

DEPARTMENT OF THE ARMY  
HEADQUARTERS, UNITED STATES ARMY MATERIEL COMMAND  
5001 EISENHOWER AVENUE, ALEXANDRIA, VA 22333-0001

AMC Supplement 1  
to AR 380-5

14 March 2003

Security

DEPARTMENT OF THE ARMY INFORMATION SECURITY PROGRAM

Supplementation by U.S. Army Materiel Command (AMC) Major Subordinate Commands (MSCs), Separate Reporting Activities (SRAs) and other installations and activities reporting directly to Headquarters (HQ), AMC is permitted at command option, but is not required. Copies of each supplement will be furnished to the Commander, HQ AMC (AMXMI-SCM), and to the AMC Security Support Division (AMXMI-SD), 1323 Cobb Street, SW, Fort McPherson, GA 30330-1074.

AR 380-5, 29 September 2000, is supplemented as follows.

Page 1, para 1-1, Purpose. Add the following at the end:

This supplement establishes responsibilities and procedures for administration of the AMC Information Security Program. It must be used in conjunction with the basic regulation.

Page 1, para 1-5, Headquarters Department of the Army (HQDA). Add subparagraph e after subparagraph d:

e. The HQ AMC Deputy Chief of Staff, G-2 is responsible for implementation of and compliance with DOD and Department of the Army Information Security Program requirements throughout AMC. The Chief, AMC Security Support Division (SSD), is responsible for monitorship (through overviews) of the AMC Information Security Program.

Page 2, para 1-6, The Commander. Add the following at the end of subparagraph e:

Requests for waivers of the minimum rank/grade requirement for the Command Security Manager (CSM) will be forwarded to this headquarters, ATTN: AMXMI-SCM.

Page 2, para 1-6, The Commander. Add subparagraph l after subparagraph k:

Initiate and supervise measures to ensure classified holdings are kept to a minimum consistent with mission accomplishment.

---

\*This supplement supersedes AMC Suppl 1 to AR 380-5, 19 April 2001.

Page 2, para 1-7, The Command Security Manager. Add subparagraph r after subparagraph q:

r. Provide an Annual Security Status Report to the Commander HQAMC, ATTN: AMXMI-SCM. Reports are due no later than 31 January of each year and will cover the preceding calendar year (1 January through 31 December). AMC MSCs will provide consolidated reports for their commands. See Appendix A for the required format for the Annual Security Status Report.

Page 4, para 1-10, Applicability Definition. Add the following at the end:

This supplement applies to HQ AMC; AMC MSCs (including their subordinate installations and activities); separate installations and activities reporting directly to HQ AMC; program/project/product managers obtaining functional support from AMC elements; and all personnel (military, civilian, and contractor) physically located at said commands, installations, and activities.

Page 5, para 1-19, Waivers and Exceptions to Policy. Add subparagraph e after subparagraph d:

e. Requests for waivers or exceptions to policy outlined in the basic regulation or this supplement will be forwarded through command security channels to Commander HQAMC, ATTN: AMXMI-SCM. Requests for waivers for SAPs will be submitted through SAP channels to AMXMI-SAP. Requests for waivers for SCI policy guidance will be submitted through SSO channels to AMXMI-SSO.

Page 7, para 1-23, Reporting Requirements. Add the following at the end:

MSCs and SRAs will submit a consolidated report for all units under their security responsibility to reach the Commander HQAMC, ATTN: AMXMI-SCM no later than 15 September or other date specified by HQAMC (AMXMI-SCM) each fiscal year.

Page 8, para 2-3, Delegation of Authority. Add subparagraphs d, e, and f after subparagraph c:

d. Requests for original classification authority will be submitted through command security channels to this HQ, ATTN: AMXMI-SCM. Each request will explain how conditions in paragraph 2-3c apply and will also provide an estimate as to the frequency with which original classification authority will be used.

e. Changes to designations of classification authorities (such as deletions or changes in position/organization titles) will be reported promptly through command security channels to this HQ, ATTN: AMXMI-SCM.

f. Commanders are responsible for maintaining a current list, by title, of original classification authorities in their respective organizations. AMXMI-SCM will maintain a master list for the command.

Page 12, para 2-18, Approval, Distribution, and Indexing. Add subparagraphs e and f after subparagraph d:

e. Copies of each approved security classification guide (less those for SAPs or programs involving SCI) and changes thereto will also be sent to the addresses listed at Appendix B of this supplement, Distribution of Security Classification Guides.

f. One copy of each completed current DD Form 2024 will also be provided to HQAMC, ATTN: AMXMI-SCM.

Page 12, para 2-19, Review, Revision, and Cancellation. Add the following at the end of subparagraph a:

Foreign military sales issues will be considered during the review of all classification guides and coordination for such issues will be made with security assistance/foreign military sales representatives.

Page 14, para 3-1, General (Army Declassification Program). Add the following at the end:

Each original classification authority will designate individuals, by position title, who are authorized to specify information under their proponency which may be downgraded and/or declassified earlier than previously specified or will specify in writing that authority is not to be further delegated. One copy of each designation and subsequent changes will be forwarded to this HQ, ATTN: AMXMI-SCM and AMC SSD, ATTN: AMXMI-SD.

Page 15, para 3-3, Declassification of Restricted Data and Formerly Restricted Data. Add the following subparagraphs:

- a. Holders of RD/FRD documents who are the proponents of the document will:
- (1) Review material to determine if it must be retained or destroyed.
  - (2) Mark documents to clearly indicate which portions are believed to be classified (and to what level) and which portions are unclassified.
  - (3) Forward documents in question and the rationale supporting their classification position to --

Office of Classification  
Mail Stop C356  
U.S. Department of Energy  
Washington, DC 20545

- (4) Advise all holders of the results of the review by the Department of Energy.
- b. Holders of RD/FRD documents who are not the proponents of the document will --

- (1) Review material to determine if it must be retained or destroyed.
- (2) If information must be retained, develop a position regarding its classification (i.e., remain at current level, downgrade, remove RD/FRD markings, or declassify).
- (3) Forward the document in question and supporting rationale to the proponent.

c. Proponents who receive RD/FRD documents from other holders will --

- (1) Review referred documents, evaluate the local position pertaining to classification, and formulate their position regarding proper classification.
- (2) Mark documents to clearly indicate which portions are believed to be classified (and to what level) and which portions are unclassified.
- (3) Forward documents in question and the rationale supporting their classification position to --

Office of Classification  
Mail Stop C356  
U.S. Department of Energy  
Washington, DC 20545

- (4) Advise all holders of the results of the review by the Department of Energy.

Page 31, para 4-23, Printed Documents Produced by AIS Equipment. Add subparagraph d and e after subparagraph c:

d. A review of classification markings applied by AIS equipment will be accomplished prior to dissemination or reproduction of documents.

e. With the advent of electronic mail, communications between units and personnel has increased rapidly. With this increase in e-mail, there is also a decrease in security awareness when it comes to proper classification markings on these messages. We must ensure that proper page and portion markings are used on all correspondence just as if it was typed or hand written. Effective immediately, each command will publish a policy and procedures for proper marking of classified and unclassified material on the Secure Internet Protocol Router Network (SIPRNET) system. Appendix I is the required format and the policy and procedures that will be established for each Command. In order to standardize the marking policy and procedures across AMC, you are required to use the procedures at Appendix I. If you already have a policy and procedures in place or have a better way of marking SIPRNET e-mail correspondence, request you forward a request for waiver along with a copy of your policy and procedures to this HQ, ATTN: AMXMI-SCM.

Page 34, para 4-35, Downgrading and Declassification in Accordance with Markings. Add the following at the end of paragraph b:

The page marking will be cancelled on the back cover also.

