

**BY ORDER OF
THE COMMANDANT**

**AIR FORCE INSTITUTE OF TECHNOLOGY
INSTRUCTION 31-101**

17 DECEMBER 2001

Security

INFORMATION SECURITY



COMPLIANCE WITH THIS PUBLICATION IS MANADATORY

NOTICE: This publication is available digitally on the Air Force Institute of Technology, Information Management Branch, web site at: http://sc.afit.edu/support/SCBI/afit_publications.htm. If you lack access, contact your Publications Management office.

OPR: AFIT/MSPS (Mr Roy LeBlanc)
Supersedes AFITI 31-101, 01 September 2000

Certified by: AFIT/CC (Col Michael L. Heil)
Pages: 22
Distribution: F;X

This instruction is affected by the Privacy Act of 1974.

This instruction provides guidance and outlines policies and responsibilities for all AFIT faculty, staff, and resident students. It is not, nor is it intended to be, all-inclusive. The procedures as outlined reflect in some cases minimum requirements of applicable DOD and Air Force instructions. They must be complied with to ensure AFIT maintains a viable and continuing information security program. This instruction establishes policies and procedures to safeguard such information and provides for oversight enforcement. It applies to all personnel assigned to AFIT.

SUMMARY OF REVISIONS

This instruction has been revised to include responsibilities for safeguarding classified holding in the event of a disaster and changes to the duties of the Office Security Monitors within AFIT.

- 1. Authority.** DOD 5200.1-R/AFI 31-401, Managing the Information Security Program.
- 2. Purpose.** The purpose of this instruction is to implement the DoD Information Security Program as applicable to AFIT.
- 3. General.** All personnel (faculty, staff, and students) whose positions require access to classified information must possess the required security clearance; complete an SF 312, Classified Information Nondisclosure Agreement; and have a need to know.
- 4. Responsibilities.**

4.1. Commandant:

4.1.1. Ensures implementation of the overall security program.

4.1.2. In writing, appoints a primary and an alternate security manager to monitor and implement the program.

4.2. The security manager (SM) is delegated the authority to establish and monitor the security policies and procedures necessary to assure the safeguarding of classified information. The SM will:

4.2.1. Provide an original ASC Form 2413, Appointment of Security Manager, to 88 SFS/SFA, and file a copy of the form in the Security Manager's Handbook.

4.2.2. Develop the unit's annual security training plan as outlined in AFI 31-401/AFMCS.

4.2.3. Attend 88 SFS/SFA quarterly SM meetings.

4.2.4. Monitor the accomplishment of the semiannual security inspections due in each sixth month after a program review conducted by 88 SFS/SFA and, when needed, ensure corrective actions are completed.

4.2.5. Provide information security assistance to management, supervisors, and all unit personnel.

4.2.6. Ensure newly assigned personnel are indoctrinated on security procedures and individual responsibilities.

4.2.7. Ensure briefing/debriefing requirements are met and that the appropriate forms are completed and retained.

4.2.8. Ensure classified material is reviewed periodically and destroyed as soon as it serves its purpose.

4.2.9. Ensure classified material is retrieved and properly stored within the WPAFB area in the event of a disaster. Once material is retrieved, SM needs to contact WPAFB Command Center to arrange for storage and transportation needs.

4.2.10. Prepare and submit reports required by higher headquarters and those deemed necessary locally.

4.2.11. Monitor the AFIT Personnel Security Program.

4.2.12. Act as the focal point for foreign travel briefings/debriefings and maintain the records associated with such travel.

4.2.13. Incorporate the awareness of and training in other security related programs, specifically the Operations Security (OPSEC) and the Antiterrorism Program, into the overall security program.

4.2.13. Ensure this instruction is current and that it is updated as dictated by changes in policies, procedures, and guidance.

4.2.15. Provide training to office security monitors (OSMs).

4.3. Deans/Directors:

4.3.1. In writing, appoint an OSM and an alternate OSM to the SM.

4.3.2. In writing, appoint a primary and alternate classified custodian to the SM for all classified material stored within the unit, if applicable.

4.3.3. Ensure employees comply with all security training requirements as directed by the SM.

4.3.4. Review sensitivity assigned to a position whenever it becomes vacant, when changes in duties occur, or periodically to ensure adequacy and accuracy of security access requirement.

4.3.5. Include security duties in the civilian position descriptions by addendum and evaluate performance of the duties on the Civilian Performance and Promotion Appraisal (AF Form 860). For military, evaluate security duties in performance appraisals. Further, ensure performance appraisals/reports adequately reflect the degree to which the individual discharges the responsibilities associated with these duties.

4.3.6. Ensure all personnel, military and civilian, terminating Air Force employment is referred to the SM for debriefing.

4.3.7. For schools only. For all courses that include classified briefings, ensure a copy of the Classified Briefing Guidelines (**Attachment 1**) is posted in the course notebook and that it is referred to prior to classified briefings and presentations.

