Security

DEPARTMENT OF THE ARMY INFORMATION SECURITY PROGRAM

SUPPLEMENTATION. Supplementation is prohibited unless prior approval is obtained from the Director of Intelligence, J2, United States Army Forces Command (FORSCOM), ATTN: FCJ2-CIC, Fort McPherson, GA 30330-6000.

SUGGESTED IMPROVEMENTS. The proponent of this supplement is the Directorate of Security (DSEC), III Corps and Fort Hood. Users are invited to send comments and suggested improvements to Commander, III Corps and Fort Hood, ATTN: AFZF-DS-S, Fort Hood, Texas 76544-5056.

AR 380-5, 25 February 1988, as supplemented by FORSCOM Supplement 1, 15 December 1988, is further supplemented as follows:

Paragraph 1-201. Applicability. Add subparagraphs e and f as follows:

e. This supplement applies to all Department of the Army (DA) civilian and military personnel under the jurisdiction of the Commander, III Corps and Fort Hood, major subordinate commands, and tenant organizations for which DSEC provides security services through Interservice Support Agreement (ISSA).

f. This supplement is intended to enforce responsibilities and liabilities associated with the Information Security Program. It does not replace the III Corps and Fort Hood Information Security Program Handbook.

Section 3. Definitions. Add paragraphs 1-348 through 1-350 as follows:

1-348. Open storage. This terms defines classified military information that is authorized by DSEC to be stored in other than GSA approved security containers (for example, vault, strong room, alarm area).

1-349. Major subordinate commands. Refers to FORSCOM divisional and nondivisional units stationed at Fort Hood.

1-350. Tenant activities. Refers to FORSCOM and other major Army command (MACOM) activities providing services on Fort Hood not part of a major subordinate command.

Paragraph 1-600c2(c). Original classification authority. Add the following after the fourth sentence.

Only the Commander, III Corps and Fort Hood, has original classification authority up to and including the Secret level. Send requests for original classification authority through channels to Commander, III Corps and Fort Hood, ATTN: AFZF-DS-S.

Paragraph 1-601. Derivative classification responsibility. Add subparagraph e:

e. Coordinate with the appropriate Top Secret control officer (TSCO) for accountability prior to creating or storing any Top Secret documents created through derivative classification authority.

Paragraph 2-102b. Classification planning. Add the following:

Coordinate security requirements with the Commander, III Corps and Fort Hood, ATTN: AFZF-DS-S.

Paragraph 2-103b. Challenges to classification. Add the following:

Send requests for formal challenges through command channels to Commander, III Corps and Fort Hood, ATTN: AFZF-DS-S.

Paragraph 2-405a. Distribution of classification guides. Add the following:

Send four copies of each classification guide originated by FORSCOM units at Fort Hood through channels to Commander, III Corps and Fort Hood, ATTN: AFZF-DS-S. DSEC will retain one copy on file and send the other three to HQDA.

Paragraph 2-501. Procedures. Add the following after the second sentence:

Refer conflicts that cannot be resolved at the operating level through command channels to Commander, III Corps and Fort Hood, ATTN: AFZF-DS-S.

Paragraph 2-600c. Procedures. Add the following:

Request original classification authority at the Confidential and Secret level through command channels from Commander, III Corps and Fort Hood, ATTN: AFZF-DS-S.

Paragraph 3-304f. Requirements for processing. Add the following:

Send appeals through command channels through Commander, III Corps and Fort Hood, ATTN: AFZF-DS-S and Commander, FORSCOM, ATTN: FCJ2-CIM, to HQDA.

Paragraph 4-100. Designation. Add the following:

FHT Handout 380-X1 (Document Marking Handbook), provides extensive guidance and is available from your security manager.

Paragraph 4-304a. Removable ADP and word processing storage media. Add before the first sentence:

Follow the instructions in AR 380-19, paragraph 2-20, for marking removable automatic data processing (ADP) and word processing storage media.