Page 63, para 6-2, Nondisclosure Agreement. Add subparagraph c after subparagraph b:

- b. The revised edition of the SF 312, edition date 1-00, changes references to Executive Order 12356 to Executive Order 12958 and adds a new law, Section 1924, of Title 18. The SF 312 is available electronically on the General Services Administration's web site at
- c. <http://www.gsa.gov> and on the Defense Security Service web site at [www.dss.mil/whatsnew/sf312.htm](http://www.dss.mil/whatsnew/sf312.htm). Additionally, a pamphlet on the use of the SF 312 can be obtained from the NARA web site at [www.archives.gov/isoo/education\\_and\\_training/standard\\_form\\_312.pdf](http://www.archives.gov/isoo/education_and_training/standard_form_312.pdf). Unused supplies of the previous edition of the SF 312 will not be used and will be destroyed. Previously executed SF 312s do not need to be replaced with the current edition.

Page 65, para 6-7, Access to Restricted data, Formerly Restricted Data, and Critical Nuclear Weapons Design Information. Add the following at the end of paragraph b:

A copy of DOE Form 5631.20 (Request for Visit or Access Approval) as well as a list of Department of the Army Officials who can certify the need for access to restricted data and critical nuclear weapon design information can be found at Appendices C and D, respectively.

Page 67, para 6-11, End-of-Day Security Checks. Add subparagraphs c and d after subparagraph b:

c. When checking a safe with conventional type combination dial, X07 or x08, check each drawer individually by depressing drawer latch and pulling. Rotate combination dial at least four times in one direction and re-check each drawer. When checking a safe with manipulation proof dial combination, reset the dial to 0 and turn the butterfly to the right to relock it and move the dial to the right until it stops. Then press down on latch of combination drawer and pull out on it at the same time. Keep the latch down on the combination drawer while checking the other drawers. After completing the check, unlock the butterfly and rotate the dial at least four times in one direction.

d. Room check procedures will be established in each separate office where classified information/materials are used or stored. SF 701 (Activity Security Checklist) will be posted near the office exit door and will be used to certify completion of the room check each duty day.

Page 68, para 6-12, Emergency Planning. Add the following at the end:

Emergency plans will be revised as needed. Such revisions will be annotated on the plan. As a minimum, emergency action plans should contain detailed procedures addressing secure storage, evacuation, or emergency destruction of classified material. Emergency plans should be tested at least annually.

Page 69, para 6-16, Visits. Add the following at the end of subparagraph a:

AMC Form 1663-R-E (Request for Visit Authorization) dated 15 Jan 92 will be used for visit requests. A copy of the form can be found at Appendix E.

Page 70, para 6-17, Classified Visits by Department of Energy Personnel and to DOE Facilities. Add the following at the end:

A copy of DOE Form 5631.20 (Request for Visit or Access Approval) as well as a list of Department of the Army Officials who can certify the need for access to Restricted Data (RD) and Critical Nuclear Weapon Design Information (CNWDI) can be found at Appendices C and D, respectively.

Page 71, para 6-18, Classified Meetings and Conferences. Add to the end of subparagraph a(1):

Commands will maintain a system of control measures that ensure access to classified information is limited only to authorized persons. The control measures will be appropriate to the environment in which the access occurs and the nature and volume of the information. The system will include technical (where applicable), physical, administrative, personal, and personnel control measures. It is incumbent upon the person holding the classified meeting to ensure that classified discussions cannot be heard outside of the conference or meeting area, and that access to the area is controlled. In approving a space for classified meetings/discussions/conferences, the following security measures will be implemented:

a. Validate security clearance and need-to-know of all attendees prior to admitting them to the meeting.

b. Ensure the room in which the meeting or conference is being held is appropriate for discussion of classified information. It must have controlled access such that no unauthorized persons can come into the room while discussions are ongoing, and should be of sufficient construction that classified conversations cannot be heard in adjoining rooms or hallways.

c. Ensure that access control is maintained at all times.

Page 71, para 6-18, Classified Meetings and Conferences. Add to the end of subparagraph c:

All requests along with a detailed security plan will be forwarded through command security channels to this headquarters, ATTN: AMXMI-SCM.

Page 71, para 6-18, Classified Meetings and Conferences. Add subparagraphs e and f after subparagraph d:

e. The authority to approve non-acquisition related, non-association related, U.S. only classified conferences being held in cleared facilities is delegated to Commanders of Major Subordinate Commands (MSCs) and to Commanders/Directors of Separate Reporting Activities (SRAs). This authority may be redelegated to MSC Chiefs of Staff with power of redelegation to senior intelligence officers provided they are Lieutenant Colonels or GS 15s and above. The delegated authority will ensure that guidelines of the basic regulation are adhered to when hosting classified conferences. Copies of all approvals will be forwarded to this office, ATTN: AMXMI-SCM.

f. Waivers: Requests for waivers to any of the requirements outlined in para 6-18 of the basic regulation must be forwarded through command security channels to this office, ATTN: AMXMI-SCM, within 150 days of the meeting.

Page 73, para 6-21, TOP SECRET Information. Add the following at the end of subparagraph a:

(1) TSCO positions within AMC intelligence and security offices are inherently governmental and therefore must be filled by either U.S. government civilian or military personnel. This determination extends to the alternate TSCO as the alternate performs TSCO duties in the absence of the TSCO.

(2) While there is no grade/rank preference for alternate TSCOs, requests for waivers of the minimum rank/grade requirement for TSCOs will be forwarded to this headquarters, ATTN: AMXMI-SCM.

Page 73, para 6-21, TOP SECRET Information. Add the following at the end of subparagraph b:

DA Form 3964 or DA Form 455 will be used for the TOP SECRET accountability record form. The description of the document must be consistent with that which appears on the applicable DA Form 969 (TOP SECRET Document Record) or another approved document register.

Page 73, para 6-21, TOP SECRET Information. Add the following at the end of subparagraph c:

AMC installations and activities with 100 or more TOP SECRET documents will conduct a 10 percent physical inventory each month until all TOP SECRET documents have been accounted for. A properly cleared, disinterested party that is neither a TSCO nor alternate or subordinate to either official will witness the 10 percent inventory report each month. The signed certification of inventory will attest that inventoried documents were physically sighted and were complete. Those with less than 100 are exempt from the 10 percent monthly inventory but must complete a 100% annual inventory.

Page 73, para 6-21, TOP SECRET Information. Add the following at the end of subparagraph e:

Within AMC, a new TSCO must be appointed under the following conditions and a 100% inventory must be conducted by the outgoing and incoming custodians:

- (1) On change of duty assignment within an office, activity, or installation.
- (2) On permanent change of station.
- (3) On temporary absence of more than 30 calendar days.
- (4) On separation from the military service or termination of employment with the Army.

Page 74, para 6-22, SECRET and CONFIDENTIAL Information. Add the following at the end:

The control system must provide a means to ensure that Secret material sent outside the command or activity has been delivered to the intended recipient. Such delivery may be presumed where the material is sent electronically over secure voice or data circuits and through hand-to-hand transfer when the receiving party acknowledges responsibility for the Secret material. AMC activities will use the DA Form 3964 as a means to verify an addressee's receipt of Secret material sent by mail outside the activity. The DA Form 3964 should also be used as a means of receipt when forwarding Confidential or Secret mail to a cleared contractor facility.

Page 74, para 6-24, Working Papers. Add subparagraph (4) after subparagraph b (3):

(4) Requests for exceptions to accountability, control, and marking requirements for working papers containing TOP SECRET information must be submitted through command security channels to this HQ, ATTN: AMXMI-SCM.

Page 75, para 6-27, Policy (Disposition and Destruction of Classified Material). Add subparagraph f after subparagraph e:

f. Each AMC installation and activity will establish an annual cleanout day. Local commanders will determine the exact date based upon mission requirements. The date chosen will be indicated in item 10 (Explanatory Comments) of the SF 311, Agency Security Program Management Classification Data Report.