4.4. Office Security Monitors (OSM). The OSM serves as the unit's focal point on all matters pertaining to the protection of classified material including, but not limited to:

4.4.1. Ensuring all personnel in the unit are aware of requirements to complete applicable security education.

4.4.2. Participating in promoting the unit's OPSEC Program and other security-related subjects.

4.4.3. Ensuring all personnel in the unit are aware of requirements to complete applicable security education.

- 4.4.4. Performing semiannual cross inspections of unit's security program.
 - 4.4.5. Serving as a destruction official.
 - 4.4.6. Monitoring completion of local semiannual security inspections as assigned.
 - 4.4.7. Provide assistance to the SM in developing and implementing the organization's security program.
- 4.5. Supervisors/Faculty Advisors. Supervisors/faculty advisors of students scheduled to take classified courses, or who plan to conduct classified research, are responsible for providing security indoctrination to the students prior to the course/research starting. See paragraph 5.4.9. and **Attachment 4**.
- 4.6. All personnel will:
- 4.6.1. Protect classified information in his or her custody or which is found not properly protected.
 - 4.6.2. Report any discovery of classified information not properly controlled or protected to the security manager, immediate supervisor, unit chief, or higher authority. Protect the classified information until it is conveyed to the appropriate custodian.
 - 4.6.3. Know their level of security clearance and any approved special-access authorization.
 - 4.6.4. Be alert to the presence or absence of classified information in the work area.
 - 4.6.5. Challenge strangers in the work area, find out who they are, and what business they have there.
 - 4.6.6. DO NOT discuss classified information in the work area without taking precautions to ensure unauthorized personnel cannot overhear the conversation.
 - 4.6.7. DO NOT discuss classified information over a non-secure telephone or in a room where someone is using the telephone.
 - 4.6.8. Become familiar with the requirements for verifying an individual's security clearance and establishing need-to-know before allowing the individual to access classified material.

5. Procedures.

5.1. Classification:

- 5.1.1. Original classification authority (OCA) is not authorized at this activity. A classification evaluation is obtained through higher headquarter channels when local personnel develop

information believed to need safeguarding. The local developer will prepare, protect, and submit the information to the SM for processing according to guidance provided in AFI 31-401.

5.1.2. Derivative classification is used whenever previously classified information is incorporated, paraphrased, restated, or generated in new form into locally prepared documents. On the first page of the new document, the preparer will record the overall classification from the original document; enter the title of the source document and its date on the "Classified by" line; enter the downgrading and declassification information from the source document on the respective "Downgrade on" and "Declassify on" lines on the new document; and carry over any additional warning notices assigned to the source document.

5.2. All personnel will mark classified documents according to regulatory guidance provided in DOD 5200.1-R. Use DOD 5200.1-PH, Guide to Marking Classified Documents, which shows examples of how to apply required markings to classified correspondence, illustrations, transparencies and slides, microforms, and other special categories of material.

5.3. Transmission, Receipt and Control:

5.3.1. Only cleared personnel will deliver, transmit, or receive classified messages and accountable mail. Personnel authorized to perform these duties will also comply with applicable telecommunications and mail regulations.

5.3.1.1. Authority notification is provided and updated as prescribed by AFIT/SCBI, Information Management Branch.

5.3.1.2. AF Form 12, Accountable Container Receipt, signed by cleared personnel, will accompany the transfer of accountable mail.

5.3.1.3. The sender of outgoing accountable mail will ensure classified documents are properly wrapped, addressed, and contain appropriate receipts. The sender will prepare receipts, obtain a container number from SM, and will comply with all transmission requirements in AFI 31-401. SM will establish and maintain a document receipt file and perform tracer actions, when necessary.

5.3.1.4. SM will sign any document receipt that may accompany incoming classified material and will promptly return the receipt to the originator.

5.3.1.5. AFIT/SCBI, Mail Room, will ensure all unopened First Class mail with the endorsement "Return Service Requested" recorded on the outer envelope is handled as if the contents are classified at the CONFIDENTIAL level. All such mail not picked up by the end of the workday will be secured in the AFIT/SCBI safe.

5.3.2. Appropriately cleared individuals who are authorized to escort or handcarry classified will comply with the procedures in AFI 31-401.

5.3.2.1. A letter or DD Form 2501, Courier Authorization, is issued as written authorization for handcarrying classified locally and within a ten-mile radius of the base. The SM retains the authorization. Personnel must contact the SM for guidance prior to performing handcarrying duties.

5.3.2.2. Classified material is properly packaged for transportation according to AFI 31-401.

5.3.2.3. SM briefs individuals designated to handcarry on their responsibilities for protecting the classified material while in transit. They will acknowledge receipt of the briefing and the understanding of their responsibilities by signing the DD Form 2501 or form letter, as appropriate.

