BY ORDER OF THE COMMANDER
AIR FORCE GLOBAL STRIKE COMMAND

AIR FORCE INSTRUCTION 31-401

AIR FORCE GLOBAL STRIKE COMMAND SUPPLEMENT

8 SEPTEMBER 2010

Information Protection (IP)

INFORMATION SECURITY PROGRAM MANAGEMENT

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

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

RELEASABILITY: There are no releasability restrictions on this publication.

OPR: HQ AFGSC/IP

Certified by: HQ AFGSC/IP
(Mrs. Wendi L. Marshall)
Pages: 25

This supplement implements and extends the guidance of AFI 31-401, ***Information Security Program Management***, 1 November 2005. This supplement describes AFGSC's procedures for use in conjunction with the basic AFI. This supplement applies to all AFGSC personnel and tenant units on AFGSC installations. This supplement provides a baseline requirement for managing the Information Security Program. Deviations to this supplement must be approved by the Office of Primary Responsibility (OPR) prior to implementation. Refer recommended changes and questions about this publication to the OPR using the AF IMT 847, ***Recommendation for Change of Publication***; route AF IMT 847s from the field through the appropriate functional's chain of command. Provide copies of base supplements and this supplement to HQ AFGSC/IP. This supplement applies to Air National Guard and Air Force Reserve units tenant on AFGSC installations and participating under program oversight. Ensure that all records created as a result of processes prescribed in this publication are maintained in accordance with AFMAN 33-363, ***Management of Records***, and disposed of in accordance with the Air Force Records Information Management System (AFRIMS) Records Disposition Schedule (RDS) located at https://www.my.af.mil/gcss-af61a/afrims/afrims/. The use of the name or mark of any specific manufacturer, commercial product, commodity, or service in this publication does not imply endorsement by the Air Force. This instruction requires collecting and maintaining information protected by the Privacy act of 1974 authorized by 10 U.S.C. 8013, Secretary of the Air Force and E.O. 9397 (SSN). System of records notice F031 AF SP M, Personnel Security Access Records, applies.

1.3.4.1. Information Security Program Managers (ISPM) below MAJCOM-level will provide additional local guidance to this supplement, as necessary. This may be as a supplement or in a local instruction. Provide AFGSC/IP with a copy of any local guidance created.

1.3.4.2.3. Contractors located on AFGSC installations will be designated as integrated visitor groups or intermittent visitors unless the Installation Commander deems circumstances exist to identify the contractor operation as a cleared facility. Ensure the procedures outlined in AFI 31-601, ***Industrial Security Program Management*** are followed if a DD Form 254, ***Department of Defense Contract Security Classification Specification*** indicates a cleared facility will be needed.

1.3.4.5. ISPMs will prepare and distribute meeting minutes to security managers and other participants attending the security manager meeting.

1.3.4.6. (Added). Non-AFGSC units with permanently assigned security specialist staff located on AFGSC installations who can demonstrate that it is impractical to receive local ISPM support must address non-participation in this support function IAW AFI 25-201, ***Support Agreement Procedures***.

1.3.4.7. (Added). ISPMs will establish files for each activity/unit and maintain the following official records, as appropriate, in accordance with (IAW) the Records Distribution Schedule (RDS):

1.3.4.7.1. (Added). Appointment letters (e.g., Security Managers, Top Secret Control Officers (TSCO), Top Secret Control Account (TSCA) establishment, etc).

1.3.4.7.2. (Added). Copy of the last annual program review report.

1.3.4.7.3. (Added). Copy of secure room and/or vault certification letters.

1.3.4.7.4. (Added). Security manager training documentation.

1.3.4.8. (Added). ISPMs invite non-AFGSC units on AFGSC bases to participate in the AFGSC Information Security Program. AFGSC units located on non-AFGSC bases will enter into a host-tenant support agreement with the host activity and participate fully.

1.3.5.1. Post AETCVA 31-9, ***Security Manager Designation***, or similar locally produced posting in a conspicuous place within each occupied unit/agency facility. Adding digital photos of the security manager and alternates to the visual aid enhances identification of each security manager is authorized, however, not manditory.

1.3.6.11. (Added). Security managers will maintain a security manager's handbook. It will include, but is not limited to, the following official records, including miscellaneous items, with accompanying separate RDS disposition instructions:

1.3.6.11.1. (Added). Appointment letters.

1.3.6.11.2. (Added). Listing of storage containers, vaults, secure rooms and any certified open discussion areas by number and location.

1.3.6.11.3 (Added). Listing of approved classified reproduction equipment by location with approval letter.

1.3.6.11.4. (Added). Internal security operating instruction(s).

1.3.6.11.5. (Added). Self-inspection checklist provided to the unit security manager by the ISPM.

1.3.6.11.6. (Added). Copy of the last self-inspection report.

1.3.6.11.7. (Added). Copy of the last annual program review report.

1.3.6.11.8. (Added). Security training material with documentation showing when training was completed on each unit member.

1.3.6.11.9. (Added). Security manager meeting minutes for the past 12 months.

1.3.3.11.10. (Added) Joint Clearance and Access Verification System (JCAVS) Eligibility and Access Report current within the last 30 days

1.3.6.11.11. (Added). Miscellaneous items.

1.4.1. Information security oversight requirements are incorporated into appropriate HQ AFGSC/IG inspection checklists and updated on a recurring basis. Utilize these checklists to develop local checklists that cover mission and unit unique requirements.

1.5.1.1. Division Chiefs and above and security managers are delegated the authority to sign DOE Forms 5631.20 "For" AFGSC/CC in his capacity as the Restricted Data access granting official for the command.

1.5.1.2.4. (Added). A sample CNWDI briefing is provided in **Attachment 8** (Added) to this supplement, that may be used when briefing individuals prior to granting CNWDI access.

1.7.1.1. The Standard Form (SF) 311, ***Agency Security Classification Management Program Data*** will include the total number of classification decisions on finished products, regardless of media or whether produced in electronic form. Units will collect numbers of classification decisions for the SF 311 the second and third full weeks of the second month of each quarter (Nov, Feb, May, Aug) and report results on SF 311 to AFGSC/IP no later than the first of the third month. Air National Guard units will report their numbers to NGB/A7SI.

1.7.1.1.3. (Added). Do not count unclassified transmittal documents.

1.7.1.2. (Added). Include the following types of materials on the SF 311: electronic presentations, e-mail, official correspondence or memoranda, photographs, reports and/or intelligence products, web pages, and Wiki articles or blog articles. The following is provided on how to count classification decisions:

1.7.1.2.1. (Added). E-Mail. If a classified e-mail is disseminated and no additional classified information is added in the replies or forwards, then only the first classified e-mail should be counted. The replies and forwards that do include additional classified information should be counted in addition to the original classified e-mail. Do not count unclassified e-mails that are created on a system that is certified to handle classified information. If the e-mail is merely a transmittal vehicle for a classified attachment and contains no classified information itself, then do not count the e-mail. Only count the classified attachment if it was originated by your office.

1.7.1.2.2. (Added). Web Pages. Each web page containing classified information that is created during the reporting period should be counted only once regardless of how many times it was modified or updated. The count should be conducted by the agency or command that hosts the web page.

1.7.1.2.3. (Added). Blogs. Every individual blog entry that constitutes a classification action should be counted. The count should be conducted by the agency or command hosting the blog.