Page 76, para 6-28, Methods and Standards for Destruction. Add the following at the end of subparagraph a:

Requests for exceptions will be forwarded through command security channels to HQAMC, ATTN: AMXMI-SCM.

Page 76, para 6-29, Records of Destruction. Add the following at the end of subparagraph a:

Each commander is responsible for ensuring destruction officers and disinterested witnessing officials for TOP SECRET materials are appointed. A sufficient number of individuals will be so designated to ensure the availability of officials for timely destruction.

Page 77, para 6-30, General. Add the following at the end:

Requests for waivers will be forwarded through command security channels to this HQ, ATTN: AMXMI-SCM. Requests for waivers for SAPs will be forwarded through this HQ, ATTN: AMXMI-SAP. Requests for waivers for SCI policy guidance will be submitted through SSO channels to AMXMI-SSO.

Page 77, para 6-34, Prior Waivers. Add the following at the end:

As stated in the basic regulation, waivers granted before the effective date of this regulation are cancelled. New/updated waiver requests must be submitted prior to their cancellation date.

Page 78, para 7-4, Storage of Classified Information. Add subparagraphs (4), (5), (6), (7), (8), and (9) after subparagraph a(3):

(4) CONFIDENTIAL and/or SECRET material will not be stored in non-GSA-approved containers having a built-in combination lock or in a non-GSA approved container secured with a rigid metal lock-bar and a GSA-approved padlock unless an exception has been granted.

(5) Authority to approve exceptions for CONFIDENTIAL and SECRET storage is delegated to Commanders of MSCs and to Commanders/Directors of SRAs. This authority may be redelegated to MSC Chiefs of Staff with power of redelegation to senior intelligence officers provided they are Lieutenant Colonels or GS 15s and above. Requests for waivers and exceptions to TOP SECRET storage requirements will continue to be forwarded to this HQ, ATTN: AMXMI-SCM. Also, requests for approval to use alarmed areas for storage of TOP SECRET material will be forwarded through command security channels to this HQ, ATTN: AMXMI-SCM. Enclosures for such requests will be in the format shown in Appendix F to this supplement.

(6) Before approving exceptions to storage standards, the approving authority should compare the construction standards of the proposed facility with those in Section III (Physical Security Standards), para 7-13, 7-19, and 7-20 of the basic regulation. The construction information, combined with other factors, such as threat, sensitivity of the classified information, amount of in-depth security safeguards, and other pertinent information should be considered. As previously stated, the format for requests for exceptions/waivers to storage requirements is located at Appendix F. Copies of approved waivers will be forwarded to this HQ, ATTN: AMXMI-SCM, with a copy furnished to AMXMI-SD.

(7) Exceptions and waivers require compensatory measures equal to or greater than the requirements of the regulation.

(8) Waivers are valid for one year only and require annual renewal, if necessary. Approvals will be based upon submission of projects and milestones, which support the attainment of the requirements of the regulations for which the waiver was issued. Requests for renewal for TOP SECRET waivers will be submitted 90 days prior to the expiration date to this HQ, ATTN: AMXMI-SCM and will provide project/milestone status updates.

(9) Exceptions are permanent and are applicable only when current procedures exceed requirements of the regulation or it is cost-prohibitive to meet the requirements. Exceptions will be reevaluated every two years and revalidated, as necessary. Requests for biennial review for TOP SECRET exceptions will be submitted 90 days prior to the expiration date to this HQ, ATTN: AMXMI-SCM.

Page 80, para 7-5, Procurement of New Storage Equipment. Add the following at the end of subparagraph a:

Requests for exceptions will be forwarded through command security channels to this HQ, ATTN: AMXMI-SCM with a copy furnished to AMC SSD (AMXMI-SD).

Page 81, para 7-8, Equipment Designations and Combinations. Add subparagraphs g, h, and i after subparagraph f:

g. Only one Standard Form 700 (Security Container Information) will normally be affixed to the inside of each security container. If a security container has drawers that are equipped with a separate external locking device and the custodians are the same, Part 1 of the SF 700 may be duplicated and placed inside each drawer. If the custodians are not the same for all drawers, a separate SF 700 will be displayed in each drawer.

h. The SF 700 will be used to list the names of the personnel to be contacted in an emergency or when the container is found open and unattended. Personnel listed on the SF700 should be knowledgeable of the contents of the security container and be able to conduct an inventory to determine if anything is missing or has been disturbed if the container is found open or unattended. The individuals listed on parts 1 and 2 of the SF 700 need not know the combination to the security container.

i. The revised edition of the SF 700, edition date 4-01, changed the completion instructions and added another identifying block for more information about the security container. The SF 700 is available in the Government supply system. Agency-wide use of the revised edition of the SF 700 is in effect. Previous editions are obsolete and should not be used. The revised edition of the SF 700 should be used when conditions for changing the combinations of security equipment occur as cited in para 7-8 of AR 380-5.

Page 83, para 7-12, General (Physical Security Standards). Add the following at the end:

When classified material is proposed for open storage in vaults, buildings, offices, or rooms, qualified facility engineer personnel will verify the structural composition of the storage facility according to standards outlined in Section III, para 7-13, 7-19, and 7-20 of the basic regulation. The facility will be certified regarding its composition and the highest level of classified material authorized for storage. This certification will be displayed inside the storage facility. The certification will be on a five-year renewal basis or when there has been a physical modification to the structure. Upon completion of all certifications, authority to approve requests for open storage of classified SECRET and CONFIDENTIAL material is delegated to Commanders of MSCs and to Commanders/Directors of SRAs. This authority may be redelegated to MSC Chiefs of Staff with power of redelegation to senior intelligence officers provided they are Lieutenant Colonels or GS 15s and above. Requests for open storage of TOP SECRET material as well as requests for waivers to TOP SECRET storage requirements will continue to be forwarded to this HQ, ATTN: AMXMI-SCM. If you are storing TOP SECRET material, an IDS is required and there are no exceptions. If you are storing SECRET and below material, an IDS is not required as long as one of the following methods is used: a) In a GSA approved container, b) In a vault that meets the standards of paragraph 7-13a of the basic regulation, or c) In a secure room that meets the standards of paragraph 7-13b of the basic regulation. For SECRET and below storage, if the area does not meet any of the above three standards, then you must invoke the criteria in paragraph 7-20 of the basic regulation (Minimum standards for deviations to construction standards for open storage areas), in which case an IDS is required.

Page 90, para 8-2, TOP SECRET Information. Add subparagraph h after subparagraph g:

h. TOP SECRET information destined for DoD contractors will not be dispatched until safeguarding and storage capability and facility clearance have been verified.

Page 90, para 8-3, SECRET Information. Add subparagraph j after subparagraph i:

j. SECRET information destined for DOD contractors will not be dispatched until the safeguarding and storage capability, facility clearance, and appropriate mailing address have been verified.

Page 91, para 8-4, CONFIDENTIAL information. Add subparagraph f after subparagraph e:

f. CONFIDENTIAL information destined for DOD contractors will not be dispatched until the safeguarding and storage capability, facility clearance, and appropriate mailing address have been verified.

Page 95, para 8-12, General Provisions (Escort or Handcarrying of Classified Material). Add the following at the end of subparagraph a(3):

The authority to approve the handcarry of classified information outside Continental United States (OCONUS), its territories, and Canada aboard commercial passenger aircraft or U.S. military conveyances is delegated to Commanders of MSCs and to Commanders/Directors of

SRAs. This authority may be redelegated to MSC Chiefs of Staff with power of redelegation to senior intelligence officers and officials who have been authorized to approve travel orders. This authority also permits the courier to handcarry the items within the OCONUS area. Commercial passenger aircraft or U.S. military conveyances must be used exclusively, and all other applicable portions of Section IV of Chapter 8 of this regulation must be adhered to. A copy of all approvals to handcarry classified material to OCONUS locations will be forwarded to this HQ, ATTN: AMXMI-SCM. The authorizing official for handcarrying classified information within and between the U.S., its territories and Canada will be determined by the Commander of the MSC or SRA.

