on the AFDPO WWW site at:
<http://afpubs.hq.af.mil>.

OPR: HQ USAFE/SFXI
(Mr. Bradley W. Himelick)
Supersedes AFI 31-401/USAFE Sup 1,
21 July 1999.

Certified by: HQ USAFE/SFX (Mr. Scott L. Peake)

Pages: 14
Distribution: F

AFI 31-401, 1 November 2001, is supplemented as follows: (This supplement applies to all US Air Forces in Europe (USAFE) units, including assigned or attached Air Force Reserve and Air National Guard units and personnel as appropriate. Maintain and dispose of records created as a result of prescribed processes in accordance with Air Force Manual (AFMAN) 37-139, Records Disposition Schedule [will become AFMAN 33-322, Volume 4].)

SUMMARY OF REVISIONS

This document is substantially revised and must be completely reviewed.

1.3. Within USAFE, the statement “through command Information Security Program Manager (ISPM) channels” is defined as from the Main Operating Base (MOB) ISPM to the HQ USAFE Information Security Branch, (HQ USAFE/SFXI).

1.3.4. The Director of Security Forces (HQ USAFE/SF) is the ISPM for the command. HQ USAFE/SFXI manages the program for the command and provides direct oversight for USAFE Mission Support Squadron (MSS) at Stuttgart, Germany and the HQ USAFE Staff organizations, agencies and units located on Ramstein Air Base, Germany and its Annexes. MOBs are responsible for ensuring supported Geographically Separated Units (GSU) comply with this program. The Numbered Air Force (NAF) staffs and their associated units fall under their host MOB ISPM. NAFs are also responsible for ensuring contingency sites and other locations under their control comply with this program.

1.3.4.4. (Added) ISPMs conduct security manager meetings no less than semi-annually.

1.3.5.1. Unit Security Managers. Primary and alternate security managers will be federal employees (military or appropriated fund civilians). Government contractors may perform duties to assist the unit secu-

urity manager but will not be appointed as primary or alternate security managers for Air Force (AF) activities.

1.3.6. USAFE Staff security managers will comply with the additional program guidance outlined in **Attachment 16 (Added)**.

1.3.6.1. Security managers are the focal point for the organizational security program with primary focus being in information, industrial, personnel, and North Atlantic Treaty Organization (NATO) security programs. Responsibilities include assuring (through oversight, training, and hands-on assistance) that classified information and material is protected in accordance with Department of Defense (DoD), AF, USAFE, and local directives and guidelines.

1.3.6.10. (Added) Maintain a security manager's handbook. As a minimum, the book should include the primary and alternate security manager memorandum of appointment, applicable operating instructions (OI), list of unit security containers, vaults, and secure rooms, last semi-annual security inspection report, last Information Security program review report, minutes of the last two security manager's meetings, and a current unit Sentinel Key (SK) Clearance and Access Verification (CAVS) roster or its successor, Joint Personnel Adjudication System (JPAS), Joint Clearance and Access Verification System (JCAVS) roster.

1.4.1. HQ USAFE/SFXI will conduct information security program reviews of MOB-level programs every 18 to 24 months.

1.4.2. (Added) ISPM program reviews are assistance-orientated visits to identify noteworthy and problem areas in the information, personnel, industrial, and NATO security programs. They must be extensive enough to determine overall status of the program and must include an assessment of the security education and training as a special interest item as outlined in paragraph **8.3.3.4**. Replies are generally not required; however, corrective actions taken to correct serious problems should be recorded.

1.4.3. Information Security Program Reviews conducted by the servicing ISPM may count for a semi-annual security self-inspection.

1.4.3.1. Security Managers will not conduct semi-annual security self-inspections on their own programs. Commanders will ensure a knowledgeable person is appointed to conduct the inspections. Completed inspection reports will be forwarded to the commander for approval.

