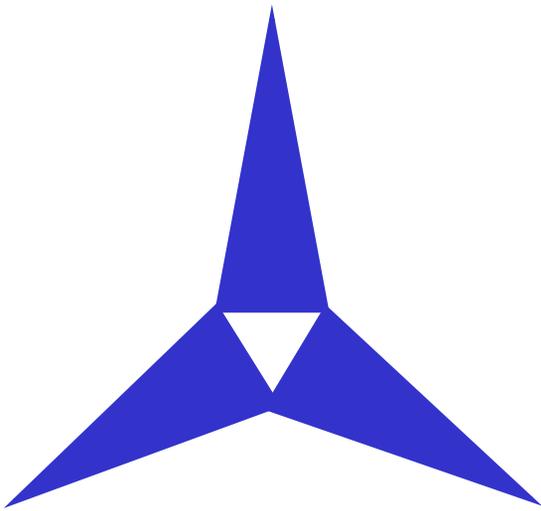


Fort Hood Pamphlet 25-5

October 15, 2001



Information Management: Sustaining Base

**Fort Hood Directorate of
Information Management:
Basic Policies and Procedures**

Headquarters,
III Corps and Fort Hood
Fort Hood, Texas

Information Management
Information Management: Sustaining Base
Fort Hood Directorate of Information Management:
Basic Policies and Procedures

History. This supersedes III Corps and Fort Hood Pamphlet 25-5 dated 15 May 2000.

Summary. This pamphlet assists the Information Management Officer (IMO) in accomplishing his mission. References to brand names or trademarks do not imply product endorsement by the government. Use of masculine gender also includes feminine gender.

Applicability. This pamphlet applies to units assigned or attached to Fort Hood.

Supplementation. Users may not supplement this pamphlet without the approval of the Directorate of Information Management (DOIM).

Changes. Changes to this pamphlet are not official unless authenticated by the DOIM.

Suggested Improvements. The proponent of this pamphlet is the DOIM. Send comments and suggested improvements to: Directorate of Information Management, ATTN: AFZF-IM, Fort Hood, Texas 76544-5056.

FOR THE COMMANDER:

STEPHEM M. SPEAKES
Brigadier General, USA
Chief of Staff

Official:



JOSEPH J. FRAZIER
LTC, SC
DOIM

DISTRIBUTION:
IAW FHT FORM 1853: S

Contents

Chapter 1 – Introduction	8
Section I – General.....	8
Purpose, 1-1.....	8
References, 1-2.....	8
Abbreviations and terms, 1-3	8
Use, 1-4.....	8
Information management support council (IMSC), 1-5	9
Section II – The Directorate of Information Management (DOIM)	9
Mission, 1-6.....	9
Organization, 1-7.....	9
Section III – The Information Management Officer (IMO).....	9
IMO Duties and Responsibilities, 1-8	9

Suggested Information Management Officer (IMO) Job Descriptions, 1-9 10

Section IV – Telephone Control Officer (TCO) 11

 TCO Duties and Responsibilities, 1-10..... 11

Section V — Official Use of Information Management Area (IMA) Assets..... 11

 General, 1-11 11

 References, 1-12..... 11

 Interpretations, 1-13 12

Chapter – 2 Plans and Projects 13

 Section I – Information Mission Area (IMA) Projects 13

 Information Mission Area (IMA) Project Management, 2-1 13

 Building Renovation and Unit Relocation, 2-2 13

 Military Construction Army (MCA) Projects, 2-3 14

 Section II – Automation Plan 14

 Purpose, 2-4..... 14

 Scope, 2-5..... 14

 Objective, 2-6 14

 Local Area Network (LAN) Support, 2-7 15

Chapter 3 – Automation..... 15

 Section I – Automation Overview 15

 The Personal Computer (PC), 3-1 15

 Software, 3-2..... 15

 Hardware, 3-3 15

 File Sharing, 3-4 15

 Servers, 3-5..... 16

 Systems, 3-6 16

 Local Area Networks (LAN), 3-7..... 16

 Installation Local Area Network (ILAN) Support, 3-8 17

 Electronic Mail (Email), 3-9 17

 Dynamic Host Configuration Protocol (DHCP), 3-10 17

 Wide Area Networks (WANS), 3-11 17

 Packet Switching, 3-12..... 17

 Addressing, 3-13 17

 Section II – Army Applications Systems 18

 Introduction, 3-14 18

 Data Processing Systems, 3-15 18

 Installation Support Modules (ISM), 3-16 18

 Army Standard Information Management Systems (ASIMS), 3-17 18

 Section III – Automated Data Networks..... 18

 Fort Hood Installation Local Area Network, (ILAN), 3-18..... 18

 Defense Information Systems Network (DISN), 3-20 18

 Internet Connectivity, 3-20 18

 Section IV – Defense Message System (DMS) Local Control Center 19

 Purpose, 3-21..... 19

 Transitioning to Defense Message System (DMS), 3-22..... 19

 Public Key Infrastructure (PKI) – Medium Grade Service (MGS): Secure Email, 3-23..... 19

 Section V – Information Assurance 20

 Information Assurance Security Officer (IASO), 3-24 20

User Identifications (USERIDs) and Password Requests, 3-2520
 Request for ASIMS or ISM Passwords, 3-2621
 Introduction, 3-2721
 ILAN Connectivity, 3-28.....21
 Internet Access, 3-2922
 Terminal Server Access Control System (TSACS), 3-3022
 Technical Assistance, 3-3123
 Section VII – Computer Assistance: Help Desk Support23
 Computer Assistance, 3-3223
 Section VIII – Acquisition and Disposition of Information Mission Area (IMA)
 Assets,23
 Approval Procedures, 3-33.....23
 Procurement, 3-34.....24
 Excess Automated Data Processing (ADP) Equipment, 3-3524
 Section IX – Information Technology (IT) Standards24
 Introduction, 3-3726
 Chapter 4 Telecommunications26
 Section I – Infrastructure26
 Copper Cabling, 4-126
 Fiber Optic Cabling, 4-226
 Digging Permits, 4-3.....25
 Outages, 4-426
 Telephone Switches, 4-5.....26
 Section II – Telephones.....27
 Emergency Situations, 4-627
 Cellular Telephone Service, 4-727
 International Maritime Satellite (INMARSAT), 4-827
 Leased Communications, 4-9.....28
 Ordering Long-Haul Point-to-Point Services, 4-1028
 Ordering Toll Free (1-800/888/877) Services, 4-1130
 Ordering Local Leased Communications Services, 4-12.....32
 Pay Telephone Service, 4-1333
 Telephone Calling Cards, 4-14.....33
 Pagers, 4-15.....34
 Section III – Radio Frequencies34
 Commercial Radio Frequencies, 4-1634
 Chapter 5 – Records Management.....35
 Section I – Headquarters III Corps Distribution Center.....35
 Purpose, 5-1.....35
 Criteria, 5-235
 Hours of Operation, 5-3.....35
 Distribution Addressing, 5-435
 Mail Scheme, 5-535
 Section II – Official Mail35
 Purpose, 5-6.....35
 Criteria, 5-735
 Cut-Off Times/Special Instructions, 5-8.....35

Section III – Freedom of Information Act (FOIA) Program.....36
 Purpose, 5-9.....36
 Criteria, 5-1036
 Response Time, 5-1136
 Procedures, 5-12.....37
 Fees, 5-1337
 Training, 5-1437
 Reports, 5-1537
 Files, 5-1638
 Section IV – Forms Management.....38
 Purpose, 5-17.....38
 Definition, 5-1838
 Forms Manager Support, 5-1938
 Forms Management Officers (FMO) and Forms Management Coordinators
 (FMC), 5-20.....38
 Procedures, 5-21.....39
 Training, 5-2239
 Phantom Corps Library of Electronic Recordkeeping (CLERK), 5-2339
 Section V – Files Management.....39
 Purpose, 5-24.....39
 Definitions, 5-2540
 General, 5-2640
 Selected File Numbers (FORSCOM Form 350-R), 5-2740
 Files Training, 5-28.....41
 Records Holding Area (RHA), 5-2941
 Files, 5-3041
 Electronic Records, 5-3143
 Section VI – Management Information Control.....43
 Purpose, 5-32.....43
 Definitions, 5-3343
 General, 5-3444
 Management Information Control Liaison (MICLOs), 5-3544
 Higher Headquarters Report Control Systems (RCS) Reports, 5-3644
 Fort Hood Report Control Systems (RCS) Reports, 5-3745
 List of Controlled Requirements, 5-3845
 Approval of Management Information Requirements, 5-3945
 Unauthorized Information Requests, 5-40.....46
 Section VII – Army Privacy Act (PA) Program46
 Purpose, 5-41.....46
 Fees, 5-4246
 Training, 5-4346
 Reports, 5-4446
 Files, 5-4546
 Section VIII – III Corps and Fort Hood Office Symbols.....46
 Purpose, 5-46.....46
 Criteria, 5-4747
 Procedures, 5-48.....47

Chapter 6 Printing.....	47
Section I – III Corps and Fort Hood Printing Program	47
Purpose, 6-1.....	47
General Information, 6-2	47
Procedures, 6-3.....	48
Satellite Facilities, 6-4	48
Reports, 6-5	48
Files, 6-6	48
Sections II – III Corps and Fort Hood Office Copier Management Program.....	49
Purpose, 6-7.....	49
Criteria, 6-8	49
Procedures, 6-9.....	49
Training, 6-10	49
Reports, 6-11	49
Relocation, 6-12.....	50
Maintenance, 6-13	50
Files, 6-14	50
Fiscal Year Copier Plan, 6-15	50
Chapter 7 – Command Administrative Publications.....	50
Section I – III Corps and Fort Hood Command Administrative Publications.....	50
Purpose, 7-1.....	50
Background Information, 7-2	50
Procedures, 7-3.....	51
Caltrop Bulletin, 7-4.....	51
Section II – Installation Publications Stockroom.....	51
General Information, 7-5	52
Procedures, 7-6.....	52
Requesting Accountable and Sensitive Forms, 7-7.....	52
Establishing Accounts, 7-8	52
Publications Management Training, 7-9.....	53
Phantom Corps Library of Electronic Recordkeeping (CLERK), 7-10	53
 List of Appendixes	
A – References.....	54
B – Points of Contact (POCs).....	59
C – Capability Request (CAPR) Formats	61
D – Defense Messaging System (DMS) Registration and Use Guidelines	63
E – Information Technology (IT) Standards.....	70
F – Information Technology (IT) Maintenance and Troubleshooting	71
G – Excess Automated Data Processing (ADP) Equipment.....	73
H – Installation Local Area Network (ILAN)	77
I – Internet	74
J – Telephone Work Order Procedures	74
K – Dynamic Host Configuration Protocol (DHCP) Configuration.....	75
L – Open Database Connectivity (ODBC)	79
M – Digital Rules of Engagement (DROE)	82
N – Terminal Server Access Controller System (TSACS).....	83