Page 96, para 8-13, Documentation. Add subparagraph c after subparagraph b:

c. Contractor employees who are required to hand carry classified information will coordinate with the contractor Facility Security Officer (FSO) for issue of an Authorization Letter, Courier Letter, or Courier Card.

Page 100, para 9-1, General Policy. Add subparagraphs e and f after subparagraph d:

d. The Security Education Program will, at a minimum, consist of the following elements:

(1) An indoctrination briefing which is an individual briefing by a supervisor or security representative and is given before granting access to classified information to ensure that newly assigned employees know the job-specific security requirements and security procedures for the office. More emphasis on security procedures will be needed when the new employee has not had previous experience handling classified information (e.g., explanation of levels of classified material, basic marking requirements, need-to-know, storage, and reporting breaches of security should be presented). This briefing may be supplemented, but not replaced, by a requirement to read applicable security regulations. See paragraph 9-4 of the basic regulation for additional information.

(2) Refresher training as outlined in paragraph 9-7 of the basic regulation.

(3) Foreign travel requirements as outlined in paragraph 9-8 of the basic regulation.

(4) Termination briefing as outlined in paragraph 9-15 of the basic regulation.

f. Records will be maintained on file to document attendance for all briefings outlined in subparagraph e above. For annual refresher briefings records will, as a minimum, consist of name, organizational element, date of training/briefing, and type of briefing. The refresher briefing records will be maintained until completion of the next year's training program.

Page 101, para 9-7, Refresher Briefing. Add the following at the end:

Annual refresher training may also combine Operations Security (OPSEC) training (required by AR 530-1) and Subversion and Espionage Directed Against the U.S. Army (SAEDA) training (required by AR 381-12). Foreign Disclosure training must be included in the annual refresher training. Also, effective immediately, your Annual Security Awareness, Education and Training (SAET) Program will include training on the handling, protection and dissemination of SCI information. The SAET program is normally your collateral security education program and generally doesn't include SCI programs, however due to individuals holding collateral clearances mistakenly receiving sensitive compartmented information, it is necessary to include it. All individuals receiving SAET should be given basic familiarity with SCI and told what do to in case they inadvertently come into contact with it. Requiring that individuals read security regulations and then certify their understanding of the requirements does not satisfy training requirements. Non-traditional methods of training such as computer-based training instead of classroom training is always an option. Appendix G of this supplement contains a list of suggested topics for briefings; security manager involvement in identifying other topics for specific audiences is recommended.

Page 104, para 9-15, General Policy (Termination Briefings). Add subparagraph e after subparagraph d:

e. Security Termination Statements will be executed only when required by the basic regulation. For example, a Security Termination Statement need not be executed for an employee transferring from one DOD office to another when it is known that the employee's new position will require a security clearance. See paragraph 6-5 of the basic regulation for more detailed policy on termination briefings.

Page 105, para 10-2, Reaction to Discovery of Incident. Add subparagraph e after subparagraph d:

e. Some examples of instances that must be reported to the security manager include discovery of any of the following:

- (1) TOP SECRET documents lost to accountability.
- (2) Security container open and unattended.
- (3) Classified documents left unsecured and unattended.
- (4) Disclosure of classified information to a person not authorized access.
- (5) Appearance of classified material in public media.
- (6) Classified information discussed or sent over an unsecured means of communication or processed on an AIS that has not been approved for classified processing.

Page 105, para 10-3, The Preliminary Inquiry. Add subparagraphs g and h after subparagraph f:

g. The inquiry, including the written report, will be completed as quickly as possible but in no case will it exceed 30 calendar days after discovery of the security incident. Progress of the preliminary inquiry will be monitored by the local security manager who will provide the commander with the written results to include providing updates until the case is closed through assignment of administrative or disciplinary action or a determination that no such action is warranted. This will be accomplished even when investigation eliminates the possibility of compromise or establishes that compromise could not reasonably be expected to cause damage to national security. Each MSC/SRA will establish a uniform system for numbering preliminary inquiries (i.e., AMC 2001-1). These numbers will be on a calendar year basis and will be used to identify violations reported as part of the Annual Security Status Report.

h. When possible, preliminary inquiries should be conducted by security specialists, regardless of grade, provided the inquiries are conclusive and the findings and recommendations are approved at the Chief of Staff or equivalent level. If a security specialist is not available to conduct the preliminary inquiry, an individual as outlined in paragraph 10-3(a) of the basic regulation will be appointed. Advice and assistance will be rendered by the security manager/security office when necessary.

Page 106, para 10-4, Reporting Results of the Preliminary Inquiry. Add the following at the end of subparagraph b:

Upon completion of the investigation and once administrative or disciplinary action has been rendered, copies of ALL preliminary inquiries, regardless of their conclusion, will be forwarded through command security channels to this HQ, ATTN: AMXMI-SCM (via e-mail, facsimile, or regular mail). Copies of preliminary inquiries of SAPs will be forwarded through command security channels to this HQ, ATTN: AMXMI-SAP (via facsimile or regular mail). Initial notification for SAP-related violations will be within 24 hours. Copies of Preliminary inquiries involving SCI information will be forwarded through SSO channels to this HQ, ATTN: AMXMI-SSO.

Page 108, para 10-8, Additional Investigation. Add the following at the end:

Security managers will establish procedures for the timely and efficient conduct of investigations within their organizations. See Appendix H of this supplement for procedures when further investigation beyond that of a preliminary inquiry is warranted.

Page 108, para 10-9, Unauthorized Absences, Suicides, or Incapacitation. Add the following at the end.

Within three workdays following a suicide or attempted suicide, the cognizant security manager will forward preliminary results of the inquiry to this HQ, ATTN: AMXMI-SCM.

The report will include --

- a. Individual's name and grade/rank.
- a. Level of security clearance.
- c. Frequency of access to classified information.
- d. Frequency with which the individual worked alone with classified materials (including overtime).
- e. Whether or not there appears to be any missing classified documents or whether or not classified material expected to be in the individual's possession can be accounted for.
- f. All other pertinent facts.
- g. This information may be included in the Serious Incident Report (SIR), provided HQ AMC, ATTN: AMXMI-SCM is included as an addressee.

Page 138, Appendix D, para D-2, Responsibilities. Add the following at the end of subparagraph b:

Within AMC, this authority is delegated to the Senior Intelligence Officers (SIOs) of the MSCs and SRAs. SIOs will verify the contractor's need-to-know prior to releasing intelligence information.

The proponent of this supplement is the United States Army Materiel Command. Users are invited to send comments and suggested improvements on DA Form 2028 (Recommended Changes to Publications and Blank Forms) to the Commander, HQ AMC, ATTN: AMXMI-SCM, 5001 Eisenhower Avenue, Alexandria, VA 22333-0001

AMC Suppl 1 to AR 380-5

FOR THE COMMANDER:

OFFICIAL:

RICHARD A. HACK  
Lieutenant General, USA  
Deputy Commanding General

DENNIS A. DAVIS  
Chief, Business Management Division

DISTRIBUTION:

B, H

[katherine.darby@hqda.army.mil](mailto:katherine.darby@hqda.army.mil)

[ssamergedes@hqamc.army.mil](mailto:ssamergedes@hqamc.army.mil)

APPENDIX A

RECOMMENDED FORMAT FOR ANNUAL SECURITY STATUS REPORT

1 January – 31 December \_\_\_\_\_

1. Security violations attributable to reporting activity. (AR 380-5, Chapter 10.)

a. Number of preliminary inquiries/formal investigations initiated for violations attributable to this activity during the reporting period: \_\_\_\_\_.

b. Provide a brief narrative for each inquiry/investigation initiated during the year and identified above. The narratives will be identified by the security violation number assigned pursuant to paragraph 10-3, AMC Suppl 1 to AR 380-5. Indicate highest level of classification involved. If investigation is complete, address findings as to the probability of compromise and possibility of damage to national security. Specify what disciplinary action (if any) was taken against responsible individual(s). If responsible individual(s) have been cited for other security violations during the past two years, identify date(s) and nature of those prior violations.

c. Provide a brief narrative of results of inquiries/investigation which were completed during the year, but were initiated during the prior year.