1.5.1.1.2. Within USAFE, incumbents in the following positions are delegated as certifying officials: Commander (HQ USAFE/CC); Vice Commander (HQ USAFE/CV); Director of Staff (HQ USAFE/DS); Director of Civil Engineer (HQ USAFE/CE); Director of Communications and Information (HQ USAFE/SC); Director of Financial Management and Comptroller (HQ USAFE/FM); Inspector General (HQ USAFE/IG); Director of Intelligence (HQ USAFE/IN); Judge Advocate (HQ USAFE/JA); Director of Logistics (HQ USAFE/LG); Director of Operations (HQ USAFE/DO); Director of Personnel (HQ USAFE/DP); Director of Plans (HQ USAFE/XP); Director of Safety (HQ USAFE/SE); Director of Security Forces (HQ USAFE/SF); Director of OSI Region 5 (HQ USAFE/IV); 3d Air Force Commander (HQ 3AF/CC); 3d Air Force Vice Commander (HQ 3AF/CV); 16th Air Force Commander (HQ 16AF/CC); 16th Air Force Vice Commander (HQ 16AF/CV); and the Commander and Vice Commander of the 86th Airlift Wing (86AW CC/CV), 31st Fighter Wing (31FW CC/CV), 48th Fighter Wing (48FW CC/CV), 52nd Fighter Wing (52FW CC/CV), 39th Wing (39WG CC/CV), and 100th Air Refueling Wing (100 ARW CC/CV).

1.5.1.3. Refer to **Attachment 14 (Added)** for a sample Critical Nuclear Weapons Design Information (CNWDI) briefing.

1.7.1. MOB ISPMs will conduct SF 311, Agency Information Security Program Data, item 6 data sampling from the 1st through the 14th of November, February, May, and August each year, and forward the completed SF Form 311 to HQ USAFE/SFXI by 20 August.

1.7.2. MOB ISPMs will provide the required data to HQ USAFE/SFXI by 10th day of January and July each year.

2.2. Declassification of Freedom of Information Act (FOIA) information will be coordinated with HQ USAFE/SCYI. Declassification of information under the mandatory declassification review provisions of Executive Order (EO) 12958 will be coordinated with HQ USAFE/SFXI.

3.3.1. HQ USAFE/SFXI is the command POC for all mandatory declassification reviews.

5.4. Only SK or its JPAS successor will be utilized to verify an individual's access level.

5.5. Only SK, its JPAS successor, or the employee's personnel records will be utilized to verify completion of the Nondisclosure Agreement (NdA).

5.10.1.3. Use the AF Form 143, **Top Secret Register Page**, and the AF Form 144, **Top Secret Access Record and Cover Sheet**, to control and document access to combinations safeguarding Top Secret information recorded on Standard Form (SF) 700, **Security Container Information (Part II)**.

5.10.2. Include Secret material internal control procedures in the organization's OI.

5.12.1. (Added) The use of SF 701, **Activity Security Checklist**, or SF 702, **Security Container Check Sheet**, is not required on security containers, vaults, or secure storage rooms when manned by cleared personnel on a 24-hour, 7-day-a-week basis.

5.12.2. (Added) Include on the SF 701 (if applicable): Check all classified computers to ensure that the hard drive has been removed and locked in a GSA approved container. Check all Secret Internet Protocol Router Network (SIPRNET) connections to ensure they have been disconnected and properly locked away. Check all printers utilized to print classified information to ensure ribbons have been removed and properly locked away.

5.13.2. Forward requests to HQ USAFE/SFXI.

5.15.1. DoD and Secretary of the Air Force (SAF) Memorandums, Classified Information at Meetings and Conferences, dated 26 Oct and 17 Dec 01 rescinds DoD 5200.1-R, paragraph 6-307b. Conducting classified conferences, symposia, etc., is restricted to U.S. Government or U.S. Government contractor facilities.

5.15.2. HQ USAFE/SF is approval authority for the HQ USAFE staff.

5.17.1. Forward written authorization requests for copiers and facsimile machines or any machines with copying capability to the servicing Communications and Information (SC) manager and retain the approval letter as long as the machine is utilized to reproduce classified information. Once approved and utilized to reproduce classified information, the machine becomes the property of the United States Government and will not be returned to the manufacture without written approval from the servicing SC manager that the machine has been properly cleared of classified information. Digital copiers approved to reproduce classified information will only be stored in a secure room or vault approved to the classification level of the information being reproduced.