List of Appendixes (continued)

O – Information Assurance (IA)90
 P – Information Mission Area (IMA) Training96
 Q – Directorate of Information Management (DOIM) Proxy Server97
 R – Leased Communications Lead Times 101
 S – Shared Files and Shared Directories 102
 T – *Bits and Bytes* Newsletter 102
 U – Public Key Infrastructure (PKI) – Medium Grade Service (MGS) 103

Figures List

3-1. Client TSACS application form25
 3-2. TSACS request form 25
 3-3. TSACS request 26
 C-1. Sample Capability Request (CAPR) 62
 J-1. Sample FHT Form 105-X1-1 (Communications Service Request)77
 N-1. Dial up networking icon 83
 N-2. Make new connection 83
 N-3. Name the connection 84
 N-4. Telephone number and country code 84
 N-5. Complete dial up networking 85
 N-6. Dial up networking properties 85
 N-7. Terminal Server dialog box 86
 N-8. Server Types 86
 N-9. TCP/IP Settings 86
 N-10. Selecting TSACS icon 87
 N-11. Connecting to the terminal server 87
 N-12. Dialing status 88
 N-13. Password verification 88
 N-14. Enter your ILAN password 88
 N-15. Connection established 89
 O-1. Sample Incident/Intrusion Checklist 97
 Q-1. Netscape Navigator open preferences 98
 Q-2. Manual proxy configuration 98
 Q-3. Netscape Navigator exceptions 99
 Q-4. Internet options 99
 Q-5. LAN settings 99
 Q-6. Advanced 100
 Q-7. Complete Internet Explorer proxy settings 100

Tables List

B-1. Points of Contact (POCs)59
 H-1. Required information for account activation 73
 R-1. Leased communications lead times 101

Glossary 110
 Index 123

Chapter 1 Introduction

Section I General

1-1. Purpose

This handbook assists the Information Management Officer (IMO) in accomplishing his mission. This pamphlet is not a Fort Hood regulation. It does incorporate DA, FORSCOM, and Fort Hood Directorate of Information Management (DOIM) policy and directives. DOIM has attempted to distinguish proprietary trademarks by marking references with appropriate symbols. References to brand names or trademarks does not imply product endorsement by the government. Use of masculine gender also includes feminine gender.

1-2. References

Appendix A defines required and related references.

1-3. Abbreviations and terms

The glossary explains abbreviations and terms used in this pamphlet.

1-4. Use

a. This information has been compiled from a wide array of sources into an easy-to-understand format for IMO use. Should this guide conflict with existing directives or policies, refer to AR 25-1 (The Army Information Management) or other appropriate regulations relating to Information Management (IM) as listed in Appendix A for clarification.

b. Typeface conventions in this handbook should make the information easier to use. Special typeface denotes certain actions or information. For example:

(1) Server names, error messages, and required actions are small caps:

N3CDOIMWINS2N (150.XXX.XXX.XXX)

or

From the FILE PULL DOWN MENU select NEW

(2) Text that you must type into a field or write in a form, such as instructions to a computer, web site addresses, or requirements on a telephone service request, appear in a different font so that you can quickly distinguish a required action. We may instruct you to:

Go to the Phantom CLERK web site at <http://pclerk.hood.army.mil>

or

When asked for the DATA SOURCE NAME enter HOODSQL1

(3) The Internet is an ever-changing entity. References to Internet address published in this title are current at publication. For assistance with site address, contact the subject point of contact (POC).

1-5. Information Management Support Council (IMSC)

a. The IMSC is a forum that provides an opportunity for installation IMOs to input and is a dialogue between IMOs and the principal DOIM representative for the various disciplines covered in the Information Mission Area (IMA).

b. The Council will discuss any item submitted by an IMO that is of general interest to The Council or other IMOs. Subjects not of general interest are addressed to IMOs individually.

Section II**The Directorate of Information Management (DOIM)****1-6. Mission**

The Commander of the 114th Signal Battalion is the DOIM for the installation and provides sustaining-base, contingency, and split-base IMA support for the III Corps, Fort Hood tenant organizations, and mobilized or mobilizing units during peacetime, transition to war, and wartime.

1-7. Organization

The DOIM is organized into two divisions:

a. The Operations Division implements all telephone, automation, and Local Control Center (LCC) actions.

b. The Support Division effects all DOIM planning actions and implementation of all printing and publications, records and forms management, and distribution for the installation.

Section III**The Information Management Officer (IMO)****1-8. IMO Duties and Responsibilities**

a. The IMO is the POC and principle advisor to a proponent organization for all information technology (IT) and IM issues. IMOs must be appointed on duty appointment orders that specify the name, rank, telephone number, building number, and office symbol of the IMO and alternate IMO. Send duty appointments to:

Commander, 1114th Signal Battalion
ATTN: AFZF-IM-OD-AB-ST
Fort Hood, TX 76544

b. The duty appointment must be received within 30 days of appointment to ensure continuity of information flow.

c. Basic duties are outlined in paragraphs 1-8(d) through 1-8(g). IMO duties are divided into three categories: hardware support, software support, and administration. IMO duties listed in paragraphs 1-8(d) through 1-8(g) are not all-inclusive and can change with organizational size, requirements, and mission. Only the IMO can coordinate required maintenance actions and submit a trouble ticket with the DOIM Support Team.

d. IMO hardware support responsibilities:

- (1) Identify required automation and communication equipment and features.
- (2) Determine hardware requirements based on proponent mission requirements.
- (3) Assist user during equipment installation.
- (4) Diagnose, identify, and troubleshoot equipment failures.
- (5) Repair equipment when possible (this duty is limited, review paragraph 1-13).
- (6) Perform network system administration in organizations having local or wide area networks.

e. IMO software support responsibilities:

- (1) Evaluate commercial software usability (before buying) based on organizational requirements.
- (2) Provide technical and functional evaluations on proposed non-commercial software to activity managers.
- (3) Install software and application programs.
- (4) Troubleshoot software errors and correct errors when possible.
- (5) Provide organizational end user assistance on back-ups, file maintenance, and other software support.

f. IMO administrative duties:

- (1) Formulate organizational level long and short term automation plans.
- (2) Coordinate organizational long and short term IT requirements and plans with the DOIM.
- (3) Keep a current organizational base-line survey (inventory) of all automation equipment and software to include basic network information (Internet Protocol [IP]) address ranges, gateway configurations, building connectivity and any other configuration settings).
- (4) Develop organizational telecommunication capability requirements (CAPRs).
- (5) Report and arrange for turn-in of all unused, obsolete, or transition equipment and software.
- (6) Ensure automation security measures are adhered to as outlined in Fort Hood Regulation 380-19 (Information Systems Security) and supplemental information assurance vulnerability assessment (IAVAs).
- (7) Maintain accountability of user accounts and number of software licenses distributed to unit.
- (8) Attend DOIM IMSC meetings, IMO, and information assurance (IA) training classes.
- (9) Keep commanders and directors informed concerning all automation related issues and provide advice concerning all automation operations.

g. Other IMO responsibilities:

- (1) May serve as Telephone Control Officer (TCO) (see paragraph 1-10).
- (2) May serve as the Information Assurance Security Officer (IASO).
- (3) May be called to assist family readiness group leaders with their automation needs.

1-9. Suggested Information Management Officer (IMO) Job Descriptions

IMO positions are either full or part time depending on organizational requirements. Job descriptions should be based on AR 25-1 and the duties and responsibilities outlined in paragraph 1-8 of this pamphlet, and tailored to the needs of a specific organization.

Section IV**Telephone Control Officer (TCO)****1-10. Telephone Control Officer (TCO) Duties and Responsibilities**

a. The TCO is the POC and principle advisor to a proponent organization for all telecommunication issues. Paragraphs 1-10b through 1-10c outline basic TCO duties. A TCO and at least one alternate will be appointed for major commands and tenant organizations. Send duty appointments that specify the name, rank, telephone number, building number, Email address and office symbol of the TCO and the alternate to:

Commander, 1114th Signal Battalion
ATTN: AFZF-IM-OD-TSC
Fort Hood, TX 76544

b. The duty appointment must be received within 30 days of appointment to ensure continuity of information flow.

c. The TCO will:

- (1) Validate and process requests for telecommunications equipment and services.
- (2) Provide technical assistance to users in formulating and submitting service requests.
- (3) Maintain control of telephone credit cards issued to the organization.
- (4) Maintain an accurate inventory of cellular telephones and pagers assigned to the organization.
- (5) Maintain a complete list of all long-haul and local data circuits belonging to the organization.
- (6) Review and validate telephone bills to control abuse of government telecommunication assets.
- (7) Issue telephone control numbers to authorized users.
- (8) Update the organizations telephone directory by keeping the DOIM telephone directory clerk informed when telephone numbers change and when an assigned position for a telephone number is changed.
- (9) Maintain a current telephone listing for the organization, containing telephone number, class of service, and directory listing.
- (10) Monitor active telephone work orders.

Section V**Official Use of Information Management Area (IMA) Assets****1-11. General**

IMA assets include telephones with all associated connections, computers including both hardware and software, the Installation Local Area Network (ILAN) with all associated hardware, software, and connections, photocopiers, facsimile machines, and etc.

1-12. References

- a. III Corps and Fort Hood Policy Letters.
- b. The Standards of Ethical Conduct for the Executive Branch, 5 CFR 2635, Sec. 2635.504, Use of Government Property.

- c. 5 CFR 2635, Sec. 2635.705, Use of Official Time.
- d. AR 25-1.
- e. DA Pamphlet 25-1-1, Installation Information Management Services.
- f. III Corps and Fort Hood Regulation 380-19 Security Policy for Information Systems (IS) and Information Local Area Network (ILAN)..