5.4. Safeguarding Classified Material.

5.4.1. Department/Division Heads and above may authorize reproduction of classified information on which reproduction limitations are not established. The approving official will sign and date the back of the file copy to document approval. When necessary to reproduce classified information, use the copier located in Building 640, Room 230A, and follow the instructions on AFVA 205-9, Classified Reproduction Authorized, posted at the machine.

5.4.2. The individual is solely responsible for the protection of classified material in his/her possession. Never leave it unattended. Avoid giving it to another person to hold; however, when unavoidable, verify the person has the appropriate clearance and the need to know. Never place classified in a desk drawer, bookcase, or file basket. Use the appropriate cover sheet when classified material is outside the container. Return classified material to the security containers when leaving for lunch, emergency situations, at the end of the workday, or whenever the user must leave the work area. In the event of a natural disaster, (fire, tornado, or flood) ensure classified material is placed in security container before departing. Removal of classified material during non-duty hours is prohibited.

5.4.3. Individuals listed on the SF 700, Security Container Information, are responsible for opening and closing security containers. The form is posted inside each locking drawer. Whether the container is or is not opened during the workday, the designated end-of-day security checker will ensure it is locked. Enter the date, time, and initials in the appropriate column on SF 702, Security Container Check Sheet, to document the check

5.4.4. At the end of each workday, all rooms containing a security container will ensure a thorough area security-check is performed by cleared personnel. Department/Division Heads will delegate area security check duties in writing. **Attachment 3** to this instruction is used as a guide for such delegations. After performing the area and security-container check, the individual annotates the SF 701, Activity Security Checklist.

5.4.5. Prior to the release of any classified material, custodians will ensure the individual has a security clearance equal to or above the level of the information being released and that the individual has the "need to know" to perform assigned duties.

5.4.6. Custodians will request maintenance on vault and secure-room doors from civil engineering every 2 years; safes from base locksmith every 5 years. The custodian will ensure personnel who service the security container are not permitted access to the classified contents. In case of malfunction of the security equipment, contact the base locksmith immediately, and remain with the equipment. If it is unlocked, remain until it is repaired or material is removed to another container. The custodian will also ensure that maintenance and/or repair are posted on the AFTO Form 36, Maintenance Record for Security Type Equipment.

5.4.7. The custodian will ensure that safe combinations are changed when persons having access to the container terminate Air Force employment or when access is withdrawn for any reason (i.e., PCS, PCA, security clearance withdrawn, etc.). The custodian will change the combination.

5.4.8. The discoverer of a security violation will immediately report the finding to the SM, immediate supervisor, or higher authority. The SM will report all incidents to 88 SFS/SFA and ensure an investigative inquiry is initiated IAW AFI 31-401.

5.4.9. Students scheduled to take classified courses or who plan to conduct classified research will receive security indoctrination by their supervisor/faculty advisor prior to starting the course or research. As a minimum, students will be briefed on proper handling, storage, marking, reproducing, and safeguarding all classified notes, drafts, reports, texts, and other related materials. The supervisor/faculty advisor and student will complete and sign the Classified Thesis/Research Briefing (**Attachment 4**) and forward a copy to the SM for filing.

5.4.10. The SM will provide liaison with AFRL/STINFO for protection of, and access to, AFIT classified material stored in Building 640, Room 67. The SM will provide access letters to AFRL/STINFO for all AFIT personnel requiring access. The SM will ensure all personnel have a valid security clearance of SECRET or higher, a completed Standard Form 312 on file, and the need to know.

5.4.10.1. Faculty, other than classified custodians, requiring access to AFIT classified material stored within AFRL/STINFO will provide a written request for access from their Department/Division Head to the SM (**Attachment 5**).

5.4.10.2. Supervisors/faculty advisors of students who are conducting classified research and require access to AFIT classified material stored within AFRL/STINFO will provide a written request to the SM for access (**Attachment 6**).

5.4.10.3. Access will be granted to AFRL/STINFO only during normal duty hours. An attempt should be made not to remove classified material from AFRL/STINFO. A working area is available within AFRL/STINFO to conduct classified study/review/research. If classified material is required to be removed from AFRL/STINFO, an AF Form 614, Charge-Out Record, will be filled out and filed in place of the removed classified document/material. The remover will ensure the classified material has a classified cover sheet (SF 704/705, as appropriate) attached, is always within their control, and will return the material to its original location in AFRL/STINFO no later than 1530 hours the same day.

5.5. Review and Destruction of Classified Material.

5.5.1. Classified custodians will, at least annually, review their classified material for downgrading, declassification, and destruction. Custodians will observe the annual clean-out day on the second Friday in March of every year.