5.17.3. Removal of ribbons from printers located in an approved secure room or vault is not required provided the room or vault continuously complies with the protection standards outlined in paragraph 5.20.1.

Ribbons from printers utilized to print classified information are classified to the level of the printed information and remain so until the ribbon has been properly destroyed. Additional declassification requirements for printers located over-seas may apply. Consult the servicing SC manager for declassification and destruction requirements and procedures.

5.20. Security managers will develop a memorandum that lists all security containers, vaults, and secure rooms located in their organization. This memorandum will include make, identification number, lock type, and location.

5.20.5. (Added) Prior to storing classified information in a vault or secure room, the servicing Civil Engineer (CE) and ISPM will survey the facility to determine if it meets the construction requirements outlined in DoD 5200.1-R, Appendix G and all other requirements of DoD 5200.1-R and AFI 31-401 for the storage of classified information. If the survey certifies that the facility meets requirements, commanders/staff agency chiefs may approve the facility for storage of classified information. If the facility does not meet requirements, consider alternate or compensatory security controls in accordance with AFI 31-401, paragraph 5.30.1.

5.20.6. (Added) Secondary doors or screens may be utilized at entrances to approved secure rooms and vaults only as an additional access control measure but will not, at any time be utilized as the primary means to secure the room or vault. Caution must be exercised to ensure the secondary door or screen affords the room or vault proper visual and audio protection to prevent compromise of the material contained within. While combinations and keys to locking mechanisms utilized to secure secondary doors and screens do not require protection to the highest classification level of material stored in the room or vault, they must be protected in such a manner to ensure only authorized personnel gain access.

5.21.1. Approval of areas to store bulky secret and confidential material using key-operated locks will be in accordance with paragraph **5.20.5. (Added)**.

5.21.2. As a minimum, lock and key custodians must be cleared to the level of the information stored in the area. Additionally, control and store all keys at the level of security required for the information contained in the area.

5.24.1. When qualified US citizen locksmiths are not available, use foreign national locksmiths to neutralize lockouts and repair security containers. Foreign national locksmiths must have a host nation-equivalent investigation for a sensitive position or position of trust (see AFI 31-501, Personnel Security Program Management, and USAFE Supplement 1), and they will be escorted at all times. The National Agency Check (NAC) or host nation-equivalent investigation is for suitability purposes only and does not allow locksmiths to have access to classified information.

5.28.3. The second Wednesday of February is the USAFE annual clean-out day.

5.29.1. Unit commanders and staff agency chiefs will post shredders approved for the destruction of classified material.

6.8. When hand carrying classified information over international borders, the courier must have identification and an authorization letter meeting the requirements of DoD 5200.1-R, paragraph 7.302a. The authorization letter will be written in English and if possible, in the language of the countries through which the courier is traveling.

7.2.1. HQ USAFE/SCYI is the command control point and maintains all USAFE nickname assignments, changes, or cancellation requests for active nicknames and code words (refer to **Attachment 15 (Added)**).

8.3.3.4. Ensure the training requirements outlined in this chapter and in Attachment 7 are included in the organization's training plan and documented in accordance with AFPD 36-22, Military Training, AFI 36-2201, Developing, Managing, and Conducting Training, AFMAN 36-2245, Managing Career Field Education and Training, and AFPAM 36-2211, Guide for Management of Air Force Training Systems. As a minimum, training documentation must include the trainee's name and grade, type of training (initial, refresher, or specialized), date of training, and a specific list of completed training subjects and tasks.

8.4. Cleared personnel are all personnel that have a security clearance.

8.5. Uncleared personnel are all personnel that do not have a security clearance.

8.15.2. ISPMs will include an assessment of the security education and training program in a separate paragraph of the annual program review report and ensure the information is discussed during the out-briefing.

9.8.1. Appoint the inquiry official within two working days from the date the incident is discovered and forward a copy of the appointment memorandum to the ISPM.