1-13. Interpretations

a. Telephones. Guidance for health, morale and welfare (HMW) calls for deployed personnel are listed in paragraphs (1) through (3) below:

(1) Deployed personnel are authorized to use the Defense Switched Network (DSN) network to place both official and unofficial (HMW) telephone calls. The definition of each call is as follows:

(a) Official military call: a call that pertains to official military matters, not of a personal nature.

(b) HMW or morale call: a personal call to a family member or spouse for the benefit of the deployed soldier's morale.

(2) Soldiers assigned to Fort Hood and deployed may place HMW calls through the Fort Hood telephone switch providing:

(a) Each soldier is authorized two, 15-minute HMW calls in a 7-day period of time.

(b) Calls must go to a local residence (see paragraph 1-13a(2)(d)). Calls placed to businesses, regardless of whether or not the immediate family member is the person taking the call, will be terminated. Soldiers are authorized one monthly call to their local bank or credit union for purposes of pay inquiry.

(c) Personal business calls cannot be substituted for HMW calls and vice versa.

(d) HMW calls will be placed for soldiers assigned to Fort Hood who live within the local and extended exchange dialing area. All other calls (toll) will not be processed unless the call is "collect" to the distant end or a commercial telephone calling card is used.

(e) DA civilians and government contractor personnel deployed outside continental United States (OCONUS) may place HMW calls through the DSN as described in paragraph 1-13a(1) for military personnel.

(3) There is no limitation placed on the number of calls placed to an official government telephone, i.e., charge of quarters (CQ) desk, orderly room, etc. As such, DOIM recommends that deployed soldiers ask family members to report to the unit at a prearranged time to receive telephone calls. The duration and frequency of HMW calls would be limited only by the unit commander.

(4) Additionally, units with many deployed personnel may request upgrade to their CQ or orderly room telephones to accommodate transfer of HMW calls from the deployed soldier directly to the soldier's local residence, bypassing the installation telephone operator completely (local, non-toll calls only).

(5) An automated calling system for morale calls is available from DSN only by dialing 73-TEXAS (738-3927). This system allows a 15-minute call on Fort Hood, the surrounding local community, or other locations using MCI™, Sprint™, AT&T™, or other pre-paid calling cards. Unless touch-tone dialing is not available, users cannot access the Fort Hood installation telephone operator for assistance (hours of operation are 0730 through 1930 Monday through Friday, and 0730 through 1530 on weekends and holidays, central standard time).

(6) Information listed in 1-13 a. is only applicable for the Fort Hood switchboard. Deployed soldiers are still required to comply with the limitations established at the deployed location.

b. Email. Many units have established special Email addresses for family support groups with the distinct purpose of passing personal mail between deployed personnel and their family members. All active duty members should have an Army Knowledge Online (AKO) account. (Your.name@us.army.mil) to use for personal mail.

Chapter 2 Plans and Projects

Section I Information Mission Area (IMA) Projects

2-1. Information Mission Area (IMA) Project Management

The DOIM Plans Branch provides project management support for all systems and projects at Fort Hood or its sub-installations. Coordinate requests for IMA support, equipment or services associated with a new system with the DOIM Plans Branch.

2-2. Building Renovation and Unit Relocation

a. Coordinate moves with the DOIM before building renovation or unit relocation. *Do not assume anything.* The Plans Branch can assist in identifying information systems and equipment that require upgrade or relocation. Included are telephone, radio, office copier, and automation systems.

b. Telephone Service. Telephone line service (moves, installations, de-installations, and changes to required capabilities) must be received at the Telephone Service Center on telephone work orders at least 2 weeks before the date an action is required. Forward work orders through the unit TCO to the Telephone Service Center. Appendix K details how to complete telephone work orders. The following information is critical to the review and approval process of all telephone movements:

(1) The POC(s), including name, rank, title, unit, and telephone number of the person with access to the area. Provide name of an alternate POC who is most knowledgeable concerning the requirements. Approval of movement must be established before transfer of telephone service.

(2) A floor plan showing locations and phone numbers.

(3) The start and end dates of movement.

(4) A completed telephone work order for each telephone number requiring action.

c. Dedicated circuits. Requirements for data circuit moves must be received by the Telephone Service Center on a FHT Form 105-X1-2 (Data Communications Service Request) at least 2 weeks before the requested movement date. (See paragraphs 4-11 and 4-12 for explanations of leased communications. The following information is critical to the review and approval process of all data circuit relocation:

(1) The POC, including the name, rank, title, unit, and telephone number.

(2) A floor plan showing locations and phone numbers.

(3) A complete circuit description including circuit identifier.

(4) New route of circuit (if known).

d. Installation Support Modules (ISM). Requests for new equipment or relocation of existing equipment are made in memorandum format to the DOIM ISM coordinator. Paragraph 3-17 discusses ISMs.

e. Cables and termination boxes. DOIM must approve cutting or relocating copper or fiber cables, or associated termination boxes (junction boxes) before work is performed. Without

prior approval, vital communication links may be lost which could jeopardize personnel or adversely affect unit and activity missions.

f. Other electronic IMA devices. The Plans Branch must concur with and determine the impact of dismantling or relocating any other electronic IMA devices.

2-3. Military Construction Army (MCA) Projects

MCA projects involve newly built structures, not renovated buildings. The DOIM Plans Branch provides cost estimates for information systems associated with MCA projects. Therefore, users are encouraged to coordinate projected requirements early in the planning phase.

Section II Automation Plan

2-4. Purpose

This pamphlet provides an overview of Fort Hood's automation architecture (AA) for information processing, data transport and the human-computer interface according to AR 25-1. Chapter 3 of this pamphlet provides an overview of automation.

2-5. Scope

An AA ensures compatibility between tactical, strategic, and sustaining base IMA systems. This architecture relies heavily upon established commercial standards and is based upon Joint Technical Architecture (JTA). AA is a living architecture that is updated by the DOIM as needed and is used in developing automation requirements.

2-6. Objective

a. New technologies are emerging and will significantly affect the future of information management within the III Corps and Fort Hood area of responsibility. Standard Army Management Information Systems (STAMIS) and ISM will be the primary means of providing automation systems support to III Corps and Fort Hood.

b. Automation plans should use III Corps standard operating systems and the ILAN when possible (see Chapter 4). PCs with compatible operating systems will be integrated with the systems and used in a client-server environment. PCs will download information from centralized databases. ILAN, Integrated Service Digital Network (ISDN), and/or Terminal Server Access (TSACS) are the communication standards.

c. Program Manager (PM) fielded systems (i.e., provided by major commands and other agencies) must be integrated into existing communication and automation systems. Functional proponents must include the DOIM in all planning and implementing phases to ensure effective integration of systems.

d. Tactical systems required to send or receive data from any STAMIS or ISM system will interface through the ILAN.

e. Standards in Chapter 3, Section IX, provide maximum flexibility and specific guidelines for acquisition of basic systems. Standardization is necessary to reduce maintenance costs, delays, and ensure compatibility with DOD and III Corps and Fort Hood architecture standards. Remember that purchasing other than standard equipment could result in the absence of maintenance support.

f. ISDN allows digital data communication for computers while simultaneously providing voice communication over a single copper telephone cable pair. ISDN provides users access to digital data lines without the need for special wiring.

g. The ILAN uses Transmission Control Protocol/Internet Protocol (TCP/IP) to access the Non-secure Internet Protocol Network (NIPRNET) through the Defense Information System Network (DISN). Through these networks, the installation has worldwide connectivity.

h. Departmental or building LANs must meet Institute of Electrical and Electronic Engineers (IEEE) 802.3 standards using Category 5E cabling. Integration of departmental LANs into the installation network must be coordinated with the DOIM.

i. Users without direct ILAN connectivity may connect to the ILAN using TSACS.

2-7. Local Area Network (LAN) Support

The DOIM Plans Branch can provide consultant support in the planning stage and advice on standards, conventions, and practices.

Chapter 3 Automation

Section 1 Automation Overview

3-1. The Personal Computer (PC)

The personal computer (PC) may be a desktop or laptop system. The PC is a device that can enhance productivity either at the office or away from the office. A PC contains a processor, internal memory, and storage.

3-2. Software

a. Software may be in two formats: an operating system or user application programs.

b. Operating systems include Windows™ 9X (where X is the version), Windows™ NT, Windows™ 2000, and UNIX/LINUX™, to name a few.

c. User application programs, whether commercial off-the-shelf (COTS) or locally developed and unique programs, focus more on specific functions, such as word processing, spreadsheets, or graphic presentation. Appendix F lists DOIM supported software packages.

3.3 Hardware

a. Hardware consists of the PC and its peripheral equipment. Peripherals include the monitor, keyboard, mouse, printer, scanner, CD-ROM, speakers, and expansion cards. Expansion cards, which are becoming more important, plug into available industry standard architecture (ISA), peripheral control interface (PCI), and accelerated graphics port (AGP) slots and provide additional services such as audio, video, facsimile (fax), and networking features.

b. Appendix F lists hardware standards.

3-4. File sharing

Many computers operate without connections to any other computers. Networking links computers together to share files, share programs, share print services and increase

information availability. Network interface cards (NICs) and MODEMs (modulators, demodulators) are two physical hardware devices that enable computers to electronically share data.

3-5. Servers

Servers perform various services on a network to include: Email, database, file storage, and network service management. These services are accessed through the ILAN and TSACS based upon a client's login ID and password. III Corps and Fort Hood uses Windows™ NT as its primary server operating system.

3-6. Systems

Systems are an accumulation of software and hardware that perform specific data management functions. The Army uses numerous data processing systems to fulfill its various data processing requirements. Some examples are STANFINS-R, SIDPERS III, ISM modules, and Global Command and Control System – Army (GCCS-A). Section II of this chapter discusses such systems.