1.7.1.2.4. (Added). Wiki Articles. Each wiki article containing classified information that is created during the reporting period should be counted, and counted only once, regardless of how

many times it is modified or updated by other users. This count should be conducted by the agency or command hosting the wiki.

1.7.1.2.5. (Added). Instant Messages. Instant messages should not be counted.

3.6. Systematic Review for Declassification. AFGSC activities will review their classified holdings with a view towards declassification during their annual clean out day(s). This review pertains to classified holdings that were originally or derivatively classified by the activity. Annual clean out days may coincide with required records conversion at minimum, on or about December 31st or September 30th as applicable. Although they will not reveal classified data, activities will ensure supporting records managers have approved classified records as maintained and listed on the activity file plan. They will also ensure proper records retention and disposition in accordance with the RDS.

5.8.1.1. Establishing a Top Secret Control Account (TSCA). Unit commanders and staff agency chiefs provide written notification to the servicing ISPM when establishing a TSCA and/or designating TSCOs. When requested, the ISPM provides training to these newly appointed officials.

5.8.2. Secret. Enclose the receipt in the inner envelope or container.

5.8.6. (Added). Commanders and staff agency chiefs ensure local security operating instructions address facsimile transmissions via secure circuits when these secure systems exist within their unit. Also, conspicuously post quick reference operating procedures at equipment authorized to transmit classified information. These procedures should outline how facsimile equipment is operated in a secure mode.

5.8.7. (Added). Include procedures for handling registered, certified, first class, and express mail in agency local operating instructions.

5.9.3. (Added). Include the Wing or equivalent records managers disaster preparedness plan and vital records program.

5.11.2. Submit residential storage requests to the Director of Information Protection (HQ AFGSC/IP) for approval. Requests will contain full justification for residential storage and operating instructions/contingency plans for the protection of classified information at the residence.

5.13.2. Facility Approval Authority. Organizations will use the checklist in **Attachment 9** (Added) before conducting conferences, seminars, exhibits, symposia, conventions, training courses, or other such gatherings during which classified information is disseminated to ensure proper safeguarding and access requirements are met.

5.13.2.1. (Added). Organizations will notify the ISPM, in writing, of all secure conference facility requirements. Information protection and civil engineering personnel will inspect all new and modified secure conference facilities to ensure security requirements and construction standards are met IAW **Attachment 10** (Added). Results of the inspection will be documented in writing and maintained in the official records repository. The servicing ISPM certifies secure conference facilities in writing. The requesting organization maintains the original certification package and the ISPM maintains a copy IAW the RDS.

5.13.2.2. (Added). Proposed structural modifications to secure conference facilities must be coordinated with the ISPM and civil engineer. The ISPM and civil engineer must recertify, in writing, the structural integrity of secure conference facilities that have been modified.

5.14.2.4. (Added). If none of the criteria in paragraphs **5.14.2.1** through **5.14.2.3** can be met, U.S. cleared personnel must provide continuous surveillance.

5.14.6. During weather diverts and in-flight emergencies, aircraft commanders will determine how classified information will be secured using the procedures in paragraph **5.14**, as applicable. When those procedures cannot be met, and U.S. cleared personnel are not available, using local guards for area control is an acceptable risk when combined with the use of tamper evident seals on aircraft openings. When local guards are not available, the use of tamper evident seals on aircraft openings will be the minimum-security requirement. If the seal is subsequently determined to have been broken, the aircraft commander inspects the aircraft for damage, theft of equipment, sabotage, etc. The aircraft commander will report the incident to their home base servicing security office.

5.15.1. Machines with Copying Capability. Copiers with volatile memory, no permanent memory, can be approved for classified reproduction. Copiers with permanent memory are not authorized for classified reproduction. Procedures must be developed to ensure volatile memory is erased after each classified reproduction. Depending on the model, memory can be erased by turning off the copier and/or unplugging the copier.

5.18.2. Organizations will notify the ISPM, in writing, of all vault or secure room requirements. Vaults and secure rooms will not be certified for convenience. Information protection and civil engineering personnel will inspect all new and modified vaults and secure rooms to ensure security requirements and construction standards are met IAW DoD 5200.1-R, Appendix 7**.** Results of the inspection will be documented in writing and maintained in the official records repository. The ISPM certifies secure rooms and vaults in writing. The requesting organization maintains the original certification package in the vault or certified room, and the ISPM maintains a copy; copies must be maintained IAW the RDS.

5.18.2.1. (Added). Proposed structural modifications made to vaults and secure rooms must be coordinated with the ISPM and civil engineer. The ISPM and civil engineer must recertify, in writing, the structural integrity of vaults and secure rooms that have been modified.

5.18.2.2. (Added). Requesting organization must develop and maintain IAW the RDS a written plan or operating instruction outlining procedures for providing protection and positive entry control to the vault or secure room.

5.18.2.3. (Added). Organizations must notify the ISPM, in writing, when the vault or secure room is no longer used for classified storage. Notify the supporting records manager when records that were required to be cross-referenced on the file plan are no longer maintained. Ensure classified records moved to a new location are appropriately identified on the file plan.

5.18.2.4. (Added). Supplemental controls, such as intrusion detection systems (IDS), continuous personal surveillance, or 4-hour checks, are required for secure rooms approved/certified after 1 Oct 95 storing Secret information.

5.24.1. Unit commanders or equivalents, and staff agency chiefs designate and approve reproduction equipment in writing.

6.1.7. (Added). Commanders will ensure the local unit INFOSEC OI covers receipt of certified, registered and first class mail by unit personnel and the need to protect it as classified. The procedures will also take into account ensuring uncleared personnel are aware they may not accept these types of items.

6.7.3.3. (Added). When classified material is handcarried off an installation, the outer wrapper will be marked **"OFFICIAL BUSINESS - MATERIAL EXEMPTED FROM EXAMINATION"** and bearing the signature of the same person who authorized the courier to handcarry classified material.

6.8. Documentation. Courier authorization letters are required when handcarrying classified information off an installation. The DD Form 2501, ***Courier Authorization***, is not authorized for use in AFGSC since a courier letter is mandated.

7.3. (Added). Unless prohibited by the SAP or classified, units will provide the ISPM with contact information (e.g., local appointment letters) for SAP managers at the unit level. This would include managers for NC2, OPSEC, CNWDI, etc. The appointed individual will also provide the ISPM with any required training standards for the program.

7.4. (Added). Unless prohibited by the SAP or classified, a copy of open storage certification paperwork will be provided to the servicing ISPM to be maintained in the unit folder.

7.4.1. (Added). Unless prohibited by the SAP the ISPM staff will conduct a certification of any approved open storage areas for "collateral" storage. This report may be provided to the HHQ SAP agency if requested and will be maintained in the unit folder.

8.3.3.1. All newly assigned security managers and alternates will notify the ISPM within 15 days of assignment to be scheduled for security manager training.

8.3.3.4. Records can be maintained electronically using spreadsheets, "read" receipts, or other tracking methods, but the records must be listed on an approved file plan.

8.3.5.7. Training certificates will, as a minimum, include the full name and rank of the student, course name, and dates of training. AF Form 1256, ***Certificate of Training***, can be used for this purpose.