2. Security awareness. (Report refresher training only. Do not include initial orientations).

a. General Security Education (AR 380-5, Chapter 9).

(1) Number eligible \_\_\_\_\_.

(2) Number trained \_\_\_\_\_.

b. Operations Security (OPSEC) Training (AR 530-1).

(1) Number eligible \_\_\_\_\_.

(2) Number trained \_\_\_\_\_.

c. Subversion and Espionage Directed Against U.S. Army (SAEDA) training (AR 381-12).

(1) Number eligible \_\_\_\_\_.

(2) Number trained: \_\_\_\_\_.

3. TOP SECRET document holdings (COLLATERAL ONLY). Report only those documents maintained under local accountability (paragraph 6-21, basic regulation). Do not include



APPENDIX B

DISTRIBUTION OF SECURITY CLASSIFICATION GUIDES

Copies of each approved Security Classification Guide (less SCI and SAPs) and changes thereto will be distributed (as a minimum) as follows:

Commander  
US Army Materiel Command  
ATTN: AMXMI-SCM  
5001 Eisenhower Avenue  
Alexandria, VA 22333-0001

Chief  
USAMC ITSA Security Support Division  
ATTN: AMXMI-SSD  
Fort McPherson, GA 30330-1074

Director  
Threat Systems Management Office (TSMO)  
ATTN: AMSTI-PMITTS-SB  
Redstone Arsenal, AL 35898-7461

Commander  
US Army Developmental Test Command  
ATTN: CSTE-DTC-IM-I  
315 Longs Corner Road  
Aberdeen Proving Ground, MD 21005-5055

Director  
US Army Materiel Systems Analysis Activity  
ATTN: AMXSY-DDS  
Aberdeen Proving Ground, MD 21005

Commander  
Military Traffic Management Command  
ATTN: MTOP-PRF  
200 Stovall St., Hoffman Bldg. #2  
Alexandria, VA 22332-5000

Commander  
US Army Forces Command  
ATTN: AFLG-FMCC  
Fort McPherson, GA 30330-1062

Commander  
US Army Training and Doctrine Command  
ATTN: ATCD-RP  
Fort Monroe, VA 23651-5000

Commander  
US Army Pacific  
ATTN: APIN-SC  
Fort Shafter, HI 96858

Commander-in-Chief  
USAREUR/7A, ODCSOPS  
Unit 29351  
ATTN: AEAGC-FMD-DE  
APO AE 09014-0030

\*\*\*Addresses for DTIC, DFOISR and ADSPO follow. IAW paragraph 2-18 of the basic regulation, approved Security Classification Guides and their changes will also be forwarded to the following addressees:

Administrator (2 Copies)  
Defense Technical Information Center (DTIC)  
ATTN: DTIC-FDAC  
Fort Belvoir, VA 22060-6218

Director of Freedom of Information and Security Review  
1400 Defense Pentagon, Room 2C757  
Washington, DC 20301-1400

Army Declassification Special Program Office  
4600 North Fairfax Drive  
Suite 101  
Arlington, VA 22203

In accordance with paragraph 2-18(b) of the basic regulation, copies of security classification guides will also be distributed to those commands, contractors, or other activities expected to be derivatively classifying information covered by the guide.

APPENDIX C  
DOE FORM 5631.20

DOE F 5631.20  
(07-90)  
(Formerly DP-277)  
EFG (70-90)

**U.S. DEPARTMENT OF ENERGY  
REQUEST FOR VISIT OR ACCESS APPROVAL  
(Not to be used for temporary or permanent personnel assignments.)**

OMB Control No.  
1910-1800  
Burden Disclosure Statement  
On Reverse of Part 5

**PART "A"**

**To:**

Date:

**From:**

Prepared by:

Symbol:

Telephone No. – Commercial:

**It is requested that the following person(s) be granted visit/access approval:**

FTS:

LAST NAME, FIRST, MIDDLE INITIAL AND SOCIAL SECURITY NUMBER	Check		DATE OF BIRTH	ORGANIZATION	TYPE CLEARANCE	CLEARANCE NO.	DATE OF CLEARANCE
	U.S. CITIZEN	ALIEN					
NAME OF FACILITY(IES TO BE VISITED)				FOR THE INCLUSIVE DATES	DOE Security Official Verifying DOE Clearance		

**FOR THE PURPOSE OF:**

**TO CONFER WITH THE FOLLOWING PERSON(S):**

**SPECIFIC INFORMATION TO WHICH ACCESS IS REQUESTED:**

Access requested to:  
 Restricted Data  Yes  No  
 Other classified info  Yes  No

**Prior arrangements have/have not been made as follows:**

**CERTIFICATION FOR PERSONNEL HAVING DOD CLEARANCE**

This certifies that the person(s) named above needs this access in the performance of duty and that permitting the above access will not endanger the common defense and security.

**Authorized access to Critical Nuclear Weapon Design Information (CNWDI) in Accordance With DoD Directive 5210.2**  Yes  No

\_\_\_\_\_  
Name and Title, Requesting DOD Official

\_\_\_\_\_  
Title, Authorizing DOD Official  
(See DOD Directive 5210.2 and 5210.8)

\_\_\_\_\_  
Signature  
(See AR 380-150; OPNAV 5510.3F; AFR 205-1)

**CERTIFICATION FOR PERSONNEL HAVING DOE CLEARANCE**

This certifies that the person(s) named above needs this access in the performance of duty.

\_\_\_\_\_  
Title

\_\_\_\_\_  
Requesting DOE or Other Government Agencies

**PART "B"**

Approval is granted with limitations indicated below:

\_\_\_\_\_  
Manager of Operations/or Headquarters Division Director

**SEE REVERSE OF PART 5 FOR PRIVACY ACT INFORMATION STATEMENT**

APPENDIX C  
DOE FORM 5631.20 (Reverse Side)

DOE F 5631.20  
(07-90)  
(Formerly DP-277)  
EFG (07-90)

**PRIVACY ACT INFORMATION STATEMENT**

Collection of the information requested is authorized by Section 145 of the Atomic Energy Act of 1954, as amended (PL 83-703, 42 USC 2165). Compliance with this request is voluntary; however, if the information submitted is inadequate or incomplete, approval for your visit to a classified DOE facility, or your access to classified information may be delayed or withheld. The information you furnish will be used by DOE and DOE contractors to control access to classified information and areas.

The social security number is not required for these purposes, but you may voluntarily furnish it to assist us in correct identification.

**BURDEN DISCLOSURE STATEMENT**

Public reporting burden for this collection of information is estimated to average 2.5 minutes per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Office of Information Resources Management Policy, Plans, and Oversight, AD-241.2 – GTN, Paperwork Reduction Project (1910-1800), U.S. Department of Energy, 1000 Independence Avenue, S.W., Washington, DC 20585; and to the Office of Management and Budget (OMB), Paperwork Reduction Project (1910-1800), Washington, D.C. 20503.

DOE P.O. -7675 (REVERSE)

## APPENDIX D

## DA CERTIFYING OFFICIALS

IAW Enclosure 5 (dated 6/7/00) of DoD Directive 5210.2, Access to and Dissemination of Restricted Data (dated 1/12/78), the following officials of the Department of the Army are authorized to certify personnel under their jurisdiction for access to Restricted Data information (to include Critical Nuclear Weapon Design Information) in the possession of employees of the Department of Energy, its contractors and employees of other federal departments or agencies and their contractors.