5.5.2. Personnel destroying classified material will place the material identified for destruction in "burn bags" and destroy it at the central destruction facility, incinerator in Bldg 305. Destruction officials will arrange use of destruction facility through the SM. At least two appropriately cleared destruction officials will prepare material for destruction, transport the material to the destruction facility, place the material in the incinerator, and remain at the facility until they are sure the material is destroyed. Using an approved shredder, if the quantity of material to be destroyed doesn't justify the use of the central destruction facility, may destroy classified material. At least two appropriately cleared destruction officials must be present when shredding SECRET material. One destruction official is required to shred CONFIDENTIAL material.

5.6. Semiannual Security Inspections (SSIs).

5.6.1. In writing, the squadron section commander will appoint OSMs to conduct cross inspections within AFIT.

5.6.2. The OSMs will contact the SM for a briefing on conducting the inspection. The SM will provide the OSMs with the SSI checklist. The OSMs will submit a written report to the squadron section commander not later than 5 workdays after the end of the inspection month.

5.6.3. The squadron section commander will review the report; approve it by written indorsement; direct corrective action, if needed; and send the entire inspection package to the SM. The SM will forward a copy of the report to 88 SFS/SFA.

5.6.4. The SM will monitor inspections to ensure timeliness of their completion and files the inspection reports with documentation of the command review/approval and documentation of completed corrective actions.

5.7. Security Manager's Meetings.

5.7.1. The primary and/or alternate SM will attend the quarterly meetings conducted by 88 SFS/SFA. The SM will use minutes of the meetings to conduct internal meetings and to assist with the unit's security education program. The SM maintains the minutes from the last four (4) meetings in the Security Manager's Handbook.

5.7.2. The unit SM will meet with the OSMs on as-needed basis, prepare and distribute minutes from those meetings, and maintain the minutes of the meetings in the Security Manager's Handbook.

5.7.3. OSM attendance at meetings held by the SM is mandatory. The OSMs will disseminate pertinent information from the meetings to all personnel within their respective offices.

5.8. Security Education.

5.8.1. Within 90 days of assignment and quarterly thereafter, personnel will receive appropriate security training/education as required by AFI 31-401. Supervisors will ensure training is accomplished; and, when required, will record completed training. See paragraph 4.5. and 5.8.3. of this instruction.

5.8.2. In accordance with AFI 31-401/AFMCS 1, the AFIT Annual Security Training Plan is included in **Attachment 2**.

5.8.3. Due to the uniqueness of AFIT and difficulty of ensuring all AFIT personnel attend quarterly security education briefings in person, the SM will provide quarterly training to AFIT personnel via email. All AFIT personnel are mandated to read the quarterly security education training email sent from the SM.

5.9. Classified Briefings/Meetings. The project officer/sponsor for the classified briefing/meeting will ensure that all security requirements are met. The SM provides guidance and assistance by directing the project officer to appropriate governing regulations and Classified Briefing Guidelines, **Attachment 1**.

5.10. Personnel Security.

5.10.1. Sentinel Key rosters are used to verify clearance eligibility and identify clearance/access problems. The SM compares each new roster with the previous roster to track completion of clearance/investigation actions. The SM maintains rosters for the current month only.

5.10.2. Pending notification of clearance, individuals will not have access to classified material. The SM will request follow-up action on clearances not received within a reasonable length of time and will notify the individual's supervisor when the clearance is received.

5.10.3. A security access requirement (SAR) code is assigned to each civilian and military position on the Unit Manpower Document (UMD). Supervisors will periodically review each position to ensure the SAR code accurately reflects the level of access to classified needed to perform the duties of the position. The supervisor will request a SAR code change according to mission needs.

5.10.4. When emergency access, periodic reinvestigation (PR) or single-scope background investigation (SSBI) is needed, the affected individual will contact the SM for specific submission procedures.

5.10.5. An AF Form 2583, Request for Personnel Security Action, is prepared when access is granted to a special program such as Critical Nuclear Weapon Design Information (CNWDI).

The SM will ensure appropriate briefings are conducted, the AF Form 2583 is accurately completed, and a file of completed forms are maintained.

5.10.6. An AF Form 2587, Security Termination Statement, is prepared when access is withdrawn for any reason or when a person separates, retires, or transfers from Air Force employment. Civilian and military personnel debriefed from special programs such as CNWDI will sign an AF Form 2587 and the SM will retain the forms for 2 years. The departing individual, regardless of access to classified material, will report to the SM for debriefing and will acknowledge the debriefing by signing the AF Form 2587. The SM retains completed civilian forms for 2 years and ensures military members submit forms to the Military Personnel Flight.

5.10.7. Continued assessment of individual trustworthiness for clearance eligibility is performed. Personnel will report suspected or known derogatory information to the supervisor or SM.

5.11. Foreign Travel Briefings/Debriefings. All personnel will report foreign travel to the SM no later than 14 days prior to travel. The SM briefs personnel on travel requirements and maintains the foreign travel records.

5.12. Other Security Programs. Education and awareness of the Antiterrorism Program, Operations Security, and other security related subjects are to be incorporated into the unit's overall security program. Education and awareness of these and other related programs are conducted in conjunction with, or separate from, information security subjects.