8.4.1.3. Use of electronic e-mail receipts satisfies written acknowledgement requirements for NATO training.

8.5.2. Document initial training for uncleared personnel in accordance with paragraph **8.3.3.4** of this instruction.

8.6. Original Classification Authorities (OCAs). OCA training records must reflect the name of the OCA and the date training was accomplished as a minimum.

8.7.1. (Added). Commanders will ensure derivative classifiers in the unit are identified and appointed. Security managers will ensure the individuals receive sufficient training to properly execute their duties. The list of derivative classifiers will be provided to the ISPM for inclusion in the unit folder.

8.8. (Added). The RD appointing official will provide the ISPM with a copy of the RD Management Official appointment letter and it will be included in the unit folder.

8.8.1. (Added). The RD Management Official will ensure standardized training and access requirements are provided to the ISPM. The ISPM will ensure the procedures are provided to units as required.

8.10.1.7. (Added). The SAP manager will ensure any required briefings/debriefings are completed and filed IAW the SAP requirements. The SAP manager will also be responsible for establishing JPAS indoctrination procedures.

9.8.4. (Added). The installation ISPM must submit the Security Incident Data Report to HQ AFGSC/IP NLT 15 Jan and 15 Jul each year as outlined in AFPD 31-4, Attachment 2, A2.1.

9.9.1. Within Headquarters AFGSC Staff element - Headquarters-level directors and division chiefs may be appointing officials. The appointed inquiry official (IO) must be an impartial individual. If the unit commander/director/staff agency chief is involved in the incident, IO appointment will be elevated to the next level of command. Security managers shall not be appointed as an IO for an incident that occurred within their unit. The individual will be a commissioned officer, a senior noncommissioned officer, or a GS-9 or Pay Band 2 civilian or higher, and will be of equal or greater rank than the subject(s) of the inquiry.

9.9.1.3. (Added). ISPMs will utilize the briefing at **Attachment 11** (Added) to brief the IO. ISPMs may add point-of-contact information to the briefing, but will not modify the briefing content.

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

9.9.9. (Added). The ISPM will perform a technical review to ensure all aspects of the incident have been addressed. If questions remain unanswered, the report will be returned to the IO for correction. Once all questions have been satisfactorily addressed, the ISPM will either concur or non-concur, in whole or in part, with the IO's recommendations and conclusions. Under no circumstances will the ISPM attempt to influence the IO's conclusions.

9.9.10. (Added). If the IO and ISPM reviews all concur with each other, and if the appointing official concurs with both of them, the appointing official may simply concur with their conclusions and recommendations and verify corrective actions are complete. If the appointing official non-concurs with the IO and /or ISPM the appointing official must state why in a memorandum.

9.9.11. (Added). If the incident involved a potential or actual compromise the closure letter will address the required damage assessment notification to the OCA.

9.14. Forms Adopted. AF Form 1256, ***Certificate of Completion***, and AF Form 2583, ***Request for Personnel Security Action***, SF 311, ***Agency Security Classification Management Program Data***.

DOUGLAS C. LITTLE, GS-14, USAF
Director, Information Protection

Attachment 1

GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

References

DoD 5200.1-R (**http://www.dtic.mil/whs/directives/corres/pdf/52001r_0197/p52001r.pdf**), *Information Security Program*, 14 January 1997

AFI 25-201, (**http://www.e-publishing.af.mil/shared/media/epubs/AFI25-201.pdf**), *Support Agreement Procedures*, 1 May 2005

AFI 31-401 (**http://www.e-publishing.af.mil/pubfiles/af/31/afi31-401/afi31-401.pdf**), *Information Security Program Management*, 1 November 2005

Air Force Records Information Management System (**https://afrims.amc.af.mil/rds/index.cfm**), *Air Force Records Disposition Schedule*

Abbreviations and Acronyms

AFNIC/CTTA—Air Force Network Integration Center Certified Technical TEMPEST Authority

AFRC—Air Force Reserve Command

ANG—Air National Guard

HQ AFGSC/IP—AFGSC Information Protection Directorate

IAW—In accordance with

LAN—Local Area Network

NIC—Noise Isolation Class

PED—Portable/Personal Electronic Devices

RDS—Records Disposition Schedule

RF—Radio Frequency

STC—Sound Transmission Class

TL—Transmission Loss

VU—Volume Unit

Attachment 8 (Added)

SAMPLE CRITICAL NUCLEAR WEAPONS DESIGN INFORMATION (CNWDI) BRIEFING

A8.1. (Added). CNWDI Definition. DoD 5200.1-R defines CNWDI as "that Top Secret Restricted Data 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 munition, or test device. Specifically excluded is information concerning arming, fusing, and firing systems; limited life components; and total contained quantities of fissionable, fusionable, and high explosive materials by type. Among these excluded items are the components that DoD personnel set, maintain, operate, test, or replace." The abbreviation "CNWDI" or its related term is unclassified.

A8.2. (Added). Granting CNWDI Access:

A8.2.1. (Added). CNWDI is vital information and access is limited to the minimum number of persons who need it to do their assigned job.

A8.2.2. (Added). Individuals granted CNWDI access must have a final Top Secret or Secret security clearance, depending on the level of information they will require. Immigrant aliens can be certified for access to CNWDI only by select officials at HQ USAF and above levels of command.

A8.2.3. (Added). Formal access authorization to CNWDI is given by division chiefs and above, and is recorded on AF Form 2583, ***Request for Personnel Security Action***. ***NOTE:*** Briefer does not require CNWDI access to serve as unit briefer.

A8.2.4. (Added). AF Form 2583. Complete Section I, blocks 1 through 7; Section II, block 9; Section III, blocks 10 through 14; Section VI, blocks 27 through 29; and Section VII by entering the following in block 30:

MEMBER REQUIRES ACCESS TO CNWDI MATERIAL FOR ROUTINE ACCESS.

Briefed according to DoDD 5210.2 and AFI 31-401. Date of briefing _____.
Signature of person receiving briefing _____.

A8.2.5. (Added). Keep the AF Form 2583 in unit files for duration of the individual's access to CNWDI and dispose of IAW RDS.

A8.3. (Added). Dissemination of Material. CNWDI material can be disclosed only to other personnel authorized such access. In cases where visitors require access to CNWDI, determine if access is authorized by verifying JPAS, official visit requests, or by contacting the visitor's parent organization.

A8.4. (Added). Procedural Requirements. In addition to those requirements already specified for other classified information, these procedures apply to CNWDI material:

A8.4.1. (Added). Marking Material:

A8.4.1.1. (Added). Mark portions of classified documents that contain CNWDI with "(N)" following the classification; for example, "(S-RD)(N)."

A8.4.1.2. (Added). 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.

A8.4.1.3. (Added). 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.

A8.4.2. (Added). Safekeeping and Storage. Protect CNWDI in the same manner prescribed for the level of other classified information; however, limit access to such containers to only those personnel who have been granted CNWDI access. When containers are unlocked, they must be under the direct surveillance of a person authorized CNWDI access.

A8.4.3. (Added). Compromise of CNWDI Material. Since CNWDI material is Restricted Data, the Atomic Energy Act of 1954 governs its use. Always send notifications of suspected CNWDI compromises through Information Protection channels to the Directorate of Information Protection (SAF/AAP).