3-7. Local Area Networks (LAN)

a. Generally, a LAN is a network that allows a group of clients to share information. A LAN is characterized as having network equipment, a server hosting a group of users, and providing some common resources such as files, printers, etc. The DOIM is responsible for the operation and maintenance of the ILAN. Organizations are responsible for maintaining departmental LANs and associated equipment.

b. The Fort Hood ILAN currently consists of Fort Hood users connecting through a mixture of 10Base-T (10mbit shared) and 10/100 switched devices operating across a routed Gigabit fiber backbone. DOIM personnel, or persons authorized by DOIM, may use routers, switches, hubs and/or repeaters to resolve a building's connectivity issues. Fort Hood users may not install their own locally purchased routers, hubs, or switches. Only personnel authorized by DOIM may connect these devices to the Fort Hood ILAN. This avoids violating the 5-4-3 Rule for Ethernet connectivity by having unknown devices connected to the ILAN and exceeding the rule limits. Violators of the 5-4-3 Rule for 10Mb Ethernet LANs is subject to the 5-4-3 Rule of repeater replacement:

(1) The network can only have five segments connected. Only three segments can have 10Base-T users attached to them. The other two segments must be inter-repeater links. If the design of the network violates the rules for placing the number of repeaters, then the timing guideline will not be met and the sending station, having not received an acknowledgement of its sent packet, will resend that packet. Failure to abide by the 5-4-3 Rule can lead to lost packet. Excessive resent packets that can slow network performance and create trouble for applications or simulating a "network down" occurrence.

(2) Violators of the 5-4-3 rule will be disconnected immediately. Reinstatement of connectivity will occur only after compliance with the 5-4-3 Rule for repeater replacement.

c. Web access from off post web sites is limited to properly authenticated HOOD domain users and transpires through proxy servers maintained by the DOIM.

d. Public Law 105-220 was amended by Section 508 of the Workforce Investment Act of 1998. The law was effective 21 June 2001. Section 508 requires that federal employees and members of the public with disabilities be provided with full access to electronic information and data to include the federally operated parts of the World Wide Web (www). Access should be comparable to that provided to individuals without disabilities. FORSCOM world wide web

policy gives detailed information regarding the operation of official DOD websites and is available at: <http://www.forscom.army.mil/info/Fcmemo25-01-2.pdf>.

e. Although penalties for non-compliance with Section 508 are not specified, failure to comply could result in civil liability to the Army. As such, all websites intended to be viewed by the public or DOD civilians must be compliant.

f. **Each page will display the DOD recommended wheelchair logo indicating compliance with Section 508 accessibility requirements**

g. All FORSCOM webmasters, DOIMs, Public Affairs Officers (PAOs), and supervisory personnel must review and become familiar with Section 508 requirements for federal web page design and presentation.

3-8. Installation Local Area Network (ILAN) Support

The DOIM Plans Branch provides advice on standards, conventions, additions, modifications, and architecture for ILAN connectivity.

3-9. Electronic Mail (Email)

a. The Email standard for the installation is Microsoft® Exchange Server. Clients will use Outlook® to access mail stored on installation mail servers. Official correspondence will be transmitted through the Defense Messaging System (DMS) (see section 3-21).

b. Microsoft™ Outlook® Web Access (OWA) provides rich outlook-style client functionality to browser based clients, thereby enabling a wider user base for Exchange® messaging and collaboration applications (Email). Using Microsoft™ Internet Explorer 5.0 (or later) gives web-based client access to Email, calendaring, public folders, and collaborative programs in Microsoft™ Exchange Server. Although Microsoft™ Outlook messaging and collaboration client experience is not necessary to quickly assimilate the OWA interface, the experienced Outlook® users would need minimal training to make use of OWA client functions.

3-10. Dynamic Host Configuration Protocol (DHCP)

Contact the DOIM Support Team for IP addresses, gateway addresses, domain name system (DNS), Windows™ Internet naming service (WINS), or computer names.

3-11. Wide Area Networks (WANs)

WANs available on Fort Hood Internet, NIPRNET, SIPRNET and tactical packet network (TPN).

3-12. Packet Switching

Packet switching is the process taken to disassemble and electronic file (such as an Email note) into manageable chunks of data. These chunks of data, or packets, are combined with the destination address and some control information, then sent to the destination. Since each packet contains the destination IP address, no packet has to follow the path of another. Packets are transmitted over the network then reassembled at the distant end.

3-13. Addressing

Each ILAN device must be assigned the correct address information to ensure delivery to the computer. Much like an envelope is marked with a person's name and street address including the city, state, and zip code allowing postal authorities to route it correctly; the

standard address contains addressing information and some control information that allows packets to be routed.

Section II

Army Applications Systems

3-14. Introduction

DOIM operates and maintains certain automated systems and functions on Fort Hood. Paragraphs 3-15 through 3-17 describe data processing systems. Functional users are those authorized by approving authority to use all or part of a system.

3-15. Data Processing Systems

The DOIM Automation Branch operates Fort Hood's data processing systems. Computer specialists and operator personnel process STAMIS, MACOM standard application systems, and locally developed application systems. Most of these systems are run remotely on Army Standard Information Management Systems (ASIMS) mainframe computers located at Defense Mega-Centers. Defense Mega-Centers are the focal point for the movement of data to and from off-site locations. Managers and functional users are provided timely and accurate processing in support of logistics, financial, and personnel management mission areas.

3-16. Installation Support Modules (ISM)

ISMs standardize automation functions within an installation. The modules developed support soldier processing and other installation support functions. Functional users gain access with a personal computer via the ILAN or using a dial-up modem. The appropriate functional administrator controls access to modules. Requests for new equipment or relocation of existing equipment are made via Email to the DOIM ISM Coordinator (Table B-1).

3-17. Army Standard Information Management Systems (ASIMS)

Functional users gain access to various legacy systems processing at DOD Mega-Centers either using a PC connected to the ILAN or using a dial-up modem. The DOIM IASO administers access, user identification (USERID), passwords and privileges. Requests for new ASIMS connectivity are submitted via the ACofS, RM, to the DOIM IASO.

Section III

Automated Data Networks

3-18. Fort Hood Installation Local Area Network (ILAN)

Appendix I contains ILAN information.

3-19. Defense Information Systems Network (DISN)

DISN connectivity is obtained through the NIPRNET via the ILAN.

3-20. Internet Connectivity

Appendix I contains Internet information.

Section IV**Defense Message System (DMS) Local Control Center (LCC)****3-21. Purpose**

a. The DMS LCC provides record communications support to the Commander, III Corps and Fort Hood and tenant organizations. The LCC allows customers to send Sensitive But Unclassified (SBU) and classified record communications from the desktop to anywhere in the world via the DMS.

b. DMS is the messaging component of the defense information infrastructure (DII). DII provides an integrated, seamless, global information environment for DOD users. DMS consists of the hardware, software, procedures, operating standards, facilities and personnel used to exchange messages electronically throughout DOD and among other authorized users. See Appendix D for more detailed information on DMS procedures and help guides.

3-22. Transitioning to Defense Message System (DMS)

a. During the transitional period from AUTODIN to DMS, certain organizational users may require the capability to send and receive official messages with non-DMS organizational users through AUTODIN. Organizations that require AUTODIN to DMS capability, must establish an electronic association between their DMS distinguished name and their organization's AUTODIN plain language address (PLA).

b. Organizations should determine if this requirement is necessary. If necessary, the organization should identify their PLA (review AUTODIN traffic received or contact the Fort Hood DMS LCC). If a new PLA is required, the LCC will assist the organization in constructing the PLA and submit the request for association. The association process usually takes between 3-5 working days. See Appendix D for further guidelines.

3-23. Public Key Infrastructure (PKI) – Medium Grade Service (MGS): Secure Email

a. PKI is the framework and services that provide the generation, production, distribution, control, tracking and destruction of public key certificates.

b. PKI manages keys and certificates so that an organization can maintain a trustworthy networking environment. PKI enables the use of encryption, digital signature, and access authentication services in a consistent manner across a wide variety of applications.

c. MGS is secure, interoperable COTS Email that uses DOD PKI Class 3 certificates for signature and encryption/decryption.

d. MGS supports DOD's policy (DOD CIO memorandum, subject: Department of Defense (DOD) public key infrastructure (PKI), dated August 12, 2000) that all electronic mail sent within DOD will be digitally signed by October 2002.

e. The Senior Leader Communications Protection Program was implemented to ensure that the Chief of Staff, Army (CSA), U.S. Army General Officers (GO), Senior Executive Service (SES) members, and selected staff can exchange secure Email NLT 31 December 2001 using PKI MGS certificates linked to their Army Knowledge Online (AKO) Email account.

f. The technical approach uses the existing Email infrastructure while allowing the use of an AKO Email address bound to DOD PKI certificates. The solution is designed to minimize impact to the AKO system, maintain the information assurance benefits of the DOD PKI, and institute a "lifetime Email address" while seamlessly impacting end-users. See Appendix V for further guidelines.

Section V Information Assurance

3-24. Information Assurance Security Officer (IASO)

The DOIM IASO validates user requirements for ASIMS and ISM modules and issues passwords.

3-25. User Identification (USERID) and Password Requests

a. USERID and password systems support the minimum requirements of accountability, access control, least privilege and data integrity of computer systems. Security of information systems is vital to the III Corps mission and is the responsibility of every user and systems administrator to comply with current IA policies and guidance. Because passwords are vulnerable to interception or inadvertent disclosure, they are also the weakest of identification and authentication methods. Passwords are only effective when used properly. Inappropriate passwords create common information system vulnerabilities.

b. All user-chosen passwords for computers and networks must not be easily guessed. Words in a dictionary, derivatives of USERIDs, and common character sequences such as 12345678 will not be used. Do not use personal demographic details such as: spouse name, license plate, social security number, pet name, and birthday. User-designated passwords must not be any part of speech. For example, proper names, geographical locations, common acronyms, and slang will not be used. Passwords will not be reused and must be substantially different from passwords that have been previously used.

c. Passwords must be a combination of upper and lower case letters, numbers, and ASCII symbols. All passwords will be a minimum of eight characters long and consist of alphanumeric characters (upper and lower case) with at least two numeric or special characters. To protect against repeated attempts to guess a password and use automated password cracking tools, users will be locked out of their accounts for one hour after three unsuccessful attempts to log on. To unlock an account sooner than the designated lockout period, the user or the user's IASO must come to the DOIM Help Desk and present a picture ID. Telephone or Email requests to unlock an account are not accepted.

d. Organization IASOs ensure personnel receive appropriate computer security training prior to issuance of a USERID or password pair. Users must be briefed on the importance of protecting their USERID and password, reporting any suspicious activity, fraud, waste, and abuse.

e. The display and printing of passwords must be masked, suppressed, or otherwise obscured so that unauthorized personnel cannot observe or recover a password. Passwords should not be written down and left in a place where an unauthorized person might discover them, for example, in a desk drawer, address file or book, taped to the monitor, under the keyboard, in unencrypted files, etc. Passwords will not be given out over the telephone nor will they be transmitted via unclassified or SBU Email systems unless encrypted, such as DMS or SIPRNET.

f. Regardless of the circumstances passwords must never be shared or revealed to anyone other than the authorized user. If users need to share computer resident data, they should use Email or public directories on LAN servers. Password sharing is not authorized. Should additional personnel need access to information assets, they should contact their S6 (or G6) who will provide them the necessary number of accounts to accomplish their mission.

g. Change passwords as follows:

(1) Unclassified and SBU computers: Every 180 days (six months) or more often if the password has been compromised, believed to be compromised, or upon direction from the DOIM.