Paragraph 4-306. Material for training purposes. Add the following:

Use only "real world" classified material and markings in connection with exercise play. Do not use the marking "classified for training only, otherwise unclassified."

Paragraph 5-101. Standards for storage equipment. Add subparagraph c:

c. Do not store classified information in any security container that does not bear a General Services Administration (GSA) approved label. If the label is missing, send a request for certification through command channels to Commander, III Corps and Fort Hood, ATTN: AFZF-DS-S, with the following information:

(1) Brand of container (if known) and number of drawers.

(2) Location (room and building number).

(3) Name and phone number of a point of contact through which a site survey can be arranged.

Paragraph 5-102a. Storage of classified information. Add subparagraph 5:

5. Store Top Secret and COSMIC Top Secret material and documents within Headquarters, III Corps and Fort Hood, in GSA approved security containers in the office of the TSCO or in those accounts approved by the TSCO and DSEC.

Paragraph 5-102a2. Storage of classified information. Add the following:

Send requests through command channels to Commander, III Corps and Fort Hood, ATTN: AFZF-DS-S.

Paragraph 5-102b. Storage of classified information. Add subparagraphs 3 and 4:

3. Send requests for security upgrading on DA Form 4283 (Facilities Engineering Work Request), to comply with the provision of this regulation through channels to Commander, III Corps and Fort Hood, ATTN: AFZF-DS-S, for approval and assignment of a work priority.

4. Do not use vaults or strong rooms for the "open" storage of classified information until they are accredited by DSEC. Send requests for open storage through channels to Commander, III Corps and Fort Hood, ATTN: AFZF-DS-S, with the following information:

(a) A complete description of the facility (for example, room, building, and street).

(b) A general description of the building's physical characteristics (for example, number of floors, material of which constructed).

(c) A general description of the area recommended for open storage and any security upgrading of windows, doors, vents and other openings (also whether it is guarded, alarmed, and so forth).

(d) The types of material that will be openly stored (for example, maps, overlays, and charts) and the highest classification.

(e) A graphic floor plan (does not have to be to scale) showing the open storage area in relationship to the building. If the open storage area is in a multistory building, show only the floor containing the open storage area.

(f) A name and phone number of a point of contact through whom a site survey can be arranged.

Paragraph 5-103. Procurement and phase-in of new storage equipment. Add subparagraph d as follows:

d. The Directorate of Information Management (DOIM) will coordinate all request for new security containers and vault doors with DSEC to ensure that the equipment ordered meets GSA standards.

Paragraph 5-104b1. Designations and combinations. Add the following after the word "Changing":

Only designated and properly cleared individuals from the Directorate of Engineering and Housing (DEH), the Directorate of Logistics (DOL), DSEC, and individuals who have been authorized by their security manager are permitted to change or supervise the change of a combination. The name, signature, and unit or activity of the person making the change will appear in block 9 of the SF 700 (Security Container Information). For changes to combinations of security containers call the DOL Lock Shop at 287-1989/5031. For changes to combinations of vault doors call the DEH Lock Shop at 288-3846.

Paragraph 5-104b1. Designations and combinations. Add subparagraph (h) as follows:

(h) DEH and DOL will require a report of survey in accordance with AR 735-5, chapter 13, for any repair of a lockout to a vault door or security container if they determine that negligence was the cause of the lockout (for example, unauthorized combination change or a failure to properly record and file SF 700).

Paragraph 5-104b3(d). Designations and combinations. Add the following after the third sentence:

Store container combinations as follows:

(1) Store combinations (SF 700, parts 2 and 2A) to other than master containers in your master container.

(2) Send combinations (SF 700, parts 2 and 2A) to your master container to your next higher security manager.

(3) Send combinations (SF 700, parts 2 and 2A) to the master containers for III Corps staff elements, divisional and nondivisional units, and tenant organizations for which security services are provided by ISSA to DOIM, Classified Control Section, for storage. If the master container is located inside a locked vault or strong room, send both combinations.