A8.4.4. (Added). Transmission of Material. Show on envelopes or other containers enclosing CNWDI the Restricted Data warning notice, the DoD Directive 5210.2 notice (see A8.4.1.2. (Added) above), and the notation "To be opened only by personnel authorized access to CNWDI material."

A8.4.5. (Added). Disposal and Destruction. Ascertain disposal IAW the RDS. In addition to the required number of persons to witness destruction of other classified material, persons destroying CNWDI or committing this material to a central destruction activity must be cleared for CNWDI access.

A8.5. (Added). CNWDI Debriefings. When access is no longer required, an individual is debriefed, using AF Form 2587, ***Security Termination Statement***. Maintain the AF Form 2587 IAW RDS.

Attachment 9 (Added)

CLASSIFIED MEETING/CONFERENCE CHECKLIST

A9.1. (Added). Initial Preparation:

A9.1.1. (Added). Determine subject of meeting and highest level of classification, to include special handling/access, NATO, CNWDI, SIOP, etc.

A9.1.2. (Added). Determine if entire meeting will be classified or limited to classified sessions.

A9.1.3. (Added). Determine where the classified material will be stored before, during, and after the meeting.

A9.1.4. (Added). If possible, select a meeting location that provides good physical control, has storage containers (if required), and provides protection from unauthorized audio and visual access.

A9.1.5. (Added). Identify potential attendees.

A9.1.6. (Added). Identify foreign attendees or representatives, if any. ***NOTE:*** Get approval for release of any information (unclassified and classified) from the Foreign Disclosure Policy Officer. Any US citizen representing a foreign interest is a foreign representative.

A9.1.7. (Added). Announce the meeting on a need-to-know basis (e-mail, phone, etc).

A9.1.8. (Added). Establish routing for visit requests for attendees.

A9.1.9. (Added). Verify security clearances using JPAS and establish need-to-know.

A9.1.10. (Added). Establish a method to identify attendees for entry/reentry.

A9.1.11. (Added). Identify any special communication requirements, i.e., STU-III (if required).

A9.2. (Added). Inspect Area Prior to Meeting:

A9.2.1. (Added). If not familiar with area, request presence of building manager.

A9.2.2. (Added). Check walls, ceilings, and floors for suspicious objects, e.g., holes, openings, exposed wires, recording devices.

A9.2.3. (Added). Ensure all doors, windows, and other openings are closed before classified briefing begins. First floor windows should be covered to prevent visual access.

A9.2.4. (Added). Check all physically accessible areas.

A9.2.5. (Added). Check, touch, and lift, if possible, the following items/areas for things out of the ordinary, i.e., recording devices.

A9.2.5.1. (Added). Trash containers

A9.2.5.2. (Added). Fire extinguishers

A9.2.5.3. (Added). Tables, desks, and chairs

A9.2.5.4. (Added). Curtains, pictures, or like accessible items on walls and windows

A9.2.5.5. (Added). Circuit breaker boxes; use safety precautions

A9.3. (Added). During the Meeting:

A9.3.1. (Added). Prevent unauthorized entry by posting appropriately cleared personnel outside the meeting area or lock entrances to control access.

A9.3.2. (Added). Ensure conversations within the meeting room/area cannot be heard by uncleared personnel outside the area.

A9.3.3. (Added). Identify all attendees upon reentry from breaks, etc.

A9.3.4. (Added). Identify and verify security clearance of attendees by checking on-hand rosters, lists, visit requests, messages, etc. that have been verified through JPAS.

A9.3.5. (Added). Check briefcases for unusual or suspicious items, if allowed beyond entry control point.

A9.3.6. (Added). Ensure cellular phones, radios, tape recorders, or devices that can transmit or record are not allowed within rooms/areas where classified information is discussed, briefed, or processed.

A9.3.7. (Added). Discourage note taking. If allowed, required safeguarding, marking, and transmission requirements apply to classified notes.

A9.3.8. (Added). Ensure the highest level of each classified session is appropriately identified to the attendees.

A9.3.9. (Added). Remind each attendee that the classified portion of the briefing should not be discussed freely once the meeting is finished and their responsibility to protect classified information.

A9.3.10. (Added). Ensure classified material used for the meeting has required classification markings and cover sheets are affixed to the front of the material to warn individuals of the classification level.

A9.3.11. (Added). Ensure AIS equipment used to process or project classified information is approved for classified use.

A9.3.12. (Added). Protect classified materials during any breaks, such as lunch periods, etc.

A9.3.13. (Added). Follow established procedures for protection and storage of classified material at all times. Maintain all electronic records in the approved electronic records management repository; this includes the classified repository on the SIPRNET.

A9.4. (Added). After the Meeting:

A9.4.1. (Added). Check area for unattended classified.

A9.4.2. (Added). Notify security authorities of all violations.

Attachment 10 (Added)

CONSTRUCTION GUIDELINES FOR SECURE CONFERENCE FACILITIES

A10.1. (Added). Objectives. To provide guidelines for the achievement of effective security in AFGSC facilities in which collateral classified information is discussed and handled on a daily basis. Normally, secure conference facilities are only set up at locations where daily classified conferences or forums occur. The guidance provided herein should be considered when building new facilities or renovating existing facilities.

A10.2. (Added). Secure Conference Facility. For the purpose of this instruction, a secure conference facility is defined as an area provided special acoustical, technical, and physical security protection, and designated for the discussion and handling of classified defense information on a continuous basis. Due to the high costs of building a secure conference facility, the number of secure conference facilities will be kept to the absolute minimum consistent with mission accomplishment.

A10.3. (Added.) General Approach. The achievement of adequate security for conference facilities so as to protect all classified information therein requires a blend of acoustical, technical, and physical security measures. This blend is obtained through the coordination of acoustical, electronics, civil engineering, and security personnel from the initial planning stage through construction and inspection phases. The installation Civil Engineer or Construction Agent is responsible for the design and construction of secure conference facilities. Qualified persons should be consulted for solutions to acoustical problems. The installation Civil Engineer, Construction Agent, or a qualified consultant should be able to help in the solution of acoustical problems. All elements comprising the physical boundaries of the facility must have a uniformly low transmission of sound through the exterior envelope (walls, ceiling, floor, and doors) of the secure space. No utilities should serve as a fortuitous probe to electronic or audio signals emanating from the secure facility. Physical access to the area must be controlled. Secure conference facilities will not be constructed adjacent to facilities not under U.S. control. After architectural plans are complete and before a contract is let, physical and technical security specialists will review the plans for potential security weaknesses. If uncleared personnel accomplish the construction, it is recommended that appropriately cleared owner/user personnel periodically check the facility, with particular emphasis on monitoring the installation of security items and to preclude the installation of clandestine surveillance devices.

A10.4. (Added). Acoustical Security. Acoustical security deals with all measures necessary to minimize the loss of intelligible information acoustically radiated within an area through proper construction techniques.

A10.4.1. (Added). Acoustical security treatment. The following facets of acoustical treatment are provided as a general guide to achieve adequate acoustical security:

A10.4.1.1. (Added). Doors & Frames. Commercially available doors acoustically rated with a proper Sound Transmission Class (STC) Laboratory rating shall be used. This rating should be 5 - 7 STC Points higher than the Noise Isolation Class (NIC) objective. One concept employs the use of a double door system. In this system two doors are mounted back-to-back with wider doorjambs used. This gives the added advantage of a relatively dead air space between the inner and outer area and overcomes the direct link from the outside to interior via the door hardware

assemblies, such as locks. Fire rated doors will not be used, as they cannot be made to meet the required STC rating. Lead sheets on the inner surface of both doors helps to increase the sound transmission loss. Any items of hardware installed on such doors should not in themselves create a sound leakage path. Doors are the weakest link in the system and because they have moving parts, they should be maintained on a scheduled basis. Doors must be acoustically tested biennially to ensure continuing compliance with required NIC standards.