(2) Classified systems up to SECRET: Every quarter (three months) or more often if the password has been compromised, believed to be compromised, or upon direction from the DOIM.

(3) All vendor-supplied default passwords on new computers must be changed prior to any computer being connected to the ILAN or processing Army information.

h. When password must be obtained from the DOIM, for example, expired password compromised, locked out, etc., Commanders may authorize their IASO or alternate IASO to pick up passwords. The IASO or alternate IASO must have a copy of their appointment orders and a copy of their IA Level 1 certificate of training on file with the DOIM IASO. Users who pick up passwords at the DOIM will have a memorandum signed by their IASO that states the user has been provided appropriate basic user IA training as stated in AR 380-19. Passwords will not be issued if these items are not provided.

i. The DOIM controls access to the ILAN. Organizations who have the capability to establish accounts and issue passwords are required to institute a program that ensures users, IASOs and IMOs receive computer security training prior to ILAN access being granted. Password issue and lock out policy at the local level should be developed consistent with the guidance and all other applicable policy and regulations.

3-26. Request for Army Standard Information Management Systems (ASIMS) or Installation Support Module (ISM) Passwords

a. Requests for account additions and deletions will be sent through the appropriate unit FA or IASO to the DOIM IASO by memorandum, Email, or ASIMS security request form and must include:

(1) The requester's name, organization, building number, and telephone number.

(2) In addition, specific network and application systems access requests must:

(a) For ASIMS: Identify the application system, terminal address if applicable, data owner and unit IASO signatures

(b) For ISM: Identify the module, FA access and FA's signature.

b. Indicate whether the action is for new user account, to update an existing account, or to delete an account. All updates or deletions must indicate the current USERID.

c. Only unit IASOs or FAs are authorized to pick up completed password requests from the DOIM IASO.

Section VI

Information Technology (IT) Troubleshooting and Assistance

3-27. Introduction

Different types of support are available through the DOIM depending on the requirement. All request actions should begin with the unit IMO. Table B-1 lists DOIM POCs.

3-28. ILAN Connectivity

a. If an individual or organization requires access to the Fort Hood ILAN.

b. There is an ILAN connected hub within the building: The IMO or TCO submits a completed FHT Form 105-X1-2 (Data Communications Request) (one per drop) to the

Telephone Service Center with a floor plan designating required location(s) for all required drops.

c. There is no ILAN connected hub within the building: The IMO sends a memorandum or Email outlining the requirements and specifying the number of users to the DOIM Plans Branch.

d. SIPRNET contact III Corps G2 for connectivity details.

3-29. Internet Access

Internet access is authorized per current III Corps and Fort Hood policy DOIM 00-01.

Appendix J outlines information for requesting additional ILAN drops to increase access to the Fort Hood ILAN and the Internet.

3-30. Terminal Server Access Control System (TSACS)

a. TSACS is an official method of accessing the Internet. TSACS is a program manager (PM) maintained, managed and monitored system that is online 24 hours per day, 7 days a week. There are a selected number of installations world-wide that have a registered TSACS terminal server. Terminal servers contain a series of modems which are available first come, first serve. Once these modems are accessed, a TSACS USERID and password authentication is required. "Camping" and "parking" are terms used to describe the act of keeping a modem on-line, but not using the modem for data transmission. The process of "camping" or "parking" is not tolerated. To ensure the continued availability of modems for remaining TSACS users, modems will be automatically reset after a specified period of inactivity.

b. Terminal server communications assets "shall be for official use and authorized purposes only" (JER 2-301). For clarification of these terms, see the III Corps and Fort Hood Command Policy Number 42. Find this policy letter in the Fort Hood Public Folders, III Corps Public Folders, III Corps Command and Staff, III Corps Policies.

c. Requirements for TSACS:

(1) Must have a computer running a Windows™ 95 or a later version of Windows™. Windows™ NT 4.0 Workstation is also supported.

(2) Must demonstrate a need to access Fort Hood ILAN or Internet remotely (i.e., building not wired into the ILAN or anticipating travel within a year's time and require the access for official government use).

(3) Must be in a position that warrants access. Authorized government contractors may request an account subject to the approval of the DOIM.

(4) Must submit the following information for each request: full name, rank or general service (GS) grade, office phone number, office mailing address, Email address, last four digits of social security number, and the reason for needing a TSACS account.

d. Requesting a TSACS account:

(1) Submit a FHT Form 25-X27 (Terminal Server Access Controller System (TSACS) Registration Worksheet) using your Outlook® mail client to TSACS Request--Ft Hood DOIM on the global email directory.

- (2) Fill out the FHT Form 25-X27 entirely and send it:
- c. If the TSACS request form does not work, send an Email with the essential data required figure 3-1 postmaster@hood.army.mil.
 - f. Upon approval, DOIM will forward your account and password to you via Email.
 - g. One month prior to your password expiring you will receive notification from TSACS requiring that you reapply for an account.

3-31. Technical Assistance

The DOIM Support Team provides technical assistance via the Help Desk in determining the nature and appropriate remedy for many types of automation problems. This first level telephonic support is generally successful in either solving the problem on the spot, recommending a course of action, or in obtaining higher level support.

Section VII

Computer Assistance: Help Desk Support

3-32. Computer Assistance

a. The Support Team's Help Desk is the source for a variety of computer support services. Services include assistance in installing and configuring devices; data network management and LAN consultation services, and help in troubleshooting problems and obtaining repair service. The Support Team can provide assistance with many common PC components and COTS software products and approved software products per Appendix F. While the level of knowledge varies between products and devices, many times a Support Team technician can provide useful insight and experience.

b. NCO LEAD computer literacy courses (CALC) sponsored by G3 Education Services Division provides formal classes in computer related subjects and provides computer labs to active duty military and civilians on a space available basis. Classes and enrollment instructions are announced through activity training coordinators.

c. Complete a FHT Form 1556 (Request Authorization Agreement Certification of Training and Reimbursement) before attending computer related training; students will hand carry the FHT Form 1556 to class. The training activity forwards the FHT Form 1556 to the Civilian Personnel Advisory Center for inclusion in the trainee's personnel file.

Section VIII

Acquisition and Disposition of Information Mission Area (IMA) Assets

3-33. Approval Procedures

a. No CAPRs are required for Garrison or base operations (BASOPS) requirements that meet the "No CAPR Rules" outlined in paragraph *b* below:

b. No CAPR rules:

(1) All requisitions must be from the authorized blanket purchase agreements (BPA) or GSA contracts. Exceptions will require a CAPR under the old guidelines approved by DOIM. A list of BPA contracts can be found at the Small Computer Program web site at: <http://pmscp@monmouth.army.mil>.

(2) Due to the impending fielding of the Common Access Card (CAC), all PC systems must be configured with a PCMCIA slot. In addition, no PC system will be purchased that is configured with a LAN card and a modem.

(3) Requisitions for new or replacement PC systems must include the purchase of software not covered by the 10,000 licenses that were purchased on the BPA.

(4) Requisitions for new PC systems that require LAN connections must be coordinated with the DOIM POC as listed in Table B-1.

d. The practice of building a PC system from scratch with parts procured locally in lieu of purchasing a PC system is strictly prohibited. The rationale for this is that such a PC might not fit the installation architecture. In addition, such a practice would lose control of accountability and not stand up to an audit.

f. The 190th Maintenance Company is the proponent for all PC upgrades for installation property book equipment on the installation.

3-34. Procurement

a. Units or activities will prepare procurement packages and process procurement documents through proper channels.

b. International Merchant Purchase Authorization Cards (IMPAC) may be used to purchase IMA assets. Follow guidelines established for the IMPAC credit card.

c. IMA asset leases must follow guidelines established in AR 25-1.

d. All IMA assets should be procured utilizing the contracts managed by the Small Computer Program Manager at Fort Monmouth, New Jersey. According to the directions outlined in DA message, subject: designation of Army point of contact (POC) for government wide agency contracts (GWACS), BPAs, indefinite delivery indefinite quantity (IDIQ) contracts, and Army and DOD enterprise agreements, dated R231312Z JUN 99.

3-35. Excess Automated Data Processing (ADP) Equipment

The DOIM screens all turn-ins of excess ADP equipment request order to determine if the equipment can be used in some other manner on the installation. Most of the excess equipment is antiquated and is quickly approved for turn-in. Savings average about \$50,000 per year. See Appendix G for excess ADP equipment turn-in procedures.

Section IX Information Technology (IT) Standards

3-36. Introduction

The standards outlined in DA Information Infrastructure Architecture (I3A) Design and Implementation Guide (2 March 1999) were established to ensure interoperability of IT resources within DA. By adhering to Army I3A standards established in the I3A Design and Implementation Guide, III Corps and Fort Hood units are assured interconnectivity during peacetime and wartime missions. It must be clearly understood that the DOIM will not support hardware and software that do not conform to established I3A standards established in the I3A Design and Implementation Guide.