(4) Send combinations (SF 700, parts 2 and 2A) for master containers for approved Top Secret subaccounts to the III Corps TSCO. Send the combination to the III Corps TSCO master container installation Telecommunications Center (TCC).

(5) Send combinations (SF 700, parts 2 and 2A) for containers storing North Atlantic Treaty Organization (NATO) Secret information within III Corps staff elements to III Corps NATO subregistry and for major subordinate commands, to their servicing NATO control point.

Paragraph 5-105a2. Repair of damaged security containers or vault doors. Add the following at the end of the subparagraph:

Paint the entire container or vault door if the repaired area must be repainted in a finish or color different from the rest of the container or vault door.

Paragraph 5-200a. Responsibilities of custodians. Add the following after subparagraph a:

Appoint document custodians in each area where classified information is stored. The appointment may be in writing, but is not required to be in writing. Custodians must possess a security clearance equal to the level of material under their control. Custodians should have control of the classified information. You may appoint more than one document custodian for a security container. Do not appoint administrative personnel as document custodians unless they actually control the material.

Paragraph 5-200c. Responsibilities of custodians. Add the following after the fourth sentence:

Send requests through command channels to Commander, III Corps and Fort Hood, ATTN: AFZF-DS-S.

Paragraph 5-202. End-of-day security checks. Add subparagraphs i through l as follows:

i. Do not designate staff duty personnel to perform *initial* end-of-day security checks. Staff duty personnel may be required to perform *additional* checks. If so designated, staff duty personnel will make the first check as soon as possible after the end of the workday.

j. Do the following in areas (desks or workstations) where classified information is stored or processed:

(1) Number each desk or workstation.

(2) Clear each desk or workstation of correspondence, working papers, reports, staff studies, For Official Use Only (FOUO) documents, and so forth, at the end of each duty day. Send requests for waivers of this requirement to Commander, III Corps and Fort Hood, ATTN: AFZF-DS-S.

(3) Lock desks and workstations and establish key control. You may exempt desks or workstations that have unserviceable locks or lost keys from the locking requirement provided you clean them off.

k. Record all openings, closings, checks, and guard checks in the appropriate columns of the SF 702 (Security Container Check Sheet). Individuals opening a security container are responsible for closing it. Individuals closing a security container are responsible for seeing that someone else checks it immediately. This applies to multiple openings and closings during a given day. Designate personnel in writing to perform end-of-day security checks. Record this check in

the GUARD CHECK column of the SF 702. Record additional after-duty-hours checks by staff duty personnel, if applicable, in the GUARD CHECK column. The same individual cannot CLOSE and CHECK, or CHECK and GUARD CHECK a security container. On days the area is occupied, but the security container is not opened, make sure the CHECKED BY and GUARD CHECK duties are performed by different individuals and recorded on the SF 702.

l. Record the numbers of security containers and desks or workstations on the SF 701 (Activity Security Checklist). In areas where there are large numbers of containers, desks, and workstations to be included in end-of-day security check procedures, you may list them on multiple SFs 701 and designate an individual for each area.

Paragraph 5-204. Telecommunications conversations. Add the following:

Affix DD Form 2056 (Telephone Monitoring Notification Decal) to standard Army telephones, including Secure Telephone Units (STUs), and on nonstandard telephones when they are connected in any way to commercial, Defense Switched Network (DSN), or other systems not wholly owned, leased, or contracted by the Army.

Paragraph 5-205c3. Security of meetings and conferences. Add after second sentence:

Send requests through command channels to Commander, III Corps and Fort Hood, ATTN: AFZF-DS-S, in sufficient time for it to be forwarded through FORSCOM and arrive at HQDA at least 120 days prior to the planned conference date.

Paragraph 5-205d2(c) (3). Security of meetings and conferences. Add the following:

Send requests through command channels to Commander, III Corps and Fort Hood, ATTN: AFZF-DS-S.

Paragraph 5-205d2(f) (2). Security of meetings and conferences. Add the following:

Send requests through command channels to Commander, III Corps and Fort Hood, ATTN: AFZF-DS-S.