A10.4.1.2. (Added). Doorjambs. Only factory supplied, acoustically rated STC doors that are delivered in factory-supplied doorframes and that have been STC rated, as a functional unit, shall be used. The doorframe shall be installed per manufacturer's instruction.

A10.4.1.3. (Added). Door thresholds. Wooden thresholds are preferred over metal because of their lower sound conductivity rating. All thresholds will be sealed at all points of contact with the floor and doorframe.

A10.4.1.4. (Added). Expansion joints. Conference facilities should not be located where building expansion joints will form a part of or be immediately against any portion of the facility perimeters. Such joints cannot be effectively soundproofed on a continuing basis, since the joints are always subject to gap changes resulting from ambient temperature variations or building movements.

A10.4.1.5. (Added). Holes or crevices. Holes or crevices in all exterior boundaries should be completely sealed with elastomeric caulking cement or equivalent mortar of such sufficiency as to prevent sound leakage and maintain the overall uniformity of sound transmission loss.

A10.4.1.6. (Added). Pipes, ducts, and conduits. Holes or crevices around pipes, ducts, and conduit passing into any part of the facility should be well sealed as discussed above. All pipes, ducts, or conduits, must contain a dielectric break (nonmetallic coupling) where passing through the perimeter wall, or be treated with structural masking. Those pipes remaining inside the facility, which are surface mounted, should be covered with an effective insulating material to attenuate the coupling of sound vibrations to the pipe (a possible transmission link from the facility). However, clean metal-to-metal contact is required where ducts or pipes pass through electrical shielding. Likewise, all service boxes connected to pipes and conduits should be covered. When necessary, a short length of pipe leaving a service box should be filled with fiberglass to attenuate airborne sound transmitted within the pipe.

A10.4.1.7. (Added). Metal beams or posts. The presence of metal beams and posts within the conference facility should be avoided wherever possible, since they both minimize the utility of a facility and require acoustical treatment in essentially the same manner as pipes and conduits mentioned above.

A10.4.1.8. (Added). Radiators. Hot water or steam radiators will not be installed, as they are difficult to make acoustically secure. The best heating system for security is an electrical heater within each room, since the electrical power circuits can be more easily made secure.

A10.4.1.9. (Added). Air conditioners. If possible, secure conference facilities should be equipped with an air conditioning system independent of the master building system. Master building systems, with all their air supply and return ducts, are more difficult to make secure. A dedicated air conditioning system should be installed in TOP SECRET areas. The background noise contribution of the heating, ventilation and air conditioning systems should not exceed 42 dB as measured inside the secure area.

A10.4.1.10. (Added). Air ducts and ventilation grills. Air ducts and ventilation grills create severe security problems in that they provide a ready path for the transmission of both airborne and structure-borne sound energy. All duct penetrations shall be fitted with commercially available duct silencers having a Dynamic Insertion Loss equal to the specified STC rating of the secure perimeter itself. The sides of the duct silencer shall have the same STC rating as the perimeter. A steel screen with ½ inch square mesh will be installed to preclude the introduction of a clandestine listening device. An approved duct silencer manufactured of non-sound conductive materials will be used to decouple duct sections where any part of air duct passes through an exterior boundary of the facility. As an alternative, the ducts may be treated with structural sound masking at the inside point of penetration.

A10.4.1.11. (Added). Sound system speakers. Speakers should be located as far as practicable from all air return inlets and, under no circumstances, mounted on perimeter surfaces. They should be mounted at a point where the sound transmission loss is the greatest (i.e., on a pillar) and likewise, the greatest levels of sound energy must be directed inward, away from any exterior walls. A sound level or volume-unit (VU) meter should be installed as part of the sound system to assure sound levels of 75dB or below are maintained to avoid nullifying the acoustical security treatment provided the area. Once the 75 dB is achieved, the volume control should be secured. Amplified sound shall utilize a well-distributed speaker system (such as speakers suspended from the ceiling) so that the sound pressure level does not exceed more than 75 dB at any place within the room (certain work areas may require a higher speaker dB).

A10.4.1.12. (Added). Communications devices. Telephones, intercoms, or any other communications devices that transmit clear text audio from an area should be kept to an absolute minimum, consistent with essential operational requirements. Each such device and its planned location should be considered carefully, for when in use they transmit from the area all conversations conducted within proximity of the device. No cell phones, camera cell phones, cordless telephones, or wireless microphones, keyboards, or mice, wireless or Infrared Local Area Networks (LANs), or devices are allowed in areas where classified information is discussed, briefed, or processed. ***"Area"*** refers to a room and/or to a space the size of a 3-meter radius sphere, centering on the classified source. In areas where classified information is discussed, briefed, or processed, wireless pointer/ mice devices are allowed for presentations only. All other wireless portable/personal electronic devices (PEDs) not specifically addressed above, that are used for storing, processing, and/or transmitting information shall not be operated in areas where classified information is electronically stored, processed, or transmitted. Classified information could unintentionally be transmitted from an area over unsecured communications systems because of poor planning. Care as to the quantity and location of communications devices, along with acoustical shells or booths about various work centers, can greatly reduce undesired sound transmissions via unsecured communication links. During planning stages, the use of secure communication devices must be considered, i.e. STU III, push to talk, etc.

A10.4.1.13. (Added). Alcoves or sound locks. A small room of suitable size can be provided at the main entrance door for both access control and the prevention of inadvertent overhearing whenever the outer door is opened. As an alternative measure, to identify visitors before opening a single door, either a closed circuit television system or a miniature, wide-angle optical lens (with a suitable hinged, lockable cover over the inside portion) may be installed in the entrance door.

A10.4.1.14. (Added). Windows. Windows will not be provided in new construction. When present in existing construction, windows will be removed or sealed and covered to provide an NIC rating equal to the surrounding wall area. Where windows must exist, venetian blinds and masking sound are required in the window area. Installation of man bars outside the windows should be considered. Completely eliminating the windows and replacing them with similar construction, as the surrounding wall is preferable. Where windows must exist, venetian blinds and flameproof heavy drapes (11 oz/sq yd or better) are encouraged to cover such windows inside the area.

A10.4.1.15. (Added). Ceilings, Walls, and Floors. True walls (structural floor to ceiling) will be installed in all new construction. For existing structures that do not meet the above requirement, a cap must be installed providing an NIC rating equal to the walls of the room. The presence of false ceilings, walls, and floors in new or old construction must be carefully compared against the total transmission loss afforded.

A10.4.1.16. (Added). Floor trenches. Service or utility trenches of any type under the floor should be filled, if possible, with concrete. If this cannot be done, masking sound is required.