Figure 3-1. Sample FHT Form 25-X27 (Terminal Server Access Controller System (TSACS) Registration Worksheet

Terminal Server Access Controller System (TSACS) Registration Worksheet <small>(Users are encouraged to visit the TSACS Home Page at http://www.tsacs.army.mil/ for more information)</small>			
Installation/Organization TriCode:	New:	Renewal:	Delete:
Personal Data Section			
Last Name:	First:	MI:	
Last 4 numbers of SSN:	Rank:	Date of Departure:	
DSN Telephone Numbers Section			
Primary:	Ext:	Fax:	
Commercial Telephone Numbers Section			
Primary:	Ext:	Fax:	
Electronic Mail Address Information Section			
Primary:			
Mailing Address Information Section			
Line 1:			
Line 2:			
Line 3:			
City:		Zip:	
Certification Section			
I certify that the above data is true and correct. I acknowledge and agree that: <ul style="list-style-type: none"> - U.S. Government resources will only be used for the performance of official duties - Data and software and hardware will be protected to the best of my abilities - Proprietary and copyrighted material will be appropriately protected - Security incidents will be reported to the ISSO immediately - Users will only use their individually assigned login ID and will protect passwords and access numbers as FOUO - Users will access only the resources as authorized and will abide by applicable security regulations 			
Applicant: I have read the above and will comply to the best of my ability			
Signature:			
Validation Verification and Authentication Section			
Applicant's Supervisor: This person has an official need for a TSACS logon and password pair to conduct daily business.			
Signature:			
Information Systems Security Officer: This person has the appropriate level of security clearance.			
Signature:			
DOIM/Service Provider Officer: Based on this document and other evidence provided to me, this person has a need for network access.			
Signature:			
NOTES: USER Applications -- Users must complete this form and return it to the service provider (i.e., IMO or DOIM) for their consideration, action and filing as appropriate. Service Providers -- Applicants for service provider accounts must complete this form and fax it to (DSN) 879-6809 (COM) 520-538-6809			

FHT Form 25-X27, March 2002 (DOIM)

Chapter 4 Telecommunications

Section I Infrastructure

4-1. Copper Cabling

Copper cabling is the mainstay to the Fort Hood telecommunications infrastructure. Copper connects almost all locations on the installation. The average age of the copper cabling is 10 years old. Once installed, communication lines should work with little loss of signaling. However, not all buildings are cabled the same. Some have more cable pairs available than others. For instance, when initially constructed, a 50-room barracks required only six cable pairs; but now, the same building may be refurbished into 45 office spaces. The same six-pair cable will not provide adequate support. Before movement into any building on this installation, the TCO should contact the Telephone Service Center to determine if existing cabling will support requirements.

4-2. Fiber Optic Cabling

Fiber is used for trunking between telephone switches and between hubs, routers, and ATMs. At this time, fiber is not connected directly to desktop equipment.

4-3 Digging Permits

a. It is imperative that those who penetrate the ground 12 inches (30.48 centimeters) deep or more by digging, driving stakes or ground rods, etc., get digging permits from the Directorate of Public Works (DPW). Buried lines contain high voltage electrical lines (7200 VAC), high pressure crude oil lines, natural gas lines, water lines, forced sewer mains, and other services. Breaking a line poses a severe, possibly life-threatening danger. Get a digging permit for not later than 10 days before required date.

b. If in the cantonment area (main post Fort Hood, West Fort Hood, North Fort Hood): bring a sketch, map, or drawing representing area to dig to DPW Engineering Plans and Services (see Table B-1). This work-group will mark the area when required. For further information, see digging permit telephone number listed in Table B-1.

c. If in a range area (i.e., field area, training area): bring a 1:50,000 map in an overlay, with the requested dig location marked, to the DPW Environmental Branch.

4-4. Outages

Normally, outages are due to equipment failures, sometimes due to weather, and at times by individuals. The DOIM maintains a list of telephone and data lines that have priority for service restoration and are mission critical. TCOs must submit a work order through the Telephone Service Center to have a telephone or data line designated as mission critical. The Telephone Service Center Chief will scrutinize the requirement.

4-5. Telephone Switches

Fort Hood digital telephone switching systems provide service to over 23,000 lines and process over 25 million calls per month. The main post telephone switch is a Nortel© Digital Meridian™ Switch-100 (DMS100) and the hospital facilities are using a Meridian™ 1 switch.

Both switches are identical to those used by the Public Switched Telephone Network (PSTN) and are capable of supporting technologies like ISDN, ADSL based on availability of unit funding.

Section II Telephones

4-6. Emergency Situations

During emergency situations like hazardous weather (i.e., tornadoes) or national emergency (declaration of war, mobilization, etc.), the DOIM will implement a minimize policy where telephone lines that are not designated mission critical are cut off. If this were not done, the telephone switch would lock out all service; therefore, telephone service must be designated as mission-critical by the TCO on a telephone work order submitted through the Telephone Service Center.

4-7. Cellular Telephone Service

a. All official cellular telephone service for III Corps and Fort Hood must be acquired under the current cellular telephone contract. Contact the POC listed in Table B-1 for more information on the cellular telephone contract. Purchases of equipment and service will be approved by the MSC CofS, G-staff, or directorate. The using activity funds equipment purchases and monthly service charges.

b. Temporary cellular service can be requested from DOIM for specific mission requirements; approval and funding are the same as paragraph 4-7a. Requests for new service or service changes should come via Email to the POC at DOIM. The Email must originate from, or come through, the Email account of an individual authorized to expend the activity's funds, and must be approved as in paragraph 4-7a.

(1) Equipment purchase is the responsibility of the using activity; is considered installation property, and must be handled according to AR 710-2 (Inventory Management Supply Policy Below the Wholesale Level). Accessory items purchased are the responsibility of the owning activity and will be accounted for as installation property.

(2) Some equipment is available at discounted prices through the vendor and can be purchased with an IMPAC card. Any purchase made in conjunction with a service request must be coordinated through the DOIM POC.

c. Maintenance for cellular phones outside the warranty period will be provided by local purchase with the user's IMPAC card.

4-8. International Maritime Satellite (INMARSAT)

a. INMARSAT was originally a ship-to-ship, ship-to-shore satellite communications service. It is now used on land as a global cellular system. INMARSAT airtime is extremely expensive; costs range between \$6.25 to \$12.00 per minute, per terminal. Due to the extremely high cost, INMARSAT should only be used when no other communications are available. Talk time should be kept to a minimum.

b. INMARSAT terminals must be commissioned and established on a government airtime contract. Requests for INMARSAT airtime are processed by the DOIM leased communications coordinator. Terminals should not be used until a government airtime contract is procured. Use of terminals that do not have an airtime contract results in an unauthorized procurement.

c. All requests for INMARSAT airtime must be approved by the unit or activity TCO.

d. Requests for INMARSAT airtime in support of an exercise must also be approved by the III Corps G6 Office.

e. All requests for INMARSAT airtime will include the name, telephone number, and address of the budget POC and a statement that funds are available. Requests submitted from Fort Hood must have approval from an RM budget POC. It is the responsibility of the requestor to coordinate funding. Requests received without proper funding will not be processed.

f. DISA Circular 310-130-1 (Submission of Telecommunications Service Requests) governs the Request for Service (RFS) message format which orders long-haul communications.

g. RFS will be submitted in writing (in memorandum format to the address in paragraph 5-9d) and include:

- (1) The name of the unit or activity requesting the service.
- (2) Brand name and model of the INMARSAT for which airtime is required.
- (3) Justification for ordering the service.
- (4) Terminal identification number of each port (voice, data and fax ports).
- (5) The date service must be operational.
- (6) Get a request for INMARSAT-M terminal time by calling the Leased

Communications Coordinator listed in Table B-1.

4-9. Leased Communications

a. Leased communications are divided into two areas, long-haul communications, which are inter-local access and transport area (LATA), and local communications, which are intra-LATA.

b. Long-haul communications services include point-to-point data circuits, toll-free numbers, telephone calling cards, FTS2001 service, DSN, DISN Video Service-Global (DVS-G) and long-haul carrier service such as AT&T™, MCI™, US Sprint™, etc.

c. Local communications include dial-up telephone lines provided by the Local Exchange Carrier (LEC), point-to-point circuits with both ends within the LEC's serving area.

d. Requests for leased communications will be processed through the DOIM leased communications coordinator at:

DOIM
ATTN: AFZF-IM-SD-PB
Fort Hood, Texas 76544-5056

e. Requirements processed through other channels may result in an unauthorized procurement and disciplinary action. Contact the DOIM lease communications coordinator on all leased communications actions.

4-10. Ordering Long-Haul Point-to-Point Services

a. All requests for leased long-haul communications must be approved by the unit or activity TCO.

b. The III Corps G6 Office must also approve requests for leased long-haul communications that are in support of an exercise. The DOIM/1114th Signal Battalion S3 must review exercise requests for technical accuracy.

c. All requests for leased long-haul communications will include the name, telephone number, and address of the budget POC and a statement that funds are available in writing not verbal. Requests submitted from Fort Hood must have approval from an RM budget POC. It is the responsibility of the requestor to coordinate funding. RFSs received without proper funding will not be processed.

d. DISA Circular 310-130-1 prescribes the procedure pertaining to the RFS message format that orders long-haul communications.

e. Submit RFSs in writing (in memorandum format to the address in paragraph 4-9d) and include:

- (1) The name of the unit or activity requesting the service.
- (2) Type of service required.
- (3) Justification for ordering the service.
- (4) Speed or bandwidth of the circuit.
- (5) The date service must be operational. If request is for a temporary exercise circuit, state both the start and the stop dates.
- (6) If overtime charges for the installation are to be authorized, state the allowable amount.
- (7) State the commercial area code and prefix (see tables 4-1 and 4-2 for a complete listing of local prefixes and area codes) for each end of the circuit.
- (8) Identify the building, room, and floor for each end of the circuit.
- (9) Specify the type of terminal equipment and end device needed at each end of the circuit.
- (10) State whether the circuit will be secure circuit. If circuit is secure, state the type of cryptographic equipment to be installed on the circuit.
- (11) Give interface requirements for each end. This information includes the type of modem equipment with the manufacturer's name and model number, whether the modem will be leased or government furnished equipment (GFE), the circuit timing (synchronous, asynchronous, isochronous), the type of interface requirements (examples: RS-232C, RS-422, RS-423, CCITT V.24, impedance, transmit level, and minimum and maximum receive signal levels).
- (12) Identify POC by name and telephone number for each end of the circuit. Provide a primary and alternate POC. Telephone fax numbers should be shown as both DSN and commercial. POCs should be familiar with the requirements and available to receive telephone calls regarding the action and also act as escorts.
- (13) Mailing address, including office symbol and nine-digit zip code for the POC at each end.
- (14) Provide the message traffic address for the activity at the distant end of the circuit, for the DOIM at the distant end of the circuit, for the funding POC, and for any other parties with a need-to-know what is happening on the circuit.

f. Lead-time is critical when ordering long-haul circuits. Official lead-time is 120 days from the time that a completed, validated RFS is received at DISA Army Telecommunications Directorate (ATD), Fort Huachuca, Arizona. Requests with shorter lead-times will be processed; however, shortened lead-time often requires expedite fees in order to obtain service on time. Lack of lead-time often results in problems with the quality of service received.

g. Coordination is important to successfully installing a long-haul circuit. Information regarding the circuit should be shared with all concerned parties. The DOIM leased

communications coordinator should be contacted anytime there is any progress or change in the status of a long-haul requirement.

h. When a call is received regarding action on a circuit, it is important to record the name of the caller, the name of the company he represents, and a telephone number where he can be reached. It is also important to take written notes on what was said regarding the circuit action.

i. When calling about leased long-haul circuit actions, reference the Telecommunications Service Request (TSR) number. Sample TSR Number: WA06JUNE950123.

k. An in-effect report must be submitted by the DOIM leased communications coordinator when service has been installed and is working. The DOIM leased communications coordinator must be informed by the POC as soon as possible after service has been provided. Information needed includes the date and time service was provided and whether or not the equipment is in-place and working.