Paragraph 5-205g1. Security of meetings and conferences. Add the following after the fifth sentence:

Send requests through command channels to Commander, III Corps and Fort Hood, ATTN: AFZF-DS-S.

Paragraph 5-205g2. Security of meetings and conferences. Add the following:

Send requests through command channels to Commander, III Corps and Fort Hood, ATTN: AFZF-DS-S.

Paragraph 5-206. Safeguarding of U.S. classified information located in foreign countries. Add the following after the fourth sentence:

Send requests through command channels to Commander, III Corps and Fort Hood, ATTN: AFZF-DS-S.

Paragraph 5-300g1. Policy. Add the following:

Entry/Exit inspections on Fort Hood are conducted in accordance with Fort Hood Regulation 380-5.

Paragraph 5-302b2. Inspection procedures and identification. Add the following:

The following applies to DD Form 2501 (Courier Authorization Cards) on Fort Hood:

(a) DD Forms 2501 are issued by Fort Hood security managers and limit carrying classified information on the installation (this does allow carrying information to and from and in and around West Fort Hood and North Fort Hood).

b. It does NOT replace courier authorization procedures in chapter 8 of this regulation.

c. Only security managers may issue DD Form 2501. Commanders or III Corps staff element chiefs may sign DD Forms 2501 issued to security managers.

d. Enter an expiration date not to exceed 1 year from date of issue.

Paragraph 6-102a. Responsibility of discoverer. Add the following:

The security manager, commanding officer, or head of the activity will notify DSEC as soon as possible.

Paragraph 6-103. Preliminary inquiry. Add the following after the first sentence:

DSEC has administrative responsibility for the processing of preliminary inquiries and proper reporting to FORSCOM and HQDA.

Paragraph 7-300a. Top Secret information. Add the following after the words "Control Officers":

Store Top Secret and COSMIC Top Secret information only in the TSCO, III Corps and Fort Hood, or in those Top Secret Subaccounts approved by the TSCO and DSEC.

Paragraph 7-305c. Restraint on Reproduction. Add the following:

DSEC is responsible for accrediting equipment used for the reproduction of classified information. Send requests through channels to Commander, III Corps and Fort Hood, ATTN: AFZF-DS-S. Include the brand name, model number, serial number, location, a unit point of contact and phone number, a description of the security afforded the machine during duty hours, and after-duty hours. Reproduction equipment not accredited to reproduce classified information will bear a warning notice to this effect. FORSCOM Poster 93-R (Warning Notice) will be used for this purpose.

Paragraph 8-102a. Secret information. Add the following:

1. The Installation DOIM Classified Control Office is responsible for mailing and distributing classified material for III Corps staff elements and nondivisional and tenant units that do not have classified mailing authorization except for the type of classified information listed below. Prepare the information listed below for mailing or distribution in accordance with chapter 8 and take it directly to the DOIM Mail and Distribution Section for mailing. Tell them the level of classification of the contents for proper classification of mail.

(a) Classified information covered by Special Access Programs (SAP) identified in chapter 12.

(b) Classified information containing special markings in accordance with paragraph 4-503 and AR 381-1.

(c) Classified information that has special dissemination restrictions in accordance with paragraph 4-505.

(d) Classified Subversion and Espionage Directed Against US Army and Deliberate Security Violations (SAEDA) reports requiring limited distribution in accordance with AR 381-12.

(e) Classified information requiring restricted dissemination by other regulations or directives not listed above.

2. NATO classified must be released by the III Corps NATO control officer.

3. Except for the type of information described above, use the following mailing procedures:

(a) III Corps and Garrison staff elements, nondivisional, and tenant units that do not have classified mailing authorization must provide two opaque envelopes of sufficient size (or a suitable container for bulky material), two completed DA Labels 18 (Mailing Label), and, if a receipt is required, 3 copies of DA Form 3964 (Classified Document Accountability Record) properly completed. **Do not attach DA labels to the envelopes or container.**

(b) Divisional and nondivisional units that have classified mailing authorization must prepare the material for mailing in accordance with chapter 8 and take it directly to the DOIM Mail and Distribution Section for mailing. Mark the level of classification of the contents for proper use and classification of mail.