A10.4.2. (Added). Sound Transmission Class: STC is a numerical rating system for laboratory determined transmission loss. In this rating system, acoustical security is determined solely by the attenuation (transmission loss) of airborne speech between the source and a potential listener outside the perimeter of the facility. The sound transmission loss (TL) of a partition is measured in 16 third-octave bands between 125 Hertz and 4000 Hertz, with each specific TL figure plotted in decibels on a graph. The resulting curve should be normalized against a standard curve, with the overall sound transmission loss expressed as a single figure value called STC (reference: ASTME E90, E-336, and E-413). The NICs provided in Table 1 are recommended minimums for secure conference facilities, depending on the level of classification discussed therein, the sound power level of speech within the area, and the ambient noise level in outside adjacent areas. Noise reduction tests in accordance with the ASTM E-413 in-to-out test procedures shall be performed after construction is completed and when modifications are made to the perimeter surface. The test data should be plotted per ASTM E-413 and expressed in a single number NIC. NIC is the same as STC except that an STC test is performed on partitions in an acoustical laboratory, and a NIC test is of a completed structure such as a finished secure facility. Thus, STC ratings are used to select the wall construction, doors, etc., and NIC is what you get when the facility is fully assembled. An ASTM E-336 test procedure shall be conducted on each wall, floor, ceiling, and perimeter door within the facility. The lowest NIC among the test points shall be that of the entire facility. Because ambient noise outside an area is a variable, i.e., day vs. night, duty hours vs. nonduty hours, etc, it may be necessary to employ sound masking techniques. Such units consist of electronically controlled noise systems or vibration transmitters installed within the perimeter. The employment of such noise generators in wall voids, doors, windows, and overhead ducts is a more economical technique to achieve acceptable transmission losses.

A10.5. (Added). Technical Security. Technical security encompasses those measures necessary to deny the use of existing technical equipment that may have compromising emanations or the installation of clandestine technical surveillance devices to collect intelligence from within an area. The servicing communications activity and Office of Special Investigations should be contacted for guidance regarding technical security issues during the initial planning stages of the secure facility. Some guidelines for technical security treatment are as follows:

A10.5.1. (Added). Electrical services. All electrical wiring should, if at all possible, be run from a common distribution panel located within the secure discussion area. A single feeder circuit entering the area should service the panel. Radio frequency filters should be included if any equipment is located within the secure conference facility that may have possible compromising emanations. Final determinations of the requirement (or lack thereof) for filters will be made by the Air Force Network Integration Center Certified Technical TEMPEST Authority (AFNIC/CTTA).

A10.5.2. (Added). Communication services. All wires or cables that transmit information to or from a secure conference facility should be routed to a common distribution frame from which a single multi-pair cable leaves the area. All obsolete wires should be removed. Unused wires required for future expansion should be electrically grounded at the distribution frame within the secure area. All communications systems installed should be the minimum necessary consistent with essential and efficient operations. All voice systems, incoming or outgoing, secure or unsecured, should be designed such that when not in use (turned "on") they do not transmit clear text conversation from the area. Line disconnect jacks on outgoing circuits and isolation amplifiers on incoming circuits are an effective means to render such systems secure when not in use. Radio frequency filters should be included if any equipment is located within the secure conference facility that may have possible compromising emanations.

A10.5.3. (Added). Telephones. All telephones should be equipped with an automatic disconnect device or a manual plug-type disconnect to disconnect the telephone from the outgoing line. When disconnects are employed nonresonant external ringers are required. See paragraph A10.4.1.12. (Added) above for further guidance.

A10.5.4. (Added). Shielding. If equipment that unintentionally radiates clear text intelligence is used in a secure conference facility to process classified information, consideration must be given to Radio Frequency (RF) shielding the equipment or the facility to contain the compromising emanations. Although technical security surveys do provide a determination if any clandestine technical surveillance devices were or currently are in place, they do not provide protection against future installations or unwitting carriers unless very stringent physical security and access controls are in effect. One countermeasure, which commanders may consider to combat clandestine RF transmitters, is the utilization of RF shielding about sensitive conference sites.

A10.6. (Added). Physical Security: Physical security encompasses those measures necessary to deny the physical access of unauthorized personnel to a designated area. Physical security can be achieved through the employment of physical barriers, locking devices, and IDS, or combinations thereof. Some physical security guidelines that can be followed for normal threat environments are as follows:

A10.6.1. (Added). Facility Structure. The floor, walls, and roof must be of permanent construction materials offering resistance to, and evidence of unauthorized entry into the area. Walls shall be extended to the true ceiling and attached with permanent construction materials. Windows should not be installed in new secure conference facility construction. Follow the guidance in paragraph A10.4.1.14. (Added) above for windows in existing construction. Clean, straightforward construction techniques should be employed. Whenever possible, all utility pipes, conduits, and related components should be run exposed on interior wall or ceiling surfaces to minimize exploitation, while facilitating their periodic examination. Likewise, access ports or doors should be provided to permit the periodic examination within concealed areas, i.e.,

above false ceilings, under stages, etc. In general, the secure conference facility should be kept orderly, with only furniture necessary to minimize concealment locations.

A10.6.2. (Added). Locking Devices. Entrances to the secure conference facility should be kept to an absolute minimum commiserate with local fire and safety codes. Doors will be substantially constructed of wood or metal. Doors will be equipped with a locking mechanism to prevent unauthorized entry into the facility when not in use. Built-in, manipulation-proof, three position combination locks with an interior safety release turn knob that conforms to GSA Federal Specifications, FF-L-2740, will be used on entry doors to provide maximum security. Panic hardware will be installed on the inner side of all emergency doors. Emergency doors will not have any hardware on the outside of the doors.

A10.6.3. (Added). Door hinges. Door hinges should be installed to deny access to the pivot pin, as its removal often makes an otherwise very secure door highly susceptible to being opened. If the hinge pin must be exposed, then it should be fixed to preclude its removal or the door additionally secured on the hinge side from within.

A10.6.4. (Added). Openings. All openings large enough to permit a person to gain unauthorized access into an area, 96 square inches or greater, should be appropriately sealed. Either physical security bars or complete and permanent blockage of the opening is desirable. Special care is necessary to ensure all utility areas such as steam tunnels, air ducts, air shafts, utility shafts, are secure, as is the area above a false ceiling. All windows and other openings which exist in boundary surfaces of a secure conference facility and which adjoin areas of lesser security must be covered or sealed to deny optical and audio surveillance of classified information therein. Optical surveillance techniques include the unaided and aided human eye (binoculars, etc,), photographic and TV cameras, infrared scanners, etc. Audio surveillance techniques include lip reading, infrared pick-off devices, etc. Protective coverings over all openings should include glass opaque to infrared or ultraviolet band energy, venetian blinds, and flameproof heavy drapes (11 oz/sq yd or heavier).

A10.6.5. (Added). Intrusion Detection Alarm System (IDS). The inclusion of IDS is only recommended when the local threat and security environment dictates more stringent security requirements to prevent the installation of clandestine technical surveillance devices. The system should include volume, perimeter, and point sensors. Proximity and motion detectors provide protection for unique problems. All intrusion alarm systems should include electrical line supervision between the protected area and monitoring location. Further, all systems should be capable of sustaining normal operation for 24 hours after a commercial power loss. All sensors employed must detect an intrusion and be immune to normal bypass techniques. When used, all intrusion detection alarm systems should be of the type, and so installed, that they do not transmit intelligence from an area.