9.8.1.2. ISPM and staff judge advocate coordination will be completed prior to initiating the inquiry.

9.8.2. The inquiry will also determine if the "subject(s) of the investigation" has completed all initial and recurring training requirements outlined in Chapter 8 and Attachment 7. Verification must include the date of initial training and all dates of recurring training.

9.8.3. The training information required in paragraph 9.8.2. will be included in the "Facts" section of the preliminary report.

9.10.1. Appoint the investigative official within two working days from the date it is determined an investigation is required and forward a copy of the appointment memorandum to the ISPM.

Abbreviations and Acronyms (Added)

CAVS—Clearance and Access Verification

CE—Civil Engineer

GSU—Geographically Separated Units

JCAVS—Joint Clearance and Access Verification System

JPAS—Joint Personnel Adjudication System

MOB—Main Operating Base

MSS—Mission Support Squadron

OI—Operating Instructions

NAF—Numbered Air Force

SAF—Secretary of the Air Force

SC—Communications and Information

SIPRNET—Secret Internet Protocol Router Network

SK—Sentinel Key

Attachment 14 (Added)**SAMPLE CRITICAL NUCLEAR WEAPONS DESIGN INFORMATION (CNWDI)
BRIEFING**

A14.1. CNWDI Definition. DoD 5200.1-R defines CNWDI as “that Top Secret or Secret Restricted Data revealing the theory of operation or design of the components of a thermo-nuclear or implosion-type fission bomb, warhead, demolition munitions, or test device. Specifically excluded is information concerning arming, fusing, and firing systems; limited life components; and total contained quantities of fissionable, fissionable and high explosive materials by type. Among these excluded items are the components which DoD personnel set, maintain, operate, test, or replace.” The abbreviation CNWDI” or its related term is unclassified.

A14.2. Granting CNWDI Access:

A14.2.1. CNWDI is vital information and access must be limited to the minimum number of persons who need it to do their assigned job.

A14.2.2. Individuals granted CNWDI access must have a final Top Secret or Secret security clearance, depending on the level of information they will require. (Reference AFI 31-501, Personnel Security Program Management).

A14.2.3. Formal access authorization to CNWDI is given by the unit commander or staff agency chief and is recorded on AF Form 2583, Request for Personnel Security Action, by the unit CNWDI designated briefer, normally security manager. NOTE: Briefer does not require CNWDI access to serve as unit briefer.

A14.2.4. Completing Air Force Form 2583:

A14.2.4.1. Complete Section I, blocks 1 through 7.

A14.2.4.2. Complete Section II, block 9.

A14.2.4.3. Complete Section III, blocks 10 through 14.

A14.2.4.4. Section VI, “X” the CNWDI block and type in the level of access (i.e., Secret.)

A14.2.4.5. Complete Section VI, blocks 27, 28 and 29.

A14.2.4.6. Complete Section VII; type the following in block 30:

MEMBER REQUIRES ACCESS TO CNWDI MATERIAL.

Briefed according to DoD 5200.1-R/AFI 31-401.

Date of briefing _____.

Signature of person receiving briefing _____.

A14.3. Dissemination of Material. Disclose CNWDI material only to other personnel authorized such access. In cases where visitors require access to CNWDI, determine if access is authorized by verifying official temporary duty (TDY) orders or by contacting the visitor’s parent organization.

A14.4. Procedural Requirements. In addition to those requirements already specified for classified information, these procedures apply to CNWDI material:

A14.4.1. Marking Material:

A14.4.1.1. Mark portions of classified documents that contain CNWDI with “N” following the classification, for example: “(S-RD)(N).”

A14.4.1.2. Mark the face or front page of documents that contain CNWDI, including unclassified letters of transmittal, with:

“CRITICAL NUCLEAR WEAPON DESIGN INFORMATION--DoD DIRECTIVE 5210.2 APPLIES.”

This marking is in addition to the Restricted Data warning notice.

A14.4.1.3. Mark messages that contain CNWDI with “CNWDI” immediately following the overall classification, which is the first item of information in the text of electronically transmitted messages.