Table 4-1. Local dialing prefixes (254 area code)

Location	Commercial Prefix
Fort Hood	254, 286, 287, 288, 618, 532*, 539*
Copperas Cove	518, 542, 547
Killeen	200, 289, 290, 519, 526, 554, 616, 628, 634, 501
Harker Heights	699, 953, 680, 690
Nolanville	698
Kempner	932

*Sprint™ prefixes on Fort Hood

Table 4-2. Conversion from commercial Fort Hood prefix to defense switched network (DSN) prefix

Fort Hood Prefix	Converts to	DSN Prefix
285	⇒	663
286	⇒	566
287	⇒	737
288	⇒	738
618	⇒	259

4-11. Ordering Toll-Free (1-800/888/877) Services

a. Since the inception of toll-free service, the service has been referred to as "1-800" and "800 service;" therefore, we continue that reference throughout this handbook and during conversations.

b. All requests for 800 service must be approved by the unit or activity TCO.

c. The III Corps G6 Office must also approve requests for 800 service that are in support of exercises.

d. All requests for 800 service will include the name, telephone number, and address of the budget POC and a statement that funds are available. Requests submitted from Fort Hood

must have approval from an ACoF, RM budget POC. It is the responsibility of the requestor to coordinate funding. Requests received without proper funding will not be processed.

e. Cost. 800 service incurs no charge to the calling party. The called party is responsible for the bill. Cost for an 800 line is \$45.00 per month recurring charge plus actual usage charges. Usage charges are based on how many calls are made, length of the call, location call was placed from, and time of day the call was made. Estimate cost at approximately \$.07 cents per minute.

f. Submit requests for 800 service in writing (in memorandum format to the address in paragraph 4-9d) and include:

- (1) The name of the unit or activity requesting the service.
- (2) The local telephone number which service will come in over. If service will come in on a rotary hunt group, then all numbers of the group must be listed with the pilot number as the first number.
- (3) Justification for ordering the service.
- (4) Estimated monthly recurring charge in dollars per month.
- (5) Provide the date service must be operational. If request is for a temporary exercise service, state both the start and the stop dates.
- (6) Identify the building, room, and floor where service will terminate.
- (7) State whether or not the circuit is to be a secure circuit. If circuit is secure, state the type of cryptographic equipment to be installed on the circuit.
- (8) Give the estimated busy hour. What hour of the day do you expect the most calls?
- (9) Give the estimated monthly usage in minutes.
- (10) Give the expected number of busy hour call attempts. How many calls do you think will be made during your busiest hour?
- (11) Give the expected seasonal volume increase. Do you expect more calls at certain times of the year than at other times?
- (12) Give the expected busy hour percent of increase after 6 months.
- (13) Give the expected busy hour percent of increase after 12 months.
- (14) Identify POC by name and telephone number. Provide a primary and alternate POC. Telephone and fax numbers should be shown as both DSN and commercial. POCs should be familiar with the requirement and available to receive telephone calls regarding the action.
- (15) Mailing address, including office symbol and nine-digit zip code for the POC.
- (16) Provide your message traffic address and that of the budget POC.

g. Lead-time is essential when ordering 800 service. Normal lead-time is 90 days from the time that a completed and validated RFS is received at DISA ATD, Fort Huachuca. Requests with shorter lead-times will be processed; however, shortened lead-time often requires expedite fees in order to obtain service on time. Lack of lead-time often results in problems with the quality of service received.

h. Coordination is important to a successful installation of 800 service. The leased communications coordinator should be contacted anytime there is any progress or change in the status of an 800 service request.

(1) When a call is received regarding action being taken on an 800 service, it is important that the name of the person calling, the name of the company he represents and a telephone number where they can be reached be obtained. It is also important to take written notes on dialog regarding the 800 service action.

(2) An in-effect report must be submitted by the DOIM leased communications coordinator when service has been installed and is working. The leased communications coordinator must be informed by the POC as soon as possible after service has been

provided. Information needed includes the date and time service was provided, the 800 number assigned and whether or not service is working satisfactorily.

4-12. Ordering Local Leased Communications Services

a. All requests for local leased communications must be approved by the unit or activity TCO.

b. The III Corps G6 office must also approve requests for leased long-haul communications that are in support of an exercise. The DOIM/1114th Signal Battalion S3 must also review exercise requests for technical accuracy.

c. All requests for leased long-haul communications must have the name, telephone number, and address of the budget POC and a statement that funds are available. Requests submitted from Fort Hood must have approval from an RM budget POC. It is the responsibility of the requester to coordinate funding. Requests received without proper funding are not processed.

d. The address where service is required must be provided. Furnish a diagram showing where service is to be located in the room or building. Service will be provided according to the diagram. If the address is not a street address or a building number, as frequently occurs in exercise requirements, provide driving directions in simple terminology. If available, reference civilian telephone pole or pedestal numbers. A current map, showing major roads and geographical features, should also be submitted with the request. Last minute changes in a desired service location cause delays in providing service.

e. Requests for local leased communications must be submitted in writing (in memorandum format to the address in paragraph 4-9d) and include:

(1) The name of the unit or activity requesting the service.

(2) Type of service required.

(3) Justification for ordering the service.

(4) Estimated cost of toll (long distance) usage.

(5) The date service must be operational. If request is for a temporary exercise circuit, state both the start and the stop dates.

(6) State whether or not installation of telephone jacks is required.

(7) Identify POC by name and telephone number. Provide a primary and alternate POC. Telephone and fax numbers should be shown as both DSN and commercial. POCs should be familiar with the requirement and available to receive telephone calls regarding the action and also act as escorts. On exercise requirements, it may be necessary to go to the site where service is required and meet with the local servicing telephone company.

(8) Mailing address, including office symbol and nine-digit zip code for the POC.

f. Lead-time for ordering local leased service is usually 30 days, but may vary with the type of service ordered and will be longer for services which require construction. Requests with fewer than 30 days lead-times will be processed; however, lack of lead-time sometimes incurs overtime charges.

g. Coordination is important to successfully installing local leased service. Information regarding the service should be shared with the leased communications coordinator. The leased communications coordinator should be contacted anytime there is any progress or change in the status of a local leased requirement.

h. When a call is received regarding action on a service, it is important that the name of the person calling, the name of the company he/she represents and a telephone number where they can be reached be obtained. It is also important to take written notes on what was said regarding the circuit action.

i. An in-effect report is required to be submitted by the DOIM leased communications coordinator when service has been installed and is working . The leased communications coordinator must be informed by the POC as soon as possible after service has been provided. Information needed includes the date and time service was provided, the telephone number(s), and whether or not service is working satisfactorily.

4-13. Pay Telephone Service

a. Pay telephones are provided through an AAFES contract. Only the building custodian can order pay telephone service. Table B-1 lists contact information.

b. Lead-time for pay telephones is eight (8) weeks.

4-14. Telephone Calling Cards

a. AR 25-1 governs ordering and use of telephone calling cards. Telephone calling cards are only used (1) for official business, (2) when the cardholder is away from his normal duty station, and (3) in a location where there is no government service available.

b. Requests for telephone calling cards must be approved by the unit or activity TCO.

c. Requests for calling cards that are in support of an exercise must also be approved by the III Corps G6 Office.

d. All requests for calling cards will include the name, telephone number, and address of the budget POC and a statement that funds are available.

e. Submit requests for calling cards will be submitted in writing (in memorandum format to the address in paragraph 4-9d) and include:

(1) The name of the unit or activity requesting the service.

(2) The number of cards required.

(3) Justification for ordering the service.

(4) The name, rank and job title of the person(s) who will be using the card(s).

(5) Calling area desired, CONUS only, OCONUS only, or a combination of CONUS and OCONUS.

(6) The date the card is required. Lead time is 10 days for calling cards.

(7) Identify POC by name and telephone number. The POC for telephone calling cards must be the unit or activity TCO. Calling cards will not be issued to anyone who is not the unit or activity TCO.

(8) Mailing address, including office symbol and nine-digit zip code for the POC.

f. Telephone calling cards require special security precautions to prevent unauthorized usage. Cards will be canceled when the cardholder separates from the organization, no longer requires use of a calling card, or when it is believed a calling card number has been compromised. The TCO must cancel the calling card by notifying DOIM in writing. (Table B-1 lists contact information.) Replacement cards may be issued, if necessary. Un-issued or returned cards should be kept in a secure area. Calling cards should not be left lying out in the open where the number could be copied. When issuing correspondence regarding calling cards, leave off or mark out (with an "X") the Personal Identification Number (PIN). The PIN is the last four digits of the calling card number. Example: 123 456 7890 XXXX. This will make it more difficult for someone to use the card number should it be compromised.

g. TCOs perform the following functions for calling cards:

(1) Sign for approved calling cards.

(2) Maintain an up-to-date listing of calling cards issued to their activity.

(3) Annually review card listing.

(4) Revalidate requirement for each card, canceling unjustified cards.

h. Cards must be canceled by the DOIM leased communications coordinator. Do not contact the vendor directly to cancel a calling card.

4-15. Pagers

a. Two options for official pager service are available in the Fort Hood area.

(1) Fort Hood owned service is available through DOL for the Fort Hood and Killeen area only, and does not incur a monthly service charge.

(2) GSA ID/IQ contract service is available directly from a national vendor; local area coverage to nationwide coverage (several options) is available. This service is funded with monthly charges to an IMPAC card, and offers leasing options (more advantageous for some options) as well as purchase options. Table B-1 lists contact information.

b. Equipment purchased for paging services becomes installation property and must be handled according to AR 710-2.

c. Maintenance is the responsibility of the owning activity. The DOL has repair facilities and should be contacted before seeking a non-government source. Commercial maintenance and equipment repairs must be purchased with unit funds (IMPAC card).