5.13. To obtain Emissions Security (EMSEC) approval for computer systems to process classified information, personnel will contact AFIT/SCB, Information Systems Division. The SM will coordinate actions necessary to obtain EMSEC approval. The SM ensures equipment, diskettes, and classified "products" are properly marked and stored, visual aids posted, and the precautions observed. AFIT/SCB ensures proper procedures are written and followed for access and use of EMSEC approved systems.

5.13.1. AFIT personnel requiring use of classified computer systems located in Bldg 640, Rm. 235, will forward to SM a written request signed by their supervisor stating their need to use these systems.

5.13.2. The SM will maintain a list of all authorized users and maintain a schedule for the use of classified computer systems. Authorized users will notify the SM and request to be scheduled for use of the classified computer systems between the hours of 0800 – 1600, Monday through Friday, on normal duty days. The SM is authorized to deny use of the classified computer systems at any time and to reschedule use as necessary.

5.13.3. At the time of scheduled use, the user will report to Bldg 640, Rm. 235. The SM will provide the user with a classified removable hard disk and any other classified media/material belonging to or required by the user. The user is responsible for all classified material until it is

handed back in person to the SM or ASM. The user will read and comply with the system operating instructions located at or near the classified computer system.

5.13.4. At completion of use of the classified computer system, the user will comply with the operating instructions/checklist for proper shutdown procedures and hand over the classified removable hard disk and all other classified media/material in their possession to the SM or ASM (as applicable).

5.13.5. If the user has a requirement to leave the room temporarily, he/she will inform the SM prior to leaving the room. If the user is to be absent from the room for more than 15 minutes, the user will complete the proper shutdown procedures and collect and hand over all classified media/material (to include the removable hard disk) to the SM for proper storage.

5.14. Classified telephone conversations are permitted on STU-III instruments only. Procedures and cautions for STU-III use include:

5.14.1. Only cleared personnel may use the equipment. The user must possess a security clearance at or above the classification level of the material being discussed and the classification level of the STU-III being used.

5.14.2. The STU-III must meet or exceed the classification level of the material being discussed.

5.14.3. The user will protect the STU-III key when it is not in use and insure it is removed from the instrument when the conversation is finished.

5.14.4. The SM will provide users with specific instructions on STU-III use.

5.15. A warning notice, DD Form 2056, will be posted on each telephone and fax that is not authorized for classified conversation. AF Form 440, Bomb Threat, is used to record threatening calls and a form is kept at each classified, unclassified, and faxes telephone.

MICHAEL L. HEIL, Colonel, USAF
Commandant
Air Force Institute of Technology

Attachments:

1. Classified Briefing Guidelines
2. AFIT Annual Training Plan
3. Sample End-of-Duty Day Security, Check Designations and Procedures Letter
4. Classified Thesis/Research Briefing
5. Sample Request for Faculty Access to AFRL/STINFO
6. Sample Request for Student Access to AFRL/STINFO

Attachment 1

CLASSIFIED BRIEFING GUIDELINES

A1.1. Briefings, conferences, and presentations involving the discussion of classified information may be held in Building 640, Room 230; Building 642, Room 2102; and Building 642, Kenney Hall if appropriate security guidelines are followed.

A1.1.1. The AFIT sponsor is responsible for ensuring proper security procedures are followed for classes and briefings presented by outside agencies as part of an AFIT program.

A1.1.2. The AFIT sponsor, or outside agency not part of an AFIT program, requesting use of AFIT facilities to conduct a classified briefing/conference will contact AFIT/SC Audiovisual Services to reserve Building 642, Room 2102 or Kenney Hall; and AFIT/ENA, Education Technician for Building 640, Room 230. The sponsor/outside agency will also promptly notify the AFIT Security Manager (SM) of the intent to conduct a classified briefing/conference within AFIT facilities.

A1.1.2.1. For classified briefings/conferences held in Building 642, Kenney Hall, the sponsor/outside agency will prepare a Security Plan and forward it to the SM no later than 10 duty days prior to the briefing/conference (contact the SM for examples and/or specific guidance). Most importantly, the sponsor/outside agency will designate an individual responsible for security in the Security Plan and ensure the individual coordinates with the SM prior to the briefing/conference for specific guidance.

PRIOR TO THE BRIEFING

A1.2. Determine the classification level of the briefing. Briefings above the SECRET level will not be presented in AFIT facilities. If AFIT facilities are used to conduct a classified briefing/conference, the contents contained herein and any additional guidance provided by the AFIT SM must be followed. If the rooms are not available, the briefer should make arrangements to schedule locations outside of AFIT. A listing of classified conference rooms is available from the 88 SFS/SFA.

A1.3. If the briefing is above the SECRET level, or if a topic is particularly sensitive, AFIT personnel should contact ASC agencies to reserve an appropriate conference room. A listing of classified conference rooms is available from the 88 SFS/SFA.