A14.4.2. Destruction:

A14.4.2.1. Two appropriately cleared personnel with need-to-know (CNWDI briefed) using approved destruction equipment (shredder or disintegrator) destroy CNWDI material.

A14.4.2.2. Destruction records are required; use AF Form 310, Document Receipt and Destruction Certificate, and file in accordance with unit file plan table and rule.

A14.4.3. Safekeeping and Storage. Protect CNWDI in the same manner prescribed for the level of classified assigned. However, limit access to such containers to only those personnel who have been granted CNWDI access. When containers are unlocked, they must be under direct surveillance by a person authorized CNWDI access.

A14.4.4. Records Management:

A14.4.4.1. File completed AF Forms 2583 in accordance with unit file plan table and rule.

A14.4.4.2. Maintain in active files until access is no longer needed.

A14.4.5. Debriefing Access:

A14.4.5.1. Debrief using AF Form 2587, Security Termination Statement.

A14.4.5.2. File completed copies of both AF Form 2583 and AF Form 2587 in accordance with unit file plan table and rule.

Attachment 15 (Added)**PROCEDURES FOR REQUESTING NICKNAME ASSIGNMENT, CHANGE, AND CANCELLATION REQUEST**

A15.1. Project officers are responsible for sending approved nicknames and exercises to appropriate communications centers or other agencies for dissemination.

A15.2. Nicknames or exercise terms cannot exceed 2 words or 21 typed spaces. In USAFE, the first word for a nickname term is “Creek” and for an exercise, “Salty.”

A15.3. A separate memorandum is required for each proposed nickname assignment, change or cancellation (refer to **Figure A15.1** below). All requests must include the action, term, Office of Primary Responsibility (OPR), unclassified meaning, duration, and point of contact information. Send requests to HQ USAFE/SCYI, Unit 3050 Box 70, APO AE 09094-5070 or E-mail: <mailto:usafe.scyi@ramstein.af.mil>

Figure A15.1. Nickname Request Memorandum

DEPARTMENT OF THE AIR FORCE

AIR FORCE UNIT HEADING

(Date)

MEMORANDUM FOR HQ USAFE/SCMI (SAMPLE)

FROM: HQ USAFE/XPP

SUBJECT: Request Nickname Assignment – CREEK ACCELERATE

1. Request assignment of the following nickname term: CREEK ACCELERATE
 - a. Unclassified Meaning: Short notice tasking for refueling-USAFE contingency support plan.
 - b. Projected Duration of Term: One year
 - c. OPR: 32 AOS/AOW
2. POC: Donald L. Larson, Major, USAF, DSN 480-5836

//Signed, 9 Feb 02//

LARNELL JONES, Colonel, USAF

Commander

1st Ind, HQ USAFE/SCMI

MEMORANDUM FOR SAF/AAZ

Request approval/disapproved.

//Signed//

RODNEY E. NEAL, MSgt, USAF

Command NICKA Manager

Attachment 16 (Added)**HQ USAFE STAFF PROGRAM GUIDANCE**

A16.1. Applicability. This attachment outlines additional procedures and requirements to govern the Information Security Program for the HQ USAFE Staff organizations. It is applicable only to the USAFE Mission Support Squadron at Stuttgart, Germany and those organizations, agencies and units assigned to the HQ USAFE Staff on Ramstein Air Base, Germany and its Annexes. It is not applicable to any other HQ USAFE Staff organization, agency or unit that is geographically separated and supported by a USAFE MOB ISPM.

A16.2. Command ISPM Channels. For the HQ USAFE Staff, the statement “through command ISPM channels” is defined as from the HQ USAFE Staff organizations, agencies, and units to HQ USAFE/SFXI.

A16.3. ISPM. The Director of Security Forces (HQ USAFE/SF) is the command ISPM. HQ USAFE/SFXI serves as the OPR to manage the program on behalf of the ISPM.

A16.4. Security Manager Meetings. HQ USAFE/SFXI will conduct semi-annual security manager meetings for the USAFE Staff.