A10.7. (Added). Masking Sound Applied to Speech Security. In order to make it impossible to understand speech outside the secure area, the system design goal must be to reduce speech intelligibility in all situations, whether it is the result of human listening or listening with detection devices. Technically, the purpose of masking sound is to reduce the signal-to-noise ratio of a sound to zero at all pertinent frequencies. In this context, the signal is the speech and the noise is the masking sound. When the speech intelligibility is zero, the privacy is total and the signal to noise ratio is zero. This is adequate for direct human listening, but when detection devices are used and signal-processing techniques are used on the derived signal, it is possible to improve the signal-to-noise ratio and recover meaning. To keep speech intelligibility at zero, the

masking should be amenable to signal processing techniques that could reduce its effectiveness. This can be done with a masking signal that is the result of a stationary random process. The masking signal becomes not only unknowable but cannot be processed with statistical techniques. Standard masking generators are digital using components in which the signal repeats itself after one minute. They are called pseudo random controlled noise generators. The sound created by them may appear random to the listener, but is in fact a deterministic process. Sophisticated techniques can make use of this deterministic property to increase the speech intelligibility and thus recover speech. Analog masking generators are somewhat better in that they create a truly random signal, but suffer from the fact that the signal is Gaussian and stationary, statistical properties that make signal processing easier. This aspect of the problem is handled in the equipment generating the masking sound. The most effective method for structural masking is when random signal vibrations are introduced directly to the perimeter barrier surface to control background sound levels at potential listening points. The sound masking system and all wires and transducers shall be located within the perimeter of the facility. Speakers can be located outside the facility and directed outward as close as practicable to the facility's perimeter where the sound transmission loss is the greatest (i.e. doors, windows, HVAC ducts, electrical and plumbing conduit, etc.) to achieve the required/desired STC rating. The sound masking system should only be utilized when the required/desired STC rating is not achievable through physical security means.

Table A10.1 (Added) Noise Isolation Class (NIC)

R U L E	Area Approved For Discussion of:	If Area Has:	
		Normal Speech	Amplified Speech
1	SECRET	45	50
2	TOP SECRET	50	55

Attachment 11 (Added)

Security Incident Preliminary Inquiry Official Briefing

Figure 11.1 Security Incident Preliminary Inquiry Official Briefing

Note: This briefing will be used in its entirety to brief security incident preliminary inquiry officials. IP Offices may add point of contact information, but will not modify the content of the briefing.

A11.1. (Added). References.
A11.1.1. (Added). Executive Order 12958, as amended, Classified National Security Information, Section 5.5
A11.1.2. (Added). DoD 5200.1-R, Information Security Program, Chapter 10
A11.1.3. (Added). AFI 31-401, Information Security Program Management, Chapter 9
A11.1.4. (Added). AFI 31-401, AFGSC SUP1, Information Security Program Management, Chapter 9
A11.2. (Added). Policy. It is Air Force policy that security incidents will be thoroughly investigated to minimize any possible damage to national security. The investigation will identify appropriate corrective actions that will be immediately implemented to prevent future security incidents. Further, if the security incident leads to the actual or potential compromise of classified information, a damage assessment will be conducted to judge the effect that the compromise has on national security.
A11.3. (Added). Definitions:
A11.3.1. (Added). Security Incident – any security violation or infraction as defined in EO 12958, as amended.
A11.3.2. (Added). Security Violation – any knowing, willful, or negligent action: 1) that could reasonably be expected to result in an unauthorized disclosure of classified information, 2) to classify or continue the classification of information contrary to the requirements of EO 12958, as amended, or its implementing directives, 3) to create or continue a special access program (SAP) contrary to the requirements of EO 12958, as amended.
A11.3.3. (Added). Security Infraction – any knowing, willful, or negligent action contrary to the requirements of EO 12958, as amended, that is not a security violation.
A11.3.4. (Added). Compromise – occurs when unauthorized individuals have had access to classified information. Unauthorized individuals include those individuals with the appropriate security clearance but do not have a need-to-know.
A11.3.5. (Added). Potential Compromise – a compromise of classified information has more than likely occurred as a result of a security incident.
A11.3.6. (Added). Access – the ability or opportunity to gain knowledge of classified information.
A11.4. (Added). Inquiry Official Procedures:
A11.4.1. (Added). The inquiry official (IO) is appointed in writing by the commander/staff agency chief/director of the unit responsible for the security incident. The IO must be an impartial individual, meaning the person(s) suspected of causing the incident shall not be in the IO's chain of command. As a minimum, the IO will be a commissioned officer, senior NCO, or GS-9/Pay Band 2 or higher, and will be of equal or greater rank than the subject(s) of the inquiry. The unit security manager may not be appointed as the IO as their actions may be scrutinized during the inquiry. Contractors may not be appointed as inquiry officials. If, at any time during the inquiry, the IO determines the unit commander or anyone else in his/her chain of command is involved in the incident, immediately cease the inquiry and notify the Information Protection (IP) office. The IP office will elevate the incident to the next level of command for a new IO appointment.
A11.4.2. (Added). The scope of this inquiry is to determine the facts of the security incident, and to make recommendations to the appointing official. The information involved in this incident is collateral classified information. If, at any time during the inquiry, the IO determines

the incident involves non-collateral (SCI, SAP or COMSEC) information, immediately cease the inquiry and notify the IP office. The IP office will notify the proper authorities.

A11.4.3. (Added). The IO may contact the IP office and/or the legal office at any time during the inquiry for guidance. Both offices may answer the IO's technical questions, but they are not permitted to lead the IO to a conclusion of any kind.

A11.4.4. (Added). The IO will interview all personnel involved with the incident, regardless of physical location. The IO will also interview personnel lending expertise to the incident, such as the Information Assurance Officer (IAO), the Foreign Disclosure Officer, the unit security manager, etc., depending on the circumstances of the incident. For security incidents involving the network, the IO will collect records of all fact-finding interviews conducted by the IAO or network control center. If the fact-finding interviews sufficiently answer the IO's questions, the IO does not need to obtain additional information from the same individuals interviewed during the fact-finding.

A11.4.5. (Added). If, during the inquiry, the IO determines the incident circumstances may have involved criminal activity or foreign intelligence agencies, temporarily suspend the inquiry and immediately notify the IP office. The IP office will, with IO assistance, immediately coordinate with AFOSI to determine what further actions will be taken.

A11.4.6. (Added). Rights Advisements. During a security incident inquiry or investigation, a rights advisement for subjects, suspects or witnesses may become an issue.

A11.4.6.1. (Added). Military. The mere fact that someone is the subject of an inquiry does not automatically trigger the need for a rights advisement. The test is whether the IO, at the time the active duty military subject is interviewed, either believes or reasonably should believe the individual committed an offense under the UCMJ or other criminal code. If so, then the subject or witness should be considered a *suspect*. In these cases, temporarily suspend the inquiry and immediately consult with the servicing legal and AFOSI offices to determine what further actions will be taken. Cases involving Guard and Reserve personnel are further complicated by their status at the time of the alleged conduct and the time of the interview. Consult with the legal advisor in these cases.

A11.4.6.2. (Added). Civilian. Even if suspected of an offense, a civilian witness or subject need not be advised of their Fifth Amendment ("Miranda") rights when interviewed as part of an inquiry. Such rights are only required in conjunction with *custodial* interrogations (i.e., interrogations in which the interviewee is not free to leave at will). Security inquiry interviews do not meet the threshold requirement for a custodial interrogation. The lack of a requirement to advise civilian witnesses of their Fifth Amendment rights does not preclude them from invoking such rights and choosing to remain silent if circumstances warrant.