1. Administrative Assistant to the Secretary of the Army
2. Chief, Administrative Division
3. Director, Executive Communications and Control
4. Director of the Army Staff
5. Commander, U.S. Army Concepts Analysis Agency
6. Commander, U.S. Army Operational Test and Evaluation Command
7. Commander, U.S. Army Center of Military History
8. Deputy Chief of Staff for Personnel
9. Deputy Chief of Staff for Operations and Plans
10. Deputy Chief of Staff for Logistics
11. Assistant Secretary of the Army for Research, Development, and Acquisition
12. Deputy Chief of Staff for Intelligence
13. Commander, National Ground Intelligence Center
14. Commander, U.S. Army Corps of Engineers
15. Commanding General, U.S. Total Army Personnel Center
16. Chief, National Guard Bureau
17. Chief, Army Reserve
18. The Adjutant General
19. The Inspector General
20. Commanding General, U.S. Army Space and Missile Defense Command
21. Commanding General, U.S. Army Materiel Command (AMC)
22. Commander, U.S. Army Operations Support Command
23. Commander, U.S. Army Soldier and Biological Chemical Command
24. Commanding General, U.S. Army Communications-Electronics Command
25. Director, U.S. Army Research Laboratory
26. Commanding General, U.S. Army Aviation and Missile Command
27. Commanding General, U.S. Army Tank-Automotive and Armaments Command
28. Command General, U.S. Army Test and Evaluation Command
29. Command General, U.S. Army White Sands Missile Range
30. Command General, U.S. Army Training and Doctrine Command (TRADOC)
31. Director, TRADOC Systems Analysis Agency, White Sands Missile Range
32. Command General, Forces Command (FORSCOM)
33. Commander, 63d Ordnance Battalion (EOD), Fort Dix, NJ
34. Commander, 79<sup>th</sup> Ordnance Battalion (EOD) Fort Sam Houston, TX
35. Commander, 184<sup>th</sup> Ordnance Battalion (EOD), Fort Gillem, GA
36. Commander, 3d Ordnance Battalion (EOD), Ft. Lewis, WA
37. Commander, U.S. Army Special Operations Command
38. Commanding General, U.S. Army Pacific
39. Commanding General, Eighth U.S. Army
40. Commanding General, U.S. Army Health Services Command
41. Commanding General, U.S. Army Intelligence and Security Command (INSCOM)
42. Commander-in-Chief, U.S. Army Europe and Seventh Army
43. Director, U.S. Army Nuclear and Chemical Agency (USANCA)
44. Commander, U.S. Army Missile and Munitions Center and School
45. Commanding General, U.S. Army Signal Command
46. Chief, Security and Intelligence Office
47. Commander, 5<sup>th</sup> Signal Command
48. Commander, 1108<sup>th</sup> Signal Brigade
49. Commander, 11<sup>th</sup> Signal Brigade
50. Commander 1<sup>st</sup> Signal Brigade
51. Commanding General, U.S. Army Armament Research, Development and Engineering Center
52. Superintendent of the U.S. Military Academy (USMA), West Point, NY
53. Commander, U.S. Army South
54. Commander, Fifth U.S. Army
55. Director, U.S. Army Surety Field Activity
56. Commander, 52d Ordnance Group (EOD), Ft. Gillem, GA

APPENDIX E  
AMC FORM 1663-R-E

<b>REQUEST FOR VISIT AUTHORIZATION</b> <b>AMC SUP 1, AR 380-5</b>		<b>DATE:</b>		
<b>THRU:</b>		<b>TO:</b>		<b>FROM:</b>
Permission is requested for the following named employee(s) to visit your facility as described below:				
<b>LINE NO:</b>	<b>NAME OF VISITOR</b>	<b>DATE AND PLACE OF BIRTH</b>	<b>SSN</b>	<b>CITIZENSHIP</b>
<b>CLASSIFICATION OF INFORMATION TO BE DISCUSSED AND PURPOSE OF VISIT:</b>				
<b>DATES) AND DURATION OF VISIT:</b>				
<b>PERSONS) TO BE VISITED:</b>				
<b>TYPED NAME &amp; TITLE OF REQUESTING OFFICIAL:</b>			<b>SIGNATURE:</b>	
<b>TO BE COMPLETED BY SECURITY OFFICE</b>				
<b>LINE NO:</b>	<b>LEVEL OF CLEARANCE AND ISSUING AUTHORITY</b>			<b>DATE</b>
<b>Unless otherwise notified, the above visit will be considered approved.</b>				
<b>TYPED NAME &amp; TITLE OF SECURITY OFFICER:</b>			<b>SIGNATURE:</b>	
			<b>DATE:</b>	

**DATA REQUIRED BY THE PRIVACY ACT OF 1974  
(5 USC 552a)**

**TITLE OF FORM**  
Request for Visit Information

**PRESCRIBING DIRECTIVE**  
AMC SUP 1, AR 380-5

**1. AUTHORITY**  
Executive Orders 10450 and 10865; Title 10, USC, Section 3012

**2. PRINCIPLE PURPOSE**  
To advise facilities of forthcoming visits of military and civilian personnel.

**3. ROUTINE USES**  
Indicates that a forthcoming visit is authorized and verifies the visitor's level of clearance and Issuing authority. Provides facility being visited with the visitor's name; date and place of birth; Social Security Number; citizenship; classification of Information to be discussed and purpose of visit; date(s) and duration of visit; and person(s) to be visited.

**4. MANDATORY OR VOLUNTARY DISCLOSURE AND EFFECT ON INDIVIDUAL NOT PROVIDING INFORMATION**  
Disclosure of the Information is voluntary. The personal information requested is necessary to preclude unauthorized disclosure of classified defense information. Refusal to provide Information will result in nonadmittance to classified areas and briefings.

APPENDIX F

RECOMMENDED FORMAT FOR REQUESTS FOR EXCEPTIONS TO STORAGE  
REQUIREMENTS

Provide answers to the following items using narrative format, including all pertinent details. Yes or no answers should be used only when data in narrative forms is not applicable. Attach blueprints, drawings, and sketches when possible. Recently conducted physical security surveys may assist in completion of items. Completed reports may be considered For Official Use Only; occasionally, classification may be warranted.

SECTION A - GENERAL

1. Name of facility.

2. Facility location and room(s).

Building number (if any).  
Geographic location.

3. Responsible officer.

Alternate.  
Telephone. (Commercial and Defense Switched Network (DSN)).

4. Type of facility.

a. Class A Vault.

b. Class B Vault.

c. Class C Vault.

d. Alarmed area.

e. Total square feet facility occupies.

f. Kind and classification of material to be protected (documents, hardware, magnetic media, etc.).

g. Duty hours \_\_\_\_\_ to \_\_\_\_\_, number of days per week \_\_\_\_\_.

h. Construction/modification is complete (yes) (no), anticipated date of completion is \_\_\_\_\_.

SECTION B - PERIPHERAL SECURITY

5. Description of surrounding area outside of building.

- a. Fence.
- b. Fence lighting.
- c. Fence guards.
- d. Relationship of building to surrounding area.

6. Building.

- a. Construction.
- b. Building access control (continuous or during security hours only).
- c. Guards (military) (civilian).
  - (1) Clearance.
  - (2) Frequency of checks.
  - (3) Communications.
  - (4) Emergency procedures.
  - (5) Reserves.

7. Remarks.

SECTION C - FACILITY SECURITY

8. Access control.

- a. Guards (military) (civilian).
- b. Assigned personnel.
  - (1) Clearances.
  - (2) Communications.
  - (3) Emergency procedures.
  - (4) Reserves.

9. Windows (number and type).
10. Ventilation ducts (number and type).
11. Construction.
  - a. Walls.
  - b. Ceiling.
  - c. Floor.
12. False Ceiling.
  - a. Type (fixed or removable).
  - b. Distance between false and true ceilings.
13. Remarks.