A16.5. Security Manager Appointment Letters. Forward a copy of the primary and alternate security manager appointment letters to HQ USAFE/SFXI.

A16.6. Unit Security Operating Instruction:

A16.6.1. Forward a copy of the unit security operating instruction to HQ USAFE/SFXI.

A16.6.2. Security managers will conduct an annual review of the unit’s operating instruction in June of each year. Document results of the review in a memorandum, forward to the commander for approval, send a copy to HQ USAFE/SFXI, and maintain a copy of the memorandum in the security manager’s handbook.

A16.7. Security Manager Meeting Minutes. Maintain the minutes of the last two security manager meetings in the security manager’s handbook.

A16.8. Semiannual Security Self-Inspections. Utilize the HQ USAFE/SFXI provided checklists (AF Form 2519, All Purpose Checklist) to conduct the semiannual security self-inspections. Maintain the last semiannual security self-inspection inspection report and completed checklists in the security manager’s handbook. Forward a copy of the semiannual security self-inspection report to HQ USAFE/SFXI.

A16.9. Security Managers Handbook. Maintain a security manager’s handbook with the following:

A16.9.1. Primary and alternate security manager memorandum of appointment.

A16.9.2. Primary and alternate security manager training certificates or other documented proof of training completion.

A16.9.3. Applicable operating instructions and annual review memorandum.

A16.9.4. List of unit security containers, vault and secure rooms.

A16.9.5. Vault and secure room survey reports and approval memorandums.

A16.9.6. List of unit shredders approved for the destruction of classified material.

A16.9.7. Unit protection, removal, or destruction of classified material plan (if not included in the unit's operating instruction).

A16.9.8. Unit classified material reproduction authority appointment letters.

A16.9.9. Last semiannual security self-inspection report and completed checklist.

A16.9.10. Last Information Security program review report, to include written replies to findings (as required).

A16.9.11. Minutes of the last two-security manager's meetings.

A16.9.12. Current unit SK CAVS roster or its successor, JPAS JCAVS roster.

A16.10. Program Reviews. USAFE/SFXI will conduct annual program reviews on the HQ USAFE Staff programs. Program review reports will identify discrepancies as either an observation or a finding. Observations and most findings do not require a reply; however, repeat findings and those deemed critical and have a significant impact on the program require a written reply from the commander to HQ USAFE/SF. Written replies will include action taken to correct the finding and status of the finding (if open, provide estimated completion date; if closed, provide the date the finding was corrected).

A16.11. Top Secret Control Account (TSCA). Forward TSCA appointment letters to HQ USAFE/SFXI.

A16.12. Secure Conference Facilities. Forward written requests for Secure Conference Facilities to HQ USAFE/SFXI.

A16.13. Security Container, Vault, and Secure Room List. Forward a copy of the security container, vault, and secure room list to HQ USAFE/SFXI.

A16.14. Vault or Secure Room Surveys and Intrusion Detection System .

A16.14.1. Vault or Secure Room Surveys . Utilize AF Form 332, **Base Civil Engineer Work Request**, for vault or secure room surveys. The request must be coordinated through the unit security manager, signed by the commander or designated representative, coordinated first through HQ USAFE/SFXI and then the 86 SFS/SFXRP, and then submitted to the 86 CES/CCD. Once the survey is scheduled, it is the requesting organization's responsibility to notify HQ USAFE/SFXI since the survey must be conducted jointly between HQ USAFE/SFXI and the 86 CES/CCD. If subsequent work requests are required for structural improvements or modifications to the vault or room, complete and submit another AF Form 332 following the procedures outlined above. Vaults or rooms that are structurally modified or altered after initial certification require re-certification to ensure they still comply with DoD 5200.1-R, Appendix G.

A16.14.2. Intrusion Detection Systems. Installation of Intrusion Detection System (IDS) requires a separate AF Form 332. The request must be coordinated through the unit security manager, signed by the commander or designated representative, coordinated first through HQ USAFE/SFXI and then the 86 SFS/SFXRP, and then submitted to the 786 CES/CEOP-R. The requesting organization must also submit an AF Form 3215, Communication Work Request to the 86 Communications Group for the installation of or to secure one free and serviceable twisted cable pair to connect the alarm to the appropriate control panel.