A1.4. Check level of clearance and need to know for all attendees and door guards. For AFIT personnel and students, submit a list of attendees/door guards to the SM for verification of security clearances. For attendees other than AFIT personnel, a Visit Request is required. If an outside facility (ASC, NAIC, etc.) is to be used, follow their security requirements.

A1.5. Foreign Disclosure. **NO FOREIGN NATIONALS ARE CLEARED FOR ENTRY UNLESS APPROVAL HAS BEEN GRANTED BY THE AIR FORCE THROUGH THE AFIT FOREIGN DISCLOSURE OFFICER.**

A1.6. Arrange for door guards with a clearance compatible with the briefing to be in place prior to the briefing. The door guards should be able to monitor all entrances. Door guards should be briefed on procedures for checking identification/clearances and ensuring individuals in the vicinity of a room are not overhearing or trying to overhear classified information. Guards are furnished by the OPR's dean/director. If the function is an overall AFIT function, door guards will be detailed. Non-sponsored outside agencies are responsible for providing their own door guards.

***NOTE:** When Room 2102 is used, both inner and outer doors must be closed during the classified portion of the briefing; no phones used or electronic equipment connected to LAN lines.*

A1.7. For outside briefers transporting classified information, WPAFB Base Operations operate a 24-hour storage safe in Area C.

AT THE TIME OF THE BRIEFING

A1.8. Confirm access control personnel are in place to monitor all entrances/exits. Perform a physical sweep of the room to ensure no unauthorized personnel, tape recorders, or other unknown devices are within this room prior to the briefing. AFIT rooms are not electronically swept. The inspection is simply a physical inspection. An electronic sweep is not required for normal SECRET and below briefings. The project officer/sponsor is responsible for ensuring the integrity of the room at all times.

A1.9. If the conference room/briefing room has restrooms or closets adjacent to the briefing room, these rooms must be secured until the briefing is complete.

A1.10. Verify the identity of each individual before allowing admittance to the classified briefing. The project officer must ensure that the person checking clearances has the same level of clearance as the briefing and is monitoring the entrances at all times. Verbal confirmation of clearances by students or staff other than the SM is not allowed. The clearances of individuals must be verified by use of the ASCAS roster or Visit Request.

A1.11. Secure both the inner and outer conference room doors. (This is a must for all rooms to maintain the security level.)

CONDUCT OF BRIEFING

A1.12. Prior to the start of the briefing, the sponsor/project officer/conference leader must brief the attendees concerning the security level and procedures for the briefing or conference and the individual responsibilities of attendees. Remember to inform attendees that recording devices are not allowed. This is particularly important when personnel from outside AFIT are attending. Do not use electronic sound amplification systems for classified briefings unless prior approval has been obtained from AFIT/SC Audiovisual Services. If this is an AFIT-sponsored briefing, the sponsor must remain at the briefing for its duration.

A1.13. The sponsor/project officer/conference leader must also inform attendees that note taking is prohibited during classified briefings.

A1.14. Ensure the conference room is secured at all times by a person with the appropriate clearance level and that classified material is not left unattended during breaks or during lunch period. Ensure classified is stored in an appropriate container.

A1.15. Identify the overall classification of information briefed prior to closing the briefing/conference.

A1.16. Perform a final physical inspection to ensure that no classified is left behind by the briefer.

A1.17. Notify the SM, ASM, or designated representative when the briefing/conference conducted in Building 642, Kenney Hall, is completed so a check can be made to ensure that no classified material has been left in the room.

Attachment 2

**AIR FORCE INSTITUTE OF TECHNOLOGY
ANNUAL TRAINING PLAN**

A2.1. References.

A2.1.1. DOD 5200.1-R

A2.1.2. AFI 31-401

A2.1.3. AFI 10-1101

A2.1.4. AFI 61-205

A2.1.5. AFI 71-101V2

A2.1.6. AFI 31-209

A2.1.7. AFP 205-11

A2.1.8. AFR 31-501

A2.1.9. AFIJ 31-404

A2.1.10. AFR 205-57

A2.1.11. AFI 33-219

A2.2. General. Commandant and staff agency chiefs must ensure personnel understand the compelling need to protect classified and sensitive resources. To accomplish this, supervisors provide an initial security briefing within 90 days of a person's assignment. Do this in a one-to-one setting or group discussion using training aids. Thereafter, security managers provide quarterly refresher training directly via email or using guest speakers.

A2.3. Schedule.

A2.3.1. First quarter:

A2.3.1.1. Security violation reporting and requirements.

A2.3.1.2. Personnel security - Clearances, periodic reinvestigations, special security files.

A2.3.1.3. Security of classified material and end-of-day security checks.

A2.3.1.4. Local security policies and practices. Results of semiannual inspection, security review, IG evaluations, and analysis of security violations.

A2.3.1.5. Selected topics from quarterly security manager's meeting.