#### SECTION D - DOORS

14. Number of entrances.
15. Type of doors used.
  - a. Vault doors (manufacturer, model number, class).
  - b. Wood (thickness/hollow/solid).
  - c. Wood with metal thickness of both door and metal covering; hollow, solid, metal on both sides).
  - d. Metal (thickness/hollow/honeycomb).
  - e. Frame.
  - f. Other.
16. Number and types of doors for emergency exits.
  - a. Vault door (manufacturer, model number, class).
  - b. Wood (thickness/hollow/solid).

c. Wood with metal (thickness of both door and metal covering; hollow, solid, metal on both sides).

d. Metal (thickness/hollow/honeycomb).

e. Frame.

f. Other.

17. Type of lock (entrance).

a. Combination (manufacturer, model number).

b. Are entrance door (if not a vault door) and/or the access control door equipped with a door closer? Yes \_\_\_\_\_ No \_\_\_\_\_ (if no, why not?)

18. Locks on windows and other openings.

19. Have hinges been properly secured on door opening outward? Yes \_\_\_\_\_ No \_\_\_\_\_  
How?

20. Type of locking device used on emergency exits.

a. Lock (manufacturer, model number).

b. Metal strap or bar (size and thickness).

c. Security deadbolt(s).

d. Panic hardware.

e. Other (describe).

21. Number and types of lock used for emergency exits.

a. Electronic cipher lock (manufacturer, model number).

b. Mechanical cipher lock (manufacturer, model number).

c. Key lock (manufacturer, model number).

d. Electronic release (manufacturer, model number).

e. Guard

f. Other

22. Is combination lock of vault door or locally fabricated door opening into a nonsecure area protected against tampering?

No \_\_\_\_\_ Why not?      Yes \_\_\_\_\_ Why Not?

23. Combination changed by:

24. Combination on file at:

25. Double check system.

26. Remarks.

#### SECTION E - CONTAINERS

27. General Services Administration (GSA) approved, Class \_\_\_\_\_ Quantity of each \_\_\_\_\_.

28. Non-GSA approved, manufacturer, model, type of lock.

29. Open/closed signs.

30. Combination changed by:

31. Combination filed at:

32. Double check system.

33. Remarks.

#### SECTION F - ALARM PROTECTION

In all cases where applicable, give manufacturer and model numbers in answering the following questions.

34. Door protection.

a. Balanced magnetic door switch.

b. Closed circuit television.

c. Heat detector.

d. Lacing.

- e. Capacitance.
  - f. Other.
35. Window protection.
- a. Alarm Tape.
  - b. Switch.
  - c. Capacitance.
  - d. Closed-circuit television.
  - e. Other.
36. Perimeter wall protection:
- a. Vibration detection.
  - b. Lacing.
  - c. Capacitance.
  - d. Other.
37. Interior protection (within the facility, below false ceiling).
- a. Volumetric alarm system.
  - b. Closed circuit television.
  - c. Other.
38. Ventilation and duct protection --
- a. Barriers.
  - b. Breakwire alarms \_\_\_\_\_, duct trap.
  - c. Capacitance.
  - d. Other.
39. Overhead protection (space above false ceiling).

- a. Volumetric alarm system.
  - b. Vibration detection.
  - c. Alarm lacing.
  - d. Other
40. Perimeter (fence) protection.
- a. Fence alarm.
  - b. Capacitance.
  - c. Closed-circuit television.
  - d. Tele-approach.
  - e. Seismic.
  - f. Guards and/or sentry dogs.
41. Transmission line supervision.
- a. Rigid or flexible conduit.
  - b. Low security.
  - c. High security.
  - d. Other.
42. Guard response time for an alarm?
- When last tested?
43. Are all alarms operational?
44. Is emergency/backup power available for the alarm system?
45. Location of alarm annunciator panel.
46. Is the alarm system equipped with a "Remote Test" feature?
47. Are all alarm control unit sensors and associated components equipped with tamper circuits?  
Yes \_\_\_\_\_ No \_\_\_\_\_ Why not?

48. Is tamper circuit operational?

49. Is procedure established for periodic testing of alarms?

50. When last tested?

By whom?

51. Description of test methods.

52. Is the facility located in an area that is subject to burglarious attack and/or mob violence?  
(Describe kind of threat).

53. Provide current assessment of hostile intelligence threat against facility. (Usually obtainable from local supporting military intelligence unit/representative).

## APPENDIX G

### SUGGESTED TOPICS FOR BRIEFINGS

Unauthorized disclosures  
Levels of classification  
Original classification  
Derivative classification  
Challenges to classification  
Effects of open publication  
Classification/declassification instructions  
Marking documents/other items  
Tentative classifications  
Combinations  
Storage/safeguarding (including computer media)  
Care during duty hours  
Violations/compromise - discovery  
Handling NATO, RD, FRD, CNWDI, TOP SECRET  
Telephone line transmission security  
End-of-day checks  
Working papers  
Security classification guides - use  
Visits by contractors  
Working with accredited foreign personnel  
Handcarrying classified material  
Foreign government information  
Meetings and conferences  
Clearance of speeches/papers  
Foreign disclosure program  
Industrial security  
Security classification guides - preparation  
Removal of classified during nonduty hours  
Need-to-know  
FOUO  
Personnel security clearances  
Briefing requirements  
Position sensitivity  
Typing/wordprocessing precautions  
Inventories  
Destruction  
DD Form 254  
Warning notices  
Compilations  
Downgrading documents  
Upgrading classifications  
Reproduction  
Transmission  
Packaging  
Receipts  
Custodial duties  
Effects of open publication  
Intelligence Collection Threat  
Technology Protection  
Protection of Controlled Unclassified Information (CUI)  
Reporting of Derogatory Information  
Reporting Suspicious Activity

SPECIALIZED GROUPS (including engineer, contracting, finance, public affairs, personnel, etc.) are sometimes overlooked in tailoring security topics to their specialized needs. Ensure that briefings for groups such as these are prepared in a similar manner to those for the larger groups addressed above.

## APPENDIX H

## 15-6 PROCEDURES (WHEN FURTHER INVESTIGATION IS WARRANTED)

Part of a preliminary inquiry includes a recommendation on the need for further investigation.

1. Further investigation is authorized only in the event of one of the following:

(a) After the preliminary inquiry finds that an actual compromise did occur or that damage to the national security is probable, provided further investigation would clarify (with reasonable assurance) the cause or causes, responsibility, or compromise aspects of the violation.

(b) When a MACOM commander or Headquarters agency head personally decides it might be useful.

2. If it is determined that further investigation is warranted, such investigation will include the following:

(a) Identification of the source, date, and circumstances of the compromise;

(b) Complete description and classification of each item of classified information compromised;

(c) A thorough search for the classified information;

(d) Identification of any person or procedure responsible for the compromise. Any person so identified shall be apprised of the nature and circumstances of the compromise and be provided an opportunity to reply to the violation charged. If such person does not choose to make a statement, this fact shall be included in the report of investigation;

(e) An analysis and statement of the known or probable damage to the national security that has resulted or may result, and the cause of the loss or compromise; or a statement that compromise did not occur or that there is minimal risk of damage to the national security;

(f) An assessment of the possible advantage to foreign powers resulting from the compromise; and

(g) A compilation of the data in paragraphs a through f above, in a report to the authority ordering the investigation to include an assessment of appropriate corrective, administrative, disciplinary, or legal actions.

3. Under the circumstances in sections 1(a) and 1(b) above, the responsible official will begin proceedings under AR 15-6 or request a higher official in the chain of command to do so.

APPENDIX I

(INSERT ORGANIZATION) POLICY AND PROCEDURES  
FOR PROPER MARKING OF CLASSIFIED AND UNCLASSIFIED MATERIAL  
ON SECURE INTERNET PROTOCOL ROUTER NETWORK (SIPRNET)

1. PURPOSE. To establish policy, procedures and responsibilities for the proper marking of classified and unclassified material created or transmitted on SIPRNET in the (INSERT ORGANIZATION). This is effective upon receipt and will remain in effect until rescinded or superseded by an update to the AMC Suppl 1 to AR 380-5.