A16.14.3. Survey Reports and Approval Memorandums. The unit security manager will maintain a copy of the vault and secure room survey report and approval memorandums in the unit security manager's handbook, and forward a copy of the approval memorandum to HQ USAFE/SFXI.

A16.15. Approved Classified Material Shredders. Security managers will develop a memorandum that lists shredders approved for the destruction of classified material located in their organization. This memorandum will include make, ID number, and location.

A16.16. Security Manager Training. HQ USAFE/SFXI is responsible for conducting security manager training for the USAFE Staff Security Managers. Forward training requests to HQ USAFE/SFXI.

A16.17. Original Classification Authority (OCA) and Declassification Authority Training. Forward requests for OCA and Declassification Authority training to HQ USAFE/SFXI.

A16.18. Security Incidents:

A16.18.1. Reporting Security Incidents . Security managers or commanders will report all security incidents to HQ USAFE/SFXI by the end of the first duty day.

A16.18.2. Preliminary Inquiry Appointment Memorandum Format. Use the preliminary inquiry appointment memorandum format outlined in [Figure A16.1](#).

Figure A16.1. Inquiry Official Memorandum.

APPOINTMENT OF INQUIRY OFFICIAL MEMORANDUM

DEPARTMENT OF THE AIR FORCE

AIR FORCE UNIT HEADING

(Date)

MEMORANDUM FOR (Inquiry Official's Name, Organization, and Office Symbol)

FROM: (Organizational Commander, Director)

SUBJECT: Appointment of Inquiry Official, Security Incident No. (USAFE/SFXI assigns the incident number)

1. Under the provisions of DoD 5200.1-R and AFI 31-401, you are appointed to conduct a security inquiry into Security Incident (Incident Number) reported to me by (rank, name, organization, and office symbol). The incident involves (provide a short summary of the incident, to include the location, time, and dated of the incident. **NOTE:** Ensure the summary of the incident does not include any classified information).

2. The purpose of this inquiry is to determine whether a compromise occurred, and to categorize this security incident as a compromise, potential compromise, security violation or security infraction as outlined in AFI 31-401, paragraph 9.2. You are authorized to interview those persons necessary to complete your findings. Your records indicate that you have a (Secret, Top Secret, etc.) security clearance; therefore, you are authorized access to all pertinent records and files, to include those classified up to and including (level of classified). Should you determine this incident involved access to program information for which you are not authorized, advise our unit security manager (name and office symbol of the unit security manager) who will coordinate with HQ USAFE/SFXI for guidance and assistance.

3. Conducting this inquiry will be your primary duty until it is completed. You will schedule an appointment with HQ USAFE/SFXI and HQ USAFE/JA for required briefings before beginning your inquiry. Your report will be coordinated through our unit security manager and forwarded in hard copy and electronically to HQ USAFE/SFXI by (give the inquiry official an exact date somewhere between 10 but not

exceeding 30 workdays from the date of appointment to complete the inquiry). As a minimum, your report must contain the following:

- a. A statement that a compromise or potential compromise did or did not occur.
 - b. Category of the security incident.
 - c. Level of classified information or material involved (Confidential, Secret, Top Secret, etc.)
 - d. Cause factors and responsible person(s).
 - e. Any previous security incidents the subject(s) caused or were involved in over the past 2 years (provide a brief description of the prior incident(s), to include date and location, whether the incident resulted in a compromise or potential compromise, category of the security incident, level of classified information involved, and outcome of the incident).
 - f. Date(s) the subject(s) of the investigation completed initial and recurring training requirements outlined in AFI 31-401, USAFE Supplement, Chapter 8 and Attachment 7.
 - g. Recommended corrective actions needed to preclude a similar incident.
4. Should you determine that a compromise did occur, you are to notify our unit security manager, HQ USAFE/SFXI, and me immediately.
5. Notify me if you have any questions. If you require technical assistance during the course of the inquiry, coordinate with our unit security manager. If further assistance is required, (name and office symbol of the unit security manager) will assist you in obtaining additional assistance from HQ USAFE/SFXI and HQ USAFE/JA.