4. Attach appropriate cover sheet to interpost distribution material. Place an OF 41 (Routing and Transmittal Slip) beneath the classified cover sheet. Do not, under any circumstances, place classified information in shotgun envelops. Take the material to the DOIM Classified Control Office for distribution.

Paragraph 8-103a. Confidential information. Add the following:

Mail Confidential information through DOIM as described in paragraph 8-102a above.

Paragraph 8-300. General restrictions. Add the following to subparagraph e:

Retain a copy of this list in the unit or activity until the classified information has reached its final destination. If an entire unit or activity is involved in the movement of classified information, send this listing to the next higher headquarters with instruction to retain until the classified information has reached its final destination. In the event of loss, compromise, or a mass casualty accident, this list will serve to identify the material requiring re-evaluation in accordance with paragraph 2-210.

Paragraph 8-302d(1)c. Procedures for handcarrying classified information aboard commercial passenger aircraft. Add the following as the first sentence:

DSEC will issue courier authorization letters for III Corps staff, nondivisional, and tenant units that do not have authority to approve travel orders.

Paragraph 8-303b. Authority to approve escort or handcarry of classified information aboard commercial passenger aircraft. Add subparagraph 5 as follows:

5. DSEC will obtain FORSCOM approval for outside continental United States (OCONUS) travel by commercial aircraft. Provide the information at paragraph 8-303b4 above, through channels to DSEC.

Paragraph 9-101. Methods of destruction. Add the following:

Obtain administrative approval on purchase requests from DSEC prior to the purchase of any classified destruction equipment, including office shredders. DOL will not process a request for the purchase of this type equipment that does not contain administrative approval of DSEC.

Paragraph 13-304a. Field program management. Add the following after the second sentence:

The DSEC serves as the installation security manager. In this capacity, the DSEC establishes, implements, and supervises security policy, and provides guidance on policy regarding security matters and procedures within the command.

Paragraph 13-304a1(b). Field program management. Add the following:

Establish these procedures in writing and include procedures for field exercises if applicable. If the unit or activity has a combat mission, include tactical security procedures.

Paragraph 13-304c1(h). Field program management. Add the following:

DSEC will conduct an announced security inspection every 18 months of III Corps staff elements and the office of the security manager of major subordinate commands. Major subordinate commands will conduct an announced security inspection at least every 18 months of their subordinate staff elements and units, record the results using the format at appendix U, and send a copy of each inspection to DSEC. DSEC will conduct an unannounced after-duty-hours security

inspection of each III Corps staff element located in building 1001 at least every 18 months. III Corps staff elements not located in building 1001 and major subordinate commands are responsible for conducting their own after-duty-hours inspections, recording the results using the format at appendix V, and keeping a copy of the latest inspection report on file. Security managers at every level are responsible for conducting periodic spot checks during duty hours, recording the results using the format at appendix V, and keeping a copy of the latest inspection report on file.

Paragraph 13-400. Information requirements. Add the following:

The III Corps and Fort Hood Command Group Security Manager will maintain fiscal year records sufficient to document all original classification decisions made by the Commander, III Corps and Fort Hood, and will submit same on SF 311 (Agency Information Security Program Data) to DSEC annually by 1 October.

The proponent for this supplement is the Directorate of Security.

FOR THE COMMANDER:

HEADQUARTERS III CORPS AND FORT HOOD — Official — FORT HOOD, TEXAS

WILLIAM A. WEST
Brigadier General, USA
Chief of Staff

STEPHEN J. BERTOCCHI
LTC, SC
DOIM

DISTRIBUTION
IAW FH Form 1853, B
PLUS: IM-Pubs (100)
IM-AO (5)
IM-ARL (1)
DS-S (25)