A2.3.2. Second quarter.

A2.3.2.1. Marking classified documents.

A2.3.2.2. Reproduction requirements and procedures.

A2.3.2.3. Reporting suspicious contacts.

A2.3.2.4. Telephone and fax transmission security.

A2.3.2.5. Security of classified and end-of-day security checks.

A2.3.2.6. Selected topics from quarterly security manager's meeting.

A2.3.3. Third quarter.

A2.3.3.1. Espionage

A2.3.3.2. Classification challenges.

A2.3.3.3. Handcarrying classified material.

A2.3.3.4. OPSEC

A2.3.3.5. Protection of government/personal property.

A2.3.3.6. Selected topics from quarterly security manager's meeting.

A2.3.4. Fourth quarter.

A2.3.4.1. Semiannual security inspection.

A2.3.4.2. Destruction of classified material.

A2.3.4.3. Bomb threats, local threats and base security OPLAN.

A2.3.4.4. Special security requirements - CNWDI

A2.3.4.5. Selected topics from quarterly security manager's meeting.

Attachment 3**SAMPLE END-OF-DUTY DAY SECURITY CHECK
DESIGNATIONS AND PROCEDURES**

MEMORANDUM FOR BARB JONES
DIANNE SMITH
PENNY NICKLE
DON DOE

FROM: AFIT/(OFF SYM of Department/Division Head)

SUBJECT: End-of-Duty Day Security Check Designations and Procedures

1. The personnel listed below will perform a room and area check at the end of each duty day IAW the following schedule:

14 - 25 Jan	Barb Jones
28 - 08 Feb	Dianne Smith
11 - 22 Feb	Penny Nickle
22 - 05 Mar	Don Doe

2. To ensure proficiency, divorce the current day's business from your mind and refrain from engaging in conversation while checking the safes and office areas.

3. The room and area check will include the following:

a. Verify the locked condition of the safes by pressing down on the handle of the locking drawer and pulling on it. If the drawer does not open, slowly rotate the locking device clockwise; press down and pull on the drawer handle. If the safe drawer still remains secured, turn the locking device four times in one direction and try to open all drawers. When you are satisfied that the safe is locked, annotate the "Checked By" column on the SF 702, Secure Container Check Sheet, located on the outside of the container. If a safe is found open and unattended, notify one of the individuals listed on the SF 700 posted inside the locking drawer. Do not leave the safe open or unattended. Remain with the safe until the person notified responds or secure the safe and depart, depending on instructions received from the safe custodian. If the safe was not opened during the day, enter the date and statement "Not Opened" and complete the "Checked By" columns.

b. Check each desktop, including file baskets, tables top, desk trays, tops of bookcases, file cabinets, etc, and assure yourself that there isn't any unsecured classified material. Check trashcans to ensure classified have not been inadvertently thrown away. If classified material is found unprotected, have it secured in a safe; notify your supervisor and security manager immediately. Ensure any unopened Registered, Certified, USPS Express Mail and/or First Class mail, with or without the "Do Not Forward" insignia, is also properly secured.

c. Check each cubicle and desk for other sensitive, unclassified material that may not be properly stored.

d. Check electrical equipment and appliances in each area to ensure they are turned off. Include typewriters, calculators and coffee pots

e. Annotate the completed room and area check on SF 701, Activity Security Checklist. On the reverse side of the checklist, record the name of each person who is still working when the check is made.

SIGNATURE ELEMENT OF
DEPARTMENT/DIVISION HEAD

Attachment 4

CLASSIFIED THESIS/RESEARCH BRIEFING

A4.1. IN ADDITION TO THE INITIAL SECURITY INDOCTRINATION YOU RECEIVED AFTER YOUR ARRIVAL AT AFIT, IT IS NECESSARY THAT YOU FULLY UNDERSTAND THE FOLLOWING INFORMATION PRIOR TO STARTING A CLASSIFIED THESIS OR CONDUCTING CLASSIFIED RESEARCH:

A4.2. AFIT/MSPS (Security) is the clearinghouse for all classified information sent to you during your tour of duty at AFIT.

A4.2.1. If a student requires classified material be mailed to AFIT, the student will ensure consent to request the material is obtained from their supervisor/faculty advisor. If approved, the student will notify the SM of the intent to receive classified mail and ensure the sender addresses the registered package as follows:

<u>Inside Envelope</u>	<u>Outside Envelope</u>
AFIT/EN [your department]	AFIT/MSPS
(Attn: [Your Name])	2950 P Street
2950 P Street	Wright-Patterson AFB OH 45433-7765
Wright-Patterson AFB OH 45433-7765	

A4.2.2. AFIT/MSPS (Security) will sign for the material and ensure that it is properly transferred to AFRL/STINFO, Bldg 640, Rm. 67. The SM will notify the requester, as identified on the inside envelope attention line, when the material is received at AFIT.