(Appointing authority's signature block and signature)

A16.18.3. ISPM and Staff Judge Advocate Coordination. Inquiry and investigative officials will schedule an appointment with HQ USAFE/SFXI and HQ USAFE/JAM to receive required briefings and materials that outlines their duties and responsibilities prior to initiating the inquiry.

A16.18.4. Preliminary Inquiry Report Format. Use the preliminary inquiry report format outlined in [Figure A16.2](#).

Figure A16.2. Preliminary Inquiry Of Security Incident Report

DEPARTMENT OF THE AIR FORCE

AIR FORCE UNIT HEADING

(Date)

MEMORANDUM FOR (Inquiry Appointing Official)

FROM: (Inquiry Official's Name, Organization, and Office Symbol)

SUBJECT: Preliminary Inquiry Report of Security Incident No.

1. Authority: A preliminary inquiry was conducted (date) under the authority of the attached memorandum.
2. Matters investigated: The basis for this inquiry was that (provide a short summary of the security incident including the date it occurred, the classification of information involved, and the document control

number if specific documents were involved. (Refer to AFI 31-401, Information Security Management Program, paragraph 9.5., for security classification requirements.).

Personnel Interviewed: (list all personnel interviewed, their position title, office symbol, and security clearance).

Facts: (List specific details answering who, what, why, where, and when questions concerning the security incident. Include information of any previous security incidents the subject(s) caused or was involved in over the past two (2) years (provide a brief description of the prior incident(s), to include date and location, whether the incident resulted in a compromise or potential compromise, category of the security incident, level of classified information involved, and outcome of the incident) and the date(s) the subject(s) of the investigation completed initial and recurring training requirements as required in AFI 31-401, USAFE Supplement, Chapter 8 and Attachment 7).

Conclusions: As a result of the investigation into the circumstances surrounding the security incident, interviews, and personal observations, it is concluded that: (List specific conclusions reached based on the facts and if a compromise or potential compromise did or did not occur. If a damage assessment is or has been done, provide the point of contact along with; the status of the assessment if it hasn't been completed; or, describe the outcome if it has been completed; or, provide a copy of the completed assessment report.)

Recommendations: (list corrective actions needed to preclude a similar incident; the category of the incident; damage assessment; if the incident is a compromise, probable compromise or no compromise; and, if this inquiry should be closed without further investigation or with a recommendation for a formal investigation).

(Inquiry official's signature block and signature)

Attachment:

Appointment of Inquiry Official Memo, (date)

1st Ind, (Inquiry Appointing Official's Organization and Office Symbol)

(Date)

MEMORANDUM FOR HQ USAFE/SF

(The Inquiry Appointing Official's endorsement will include concurrence or nonconcurrence with the findings, conclusions, and recommendations contained in the report, corrective actions to be implemented by the unit to prevent future occurrences (be as specific as possible to include the type of action and dates the action will be completed), and the recommendation that the inquiry be closed or a formal investigation initiated.)

(Appointing authority's signature block and signature)

A16.18.4. Completed Report Coordination. Forward completed reports to HQ USAFE/SFXI through the unit security manager. HQ USAFE/SFXI will review the report and forward it to HQ USAFE/JAM for coordination. Upon completion of the coordination process, HQ USAFE/SFXI will complete a memorandum recommending concurrence or non-concurrence and forward the report to the HQ USAFE/SF for approval. Once HQ USAFE/SF approves the report, HQ USAFE/SFXI will forward a hard copy of the approval memorandum and the report to the unit commander or equivalent through the unit security manager.

A16.18.5. Report Disposition. Security managers will provide a copy of the completed report to HQ USAFE/SFXI and maintain a copy in accordance with AFMAN 37-139, Records Disposition Schedule.

JOHN T. SALLEY, JR., Colonel, USAF
Director of Security Forces