A11.4.7. (Added). Third-Party Presence During Interviews. An interview will normally only involve the IO and the witness. Sometimes a technical advisor or administrative assistant appointed to assist the IO will accompany the IO during interviews. For example, while interviewing witnesses of the opposite sex, the IO may want an assistant present to avoid any appearance of impropriety. Additionally, if the testimony of a particular witness is especially important to the investigation, the IO may want a third party present to take notes and act as a witness to what is said. Although the IO can have team members present during witness interviews, generally speaking witnesses cannot have third parties present. This section discusses how to proceed when a witness requests that a third party be present during their interview.

A11.4.8. (Added). Labor Union Representatives. Civilian subjects or witnesses who are

members of collective bargaining units, and their labor unions, have specific rights with regard to labor organization presence during interviews. Employees have the right, during an *investigatory interview* conducted by a representative of the Air Force, where the employee reasonably believes discipline may occur as a result, to request the presence of a representative from the labor organization that represents the bargaining unit to which the employee belongs ("Weingarten" rights). To exercise this right, the employee must request representation. *There is no duty for the IO to advise the employee of this right.* When this right is invoked, the IO may wait until a representative from the labor organization arrives or inform the witness that if a representative is desired, no interview will take place, and the case will proceed without any input from the witness. The representative is a *personal representative* of the employee and may provide advice, consult with the witness, and suggest areas of inquiry, but may not obstruct the interview or instruct the witness not to answer legitimate questions. The situation can occur where both the rights of a labor organization and the rights of an employee arise and could result in two representatives from the labor organization. The Civilian Personnel Office and JAG legal advisor can help the IO navigate the unique labor law issues present at each base.

A11.4.9. (Added). Chief of Staff Hand-Off Policy. The CSAF's 26 November 2002 Policy for Investigative Interviews applies to security incident inquiries and investigations. This policy requires a person-to-person hand-off of all subjects and suspects, and any distraught witnesses following an investigative interview. The hand-off must take place between the IO and the individual's commander or the commander's designated representative. The policy applies to everyone, regardless of rank or position. See AFI 901-301, para 2.46.

A11.5. (Added). Inquiry Report. The IO will gather all facts surrounding the incident and will detail the findings in an inquiry report.

A11.5.1. (Added). Specifically, the IO will address the following questions:

A11.5.1.1. (Added). Who? Who was involved in the incident? Who may have come into direct or indirect contact with the information?

A11.5.1.2. (Added). What? What information was involved in the incident? Identify the information, in an unclassified format, by subject and original classification authority (OCA), if known, that was involved in the incident. What specific equipment, if any, was involved? For incidents involving the network, obtain the incident number from the IAO or network control center (NOTE: this is a different number than the one assigned by the IP office). Include this number in the body of the report.

A11.5.1.3. (Added). When? When did the incident occur? Develop a timeline that covers the entire timeframe, from the occurrence of the incident through discovery of the incident and proper protection of the information.

A11.5.1.4. (Added). Where? Where did the incident occur?

A11.5.1.5. (Added). Why? How did the incident occur? What situations or conditions caused or contributed to the incident? The IO must determine the root cause of the incident.

A11.5.2. (Added). There is usually no need to include classified information in the report. However, if it does become necessary to include classified information, if possible, include the classified portion in an attachment that can be separated from the rest of the report. If classified information is in an unsecured environment (for example, a press article), the inquiry report must be classified at the same level as the information compromised if it contains sufficient information that would enable unauthorized individuals to access the classified information in an unsecured environment. All unclassified reports will be marked as "For Official Use Only."

A11.5.3. (Added). In addition to detailing the facts and drawing conclusions based on the facts,

the IO will make recommendations to the appointing official. If there is an environment present within the organization that could lead to a similar incident reoccurring, the IO must make recommendations on how to correct the situation. If there are weaknesses in security policy or security classification guidance, recommended corrective actions will be identified in this portion of the report.

A11.5.4. (Added). The IO will also make an incident closure recommendation to the appointing official. Closure options are: 1) Security violation; 2) Security infraction; or 3) Unfounded (only used when the determination is no classified information was involved in the incident). The IO will also indicate: 1) a compromise occurred (will always be categorized as a violation); 2) a potential compromise occurred; or 3) no compromise occurred.

A11.6. (Added). Inquiry Report Coordination Procedures.

A11.6.1. (Added). Once the IO has completed the inquiry report, the report and all attachments will be submitted to the ISPM. The IO will not submit the inquiry report to the appointing official or anyone else in the unit for coordination/review prior to the report being submitted to the ISPM.

A11.6.2. (Added). The ISPM will perform a technical review to ensure all aspects of the incident have been addressed. If questions remain unanswered, the report will be returned to the IO for correction. Once all questions have been satisfactorily addressed, the ISPM will either concur or non-concur, in whole or in part, with the IO's recommendations and conclusions.

A11.6.4. (Added). Once the technical review is accomplished, the inquiry report will be forwarded to the appointing official for closure. The appointing official may concur or non-concur, in whole or in part, with the IO's and ISPM's recommendations and conclusions. The preliminary inquiry is sufficient to resolve the security incident if: 1) the inquiry determines that loss or compromise of classified information has not occurred; 2) the inquiry determines that loss or compromise of classified information has occurred, but there is no indication of significant security weakness; or 3) the appointing official determines that no additional information will be obtained by conducting a formal investigation.

A11.6.5. (Added). The inquiry report with all attachments will be forwarded back to the IP office. The IP office will maintain all documentation on file for two years.

A11.7. (Added). Formal Investigation. If the appointing official determines the preliminary inquiry is not sufficient to resolve the security incident, he/she will initiate a formal investigation. This does not relieve the IO from conducting the preliminary inquiry to the best of their ability. If the IO cannot answer a particular question(s) during the inquiry, he/she must indicate in the preliminary inquiry report what actions were taken to answer the question(s) and why attempts to answer the question(s) were unsuccessful. This enables the appointing official to make an informed decision when determining whether a formal investigation is necessary.

PRELIMINARY INQUIRY REPORT FORMAT
(Extracted from AFI 31-401, Attachment 6)
Unit Letterhead

MEMORANDUM FOR (APPOINTING AUTHORITY)

FROM: (Inquiry Official)

SUBJECT: Preliminary Inquiry of Security Incident No. XX

1. AUTHORITY: A preliminary inquiry was conducted on (dates) 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 Program Management, paragraph 9.5 for security classification requirements.
3. PERSONNEL INTERVIEWED: (List all personnel interviewed, position title, office symbol, and security clearance).
4. FACTS: (List specific details answering who, what, why, where, and when questions concerning the incident).
5. CONCLUSIONS: As a result of the inquiry 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.
6. RECOMMENDATIONS: (list corrective actions needed to preclude a similar incident; the category of the incident; damage assessment; if the incident is a compromise, potential compromise or no compromise; and if this inquiry should be closed without further investigation or with a recommendation for a formal investigation).

SIGNATURE BLOCK
Master Sergeant, USAF
NCOIC Operations

Attachments:
1. Appointment of Inquiry Official Memo, (date)
2. Witness Statements