A4.2.3. Students will ensure all classified material requested and received by them is marked correctly. If the material received is marked incorrectly, the student will notify the sender and request further guidance as to the discrepancies noted.

A4.3. Key-lockable cabinets within AFRL/STINFO will be used to store all incoming classified material and any classified texts, lecture notes, and student notes created.

A4.3.1. The student must have an access letter submitted, approved by the SM, and on file before being granted access to classified material maintained in AFRL/STINFO (Attachment 6).

A4.3.2. Students are responsible for all classified material they create and/or receive and store in AFRL/STINFO. In addition, students will follow proper procedures for handling/safeguarding classified material as identified in DOD 5200.1-R, Information Security Program; AFI 31-401, Information Security Program; and AFITI 31-101, paragraph 5.4.10.3.

A4.3.3. Students storing classified material in AFRL/STINFO will destroy all of their classified research material prior to graduating or departing AFIT (see AFITI 31-101, paragraph 5.5.2). Students identifying classified material for continued storage after their departure from AFIT

will turn over custodianship of the material to their supervisor/faculty advisor. The supervisor/faculty advisor will in turn contact the SM of the need to further store the classified material in AFRL/STINFO.

A4.4. Prior to preparing any classified notes, working papers, drafts, and the finished product, it is the student's responsibility to review DOD 5200.1-R, Chapter 5, Section 2; AFI 31-401; and DOD 5200.1-PH, Marking Classified Documents.

A4.4.1. Most importantly, students will ensure they mark all documents to include classified theses IAW AFI 61-204, Disseminating Scientific and Technical Information, immediately upon creation.

A4.4.2. If the student has reviewed AFH 31-405 and AFI 61-204 and are still unsure on how to mark the material correctly, he/she should request assistance from their faculty advisor or SM/ASM (in that order).

A4.5. A good rule to remember is . . . WHEN YOUR CAREER IS ON THE LINE, IT'S BETTER TO BE SAFE THAN SORRY!

I HAVE READ AND UNDERSTAND THE REQUIREMENTS OF THIS BRIEFING AND I HAVE REVIEWED AND UNDERSTAND AFITI 31-101. A COPY OF THIS SIGNED BRIEFING WILL BE FORWARDED TO THE SECURITY MANAGER (AFIT/MSPS).

(SIGNATURE OF STUDENT)

(SIGNATURE OF SUPERVISOR/
FACULTY ADVISOR)

(STUDENT'S PRINTED LAST NAME, FIRST, M.I.)

(DATE)

Attachment 5

**SAMPLE REQUEST FOR FACULTY
ACCESS TO AFRL/STINFO**

MEMORANDUM FOR AFIT/MSPS
AFRL/STINFO
IN TURN

FROM: AFIT/(OFFICE SYMBOL)

SUBJECT: Request for Access to AFIT Classified Material Stored in AFRL/STINFO

1. Request the following faculty be granted access to AFIT classified material stored within AFRL/STINFO, Bldg 640, Rm. 67, in the performance of their official duties:

<u>RANK/ GRADE</u>	<u>NAME Last, First MI</u>	<u>SSAN</u>	<u>SECURITY CLEARANCE</u>	<u>DUTY PHONE</u>
Capt	Jones, John J.	111-22-3333	SECRET	5-3636 x1111

2. I certify the individual(s) identified above has been briefed on proper procedures for handling/safeguarding AFIT classified material stored in AFRL/STINFO as outlined in AFITI 31-101, Attachment 7.

SIGNATURE OF ELEMENT OF
DEPARTMENT/DIVISION HEAD
(or higher)

Attachment 6

**SAMPLE REQUEST FOR STUDENT
ACCESS TO AFRL/STINFO**

MEMORANDUM FOR AFIT/MSPS
AFRL/STINFO
IN TURN

FROM: AFIT/(OFFICE SYMBOL)

SUBJECT: Request for Access to AFIT Classified Material Stored in AFRL/STINFO

1. Request the following student(s) be granted access to AFIT classified material stored within AFRL/STINFO, Bldg 640, Rm. 67, in the performance of conducting classified research in conjunction with thesis work:

<u>RANK/ GRADE</u>	<u>NAME Last, First MI</u>	<u>SSAN</u>	<u>SECURITY CLEARANCE</u>	<u>DUTY PHONE</u>
Capt	Jones, John J.	111-22-3333	SECRET	5-3636 x1111

2. I certify the individual(s) identified above has been briefed on proper procedures for handling/safeguarding AFIT classified material stored in AFRL/STINFO as outlined in AFITI 31-101, Attachment 7. I further state that a Classified Thesis/Research Briefing, AFITI 31-101, Attachment 4, has been conducted IAW AFITI 31-101, par. 5.4.9, and a copy has been forwarded to AFIT/MSPS, Security Manager.

SIGNATURE OF ELEMENT OF
SUPERVISOR/FACULTY ADVISOR (or higher)