2. POLICY. The following procedures for generating/creating documents on SIPRNET systems will be followed to eliminate the possibility of accidental security violations.

3. APPLICABILITY. These procedures apply to all personnel utilizing (INSERT ORGANIZATION) SIPRNET.

4. RESPONSIBILITIES.

a. The Head of each Directorate/Office will ensure their personnel understand and are in compliance with these procedures.

b. All personnel will follow procedures described in paragraph 5 below.

5. PROCEDURES.

a. To ensure the security of classified information, classification markings WILL be applied to the first and last page of an email and its attachments. If the entire message on a secure network is UNCLASSIFIED, it can be marked on its face, top and bottom: "UNCLASSIFIED", and a statement added: "All portions of this message are UNCLASSIFIED." (Under no circumstances will a single line classification marking of this nature be applied to an email containing classified information). All other classified emails will be marked according to chapter 4 of AR 380-5 and this memorandum. Additionally, the SUBJECT line of every email will clearly indicate the classification of the most sensitive, highest level of information contained within the email and its attachments. When forwarding an e-mail, the individual forwarding the e-mail will apply the highest classification markings on the top of his e-mail and ensure the classification is reflected at the bottom of the e-mail on the last page.

b. Chapter 4-4, AR 380-5. Classified and sensitive documents will be marked to show the highest classification/sensitivity of information contained in the document. For documents containing information classified at more than one level, the overall marking will be the highest level. For example, if a document contains some information marked "SECRET" and some information marked "CONFIDENTIAL", the overall marking would be "SECRET." This marking must be conspicuous enough to alert personnel handling the material that it is classified

and must appear in a way that will distinguish it clearly from the text of the document. The overall classification/sensitivity will be conspicuously marked at the top of the e-mail on the first page and at the bottom of the e-mail on the last page. This marking must be in letters larger than those on the rest of the page.

c. Chapter 4-6, AR 380-5. Each classified and/or sensitive document must show, as clearly as possible and feasible, which information is classified and/or sensitive and at what level.

d. Each section, part, paragraph and similar portion of a classified and/or sensitive document will be marked to show the highest level of classification/sensitivity of information it contains.

e. Each portion of the text will be marked with the appropriate abbreviation (“TS” for TOP SECRET, “S” for SECRET, “C” for CONFIDENTIAL, or “U” for UNCLASSIFIED) placed in parentheses immediately before the beginning of the portion.

#### SIPRNET USERS:

E-MAIL on the SIPRNET should be treated the same as any other type of classified document and must be marked as required by AR 380-5.

Appropriate classification markings of SIPRNET e-mail will be applied IAW AR 380-5 and this memorandum. Until an automated solution has been evaluated and approved for use in classification, the individual creating the email will apply markings manually.

All emails transmitted via SIPRNET will include classification markings appropriate to the level and sensitivity contained in the email. This includes unclassified mail.

The following examples of email documents illustrate an:

Example 1 - UNCLASSIFIED E-mail

Example 2 - UNCLASSIFIED E-mail document with UNCLASSIFIED attachments

Example 3 - UNCLASSIFIED E-mail with a SECRET attachment

Example 4 - SECRET E-mail document with declassification instructions.

NOTE: Each example is unclassified, and all markings are for training purposes only.

EXAMPLE 1

(CLASSIFICATION MARKINGS FOR TRAINING PURPOSES ONLY)

Doe, John CIV AMC G2

---

To: gsmart@hqtradoc.smil.mil  
Cc: gijoe@hqamc.smil.mil  
Subject: (U) Proper Marking of UNCLASSIFIED SIPRNET E-mail

UNCLASSIFIED

THE CLASSIFICATION OF THIS EMAIL IS UNCLASSIFIED. (The font size of "UNCLASSIFIED" classification should be at least 14 PITCH)

1. The purpose of this e-mail message is to illustrate how to mark an e-mail created on SIPRNET that is entirely UNCLASSIFIED.
2. No portion markings for this document are necessary because the entire email is UNCLASSIFIED.

UNCLASSIFIED

(CLASSIFICATION MARKINGS FOR TRAINING PURPOSES ONLY)

EXAMPLE 2

(CLASSIFICATION MARKINGS FOR TRAINING PURPOSES ONLY)

Doe, John CIV AMC G2

---

To: gsmart@hqtradoc.smil.mil  
Cc: gijoe@hqamc.smil.mil  
Subject: (U) Proper Marking of SIPRNET E-mail (UNCLASSIFIED with UNCLASSIFIED ATTACHMENTS)

UNCLASSIFIED

ALL PORTIONS OF THIS E-MAIL ARE UNCLASSIFIED AND ITS ATTACHMENTS ARE UNCLASSIFIED. (The font size of the "UNCLASSIFIED" classification should be at least 14 PITCH)

The purpose of this e-mail is to illustrate how to mark an e-mail message created on SIPRNET that is UNCLASSIFIED with UNCLASSIFIED attachments.



AGENDA.doc

UNCLASSIFIED

(CLASSIFICATION MARKINGS FOR TRAINING PURPOSES ONLY)

EXAMPLE 3

(CLASSIFICATION MARKINGS FOR TRAINING PURPOSES ONLY)

Doe, John CIV AMC G2

---

To: gsmart@hqtradoc.smil.mil  
Cc: gijoe@hqamc.smil.mil  
Subject: (U) Proper Marking of SIPRNET E-mail (UNCLASSIFIED with CLASSIFIED ATTACHMENTS)

SECRET

THE CLASSIFICATION OF THIS E-MAIL IS SECRET, REGRADE UNCLASSIFIED WHEN SEPARATED FROM CLASSIFIED ATTACHMENTS. (The font size of the "SECRET" classification should be at least 14 PITCH)

1. (U) The attached MS Word file is classified SECRET//NOFORN and is the most recent edition of the HQ AMC Terrorism INTSUM.
2. (U) MSC Operations Center, ensure a copy is provided to your command's Senior Intelligence Officer (SIO).
3. (U) All personnel are required to respond back if you receive duplicate e-mails.



AGENDA.doc

REGRADE UNCLASSIFIED WHEN SEPARATED  
FROM CLASSIFIED ATTACHMENTS

SECRET

(CLASSIFICATION MARKINGS FOR TRAINING PURPOSES ONLY)

EXAMPLE 4

(CLASSIFICATION MARKINGS FOR TRAINING PURPOSES ONLY)

Doe, John CIV AMC G2

---

To: gsmart@hqtradoc.smil.mil  
Cc: gijoe@hqamc.smil.mil  
Subject: (U) Proper Marking of SIPRNET E-mail (CLASSIFIED with  
DECLASSIFICATION INSTRUCTIONS)

SECRET

THE CLASSIFICATION OF THIS E-MAIL IS SECRET. (The font size of the "SECRET" classification should be at least 14 PITCH)

1. (U) The purpose of this e-mail message is to illustrate how to mark an e-mail created on SIPRNET with declassification instructions. This is paragraph 1 and contains UNCLASSIFIED information. Therefore, this portion will be marked with the designation "U" in parentheses after the paragraph number.
2. (S) This is paragraph 2 and contains the highest classification for this SIPRNET e-mail, which is SECRET information. Therefore, this portion will be marked with the designation "S" in parentheses after the paragraph number.
3. (C) This is paragraph 3 and contains CONFIDENTIAL information. Therefore, this portion will be marked with the designation "C" in parentheses after the paragraph number.

DERIVED FROM: XYZ Memo, 14 March 1995  
DECLASSIFY ON: Source marked X2  
DATE OF SOURCE: 14 March 1995

SECRET

(CLASSIFICATION MARKINGS FOR TRAINING PURPOSES ONLY)