Section III Radio Frequencies

4-16. Commercial Radio Frequencies

a. Commercial radio units and systems require a CAPR for approval. Appendix C discusses CAPRs.

b. All commercial radio purchases require a memorandum with requirements and justification clearly stated. Funding is the responsibility of the MSC or Directorate.

c. Maintenance is the responsibility of the owning activity. The DOL E and C Shop has repair facilities and should be contacted before seeking a non-government source. Table B-1 lists contact information.

d. Fort Hood has limited commercial frequencies. Send request for commercial frequencies (non-tactical) to the DOIM Plans Branch (see Table B-1 for contact information).

e. Special note: commercial radios are approved for use within a 50-mile radius (80.45 kilometers) of Fort Hood only. Additional coordination is required for use in the CONUS and overseas. Each nation has its own frequency management plan; therefore, when a unit is deployed overseas, transmission on CONUS assigned frequencies may interfere with host country facilities or functions.

f. All commercial radio frequency equipment must have an approved JF-12 (see AR 5-12) number assigned. JF-12s are assigned by submitting a DD-1494 (Application for Equipment Frequency Allocation) to DOIM Plans Branch.

Chapter 5 Records Management

Section 1 Headquarters III Corps Distribution Center

5-1. Purpose

Ensure that incoming and outgoing correspondence and mail flow smoothly, with minimum processing steps.

5-2. Criteria

Send a written request for a distribution box to:

Commander
HQ, III Corps and Fort Hood
ATTN: AFZF-IM-SD-SBR
Fort Hood, TX 76544-5056

5-3. Hours of Operation

DOIM Services Branch personnel sort incoming official mail and sort drop off incoming official mail into distribution boxes between 0900-1230.

5-4. Distribution Addressing

Distribution is made according to FH Form 1853 (Distribution Scheme). Do not use building numbers or communication security (COMSEC) account numbers as an address to receive official mail or on-post distribution.

5-5. Mail Scheme

To avoid delay in receiving mail, notify correspondents of the correct mailing address. The Official Mail and Distribution Center publishes the authorized mail scheme that also includes office symbols.

Section II Official Mail

5-6. Purpose

To move official mail at the most cost effective postage rate to meet the required delivery date, security, and accountability requirements.

5-7. Criteria

Send a written request for an official mail account to the address in paragraph 5-2.

5-8. Cut-off Times and Special Instructions

a. To expedite processing of official mail, assemble all mail pieces so they face the same direction and sort pieces according to the service required. Items must be delivered to the Official Mail and Distribution Center (Table B-1) before the designated service cut-off time if pick-up is desired the same day.

- b. Mail leaves same day: 0800 through 1130 and 1230 through 1500.
- c. Mail leaves next day: 1530 through 1630.
- d. Federal Express®: 1030; see special instructions:
 - (1) Mail directed to a military installation requires a building number.
 - (2) Mail directed to a large building requires a room number.
 - (3) Mail directed to an Army Post Office (APO) address requires a POC and telephone number.
 - (4) Mail directed to a non-military address requires a street address. To by-pass official mail use your own fund site. Mail directed through Federal Express® does not have weight or size restrictions.
- e. Registered Mail: 0930; special instructions: All seams must be sealed with brown Kraft™ paper tape (matte). Tape must be adhered to package or post office will not accept the package.
- f. Certified Mail - 1400 - Special instructions: Mail directed through the United States Postal Service cannot weigh more than 70 pounds and may not be more than 108 inches in length and girth combined. All addresses must be typed.

Section III

Freedom of Information Act (FOIA) Program

5-9. Purpose

To provide information concerning public release of DA records under the Freedom of Information Act (FOIA).

5-10. Criteria

- a. Any person can file a FOIA request, including U.S. citizens, foreign nationals, organizations, universities, businesses, and state and local governments.
- b. Individuals can submit requests for III Corps and Fort Hood records by:
 - (1) Address mail to:

Commander
III Corps and Fort Hood
ATTN: AFZF-IM-SD-SB (FOIA)
Fort Hood, TX 76544-5056
 - (2) Fax to telephone number listed in Table B-1.
- c. Tenant organizations located at Fort Hood have separate FOIA programs.

5-11. Response Time

- a. Title 5 USC, Section 552 requires:
 - (1) The FOIA official must release or deny a record to the requester normally within 20 working days from receipt of the request.
 - (2) The FOIA official will notify the requester in writing when time limits are extended due to unusual circumstances. Examples when extended time limits are justified:
 - (a) When coordination efforts to locate and gather requested records involves several activities and units.
 - (b) When a search for and examination of information involves voluminous records.

b. Failure to comply with these time limits could result in legal action against the U.S. Army.

5-12. Procedures

a. DOIM Services Branch processes all FOIA requests for III Corps and Fort Hood records. Table B-1 contains FOIA contact information. The operating hours are 0730-1630 Monday through Friday.

b. The FOIA official initiates immediate action to gather requested documents when a FOIA request is received. DOIM formally tasks the custodian(s) of the requested records by memorandum. The memorandum prepared by DOIM establishes a suspense date to allow records review, releaseability determination, coordination within the 10-day response time, and follow-up to assure receipt within the designated time frame.

c. Upon receipt of requested records in DOIM, the FOIA official reviews the records to determine if they are releasable according to the referenced guidelines. DOIM forwards releasable documents directly to the requester by letter. DOIM obtains Staff Judge Advocate coordination on documents determined not releasable, and the FOIA official prepares a transmittal package to the appropriate initial denial authority as defined in AR 25-55 (The Army Freedom of Information Act Program).

5-13. Fees

a. Units and activities responding to FOIA requests complete DD Form 2085 (Record of Freedom of Information Processing Cost) to document fees for search, review, and reproduction. The FOIA official uses this document to determine reimbursable costs associated with processing the FOIA action. DOIM provides notification of outstanding debt to the requester at the time of record release. The requester submits payment for the information to the below address within 30 days from the date of the notification letter:

DOIM
ATTN: AFZF-IM-SD-SB (FOIA)
Fort Hood, Texas 76544-5000

b. Failure by the requester to submit payment establishes a precedent in not releasing of future records pending settlement of outstanding debts.

c. When DOIM receives payment, the FOIA official transfers the fees to the Defense Accounting Office.

5-14. Training

Records management training is conducted monthly by G3 Training. Dates and times are published in the Computer Literacy Program schedule published by G3 Education Services Division each month.

5-15. Reports

Reports are submitted each fiscal year. The FOIA official maintains required statistics for this annual report and forwards the Fort Hood report to FORSCOM each January.

5-16. Files

a. Record custodians use guidelines in AR 25-400-2 to maintain their FOIA files.

b. Files are calendar year files.

Section IV Forms Management

5-17. Purpose

- a. To provide information on how to request, revise, replace, or rescind local forms.
- b. The goal of the Forms Management program is to standardize and simplify forms, reduce the number of forms in existence by eliminating duplicate and nonessential forms, and to use higher-echelon forms wherever possible.

5-18. Definition

- a. A form is a predetermined arrangement of prepared spaces for the collection, recording, and extraction of information, including worksheets. Although most forms provide spaces for inserting information, this is not a requirement for classification as a form. Handouts, labels, stickers, and similar items may not require the insertion of information; however, when these items are reproduced or stocked for future use, they are classified as forms. There are three categories of forms used at Fort Hood:
 - b. Local forms include Fort Hood forms, 1st Cavalry Division (1CD) forms, 4th Infantry Division (4ID) forms, OTC forms, and MEDDAC forms.
 - c. Command or agency forms include FORSCOM forms.
 - d. Examples of Army-wide forms include such forms as DA forms, DD forms, Optional Forms (OF), and Standard Forms (SF).

5-19. Forms Manager Support

The Installation Forms Management Officer (IFMO) within DOIM Services Branch provides the following support to units and activities.

- a. Process requests for new forms, revisions to existing forms, replacement of forms, and deletion of forms.
- b. Assure local forms comply with governing regulations (including AR 25-30, The Army Integrated Publishing and Printing Program; DA Pamphlet 25-31, Forms Management, Analysis, and Design; DA Pamphlet 25-51, The Army Privacy Program), and subject guidance.
- c. Ensure requests for changes to forms and request for new forms are coordinated with applicable units and activities.
- d. Receive and process printing requests for reproduction of local forms and higher headquarters reproducible forms. Process printing requests to maintain adequate stockage level at the Installation Publication Stockroom.
- e. Conduct staff assistance visits to provide guidance on the Forms Management program and to coordinate support for computer-generated forms.
- f. Publish consolidated index of Fort Hood blank forms.
- g. Develop and publish the III Corps and Fort Hood Director of Key Personnel.
- h. Prepare and forward required reports on forms management to FORSCOM.
- i. Conduct forms management surveys in conjunction with scheduled records management surveys.

5-20. Forms Management Officers (FMO) and Forms Management Coordinators (FMC)

FMOs are appointed within the 1CD, 4ID, OTC, and MEDDAC to assist in forms management actions. Division FMOs are responsible for operating forms programs within their command. FMCs are appointed within 13th COSCOM, 3rd Signal Brigade, Headquarters Command, tenant activities, and Corps and Garrison activities to coordinate forms actions. FMOs and

FMCs serve as POC for the IMFO. Commanders should issue appointment orders for FMOs and FMCs and send a copy to DOIM Service Branch, Forms Management Office, Bldg 1001, Room E125A.

5-21. Procedures

a. Units and activities should submit requests for new or revised forms through the appropriate FMO/FMC using DD Form 67 (Form Processing Action Request). Attach to the DD Form 67:

(1) A copy of the proposed form or revision.

(2) A copy of the prescribing directive, if the directive is not electronically available.

(3) A DAPS-FH 5604 (Printing/Reprographic Request) available at the DOIM printing liaison office (Table B-1).

b. The FMO/FMC will analyze the request to ensure the request is valid, the required paperwork is filled out completely and accurately, and the form is signed. The FMO/FMC will return incomplete requests to the requester for correction.

c. The IFMO will process the requests for new or revised forms.

d. Reinstated forms: Requests to reinstate obsolete forms should include justification for reinstating the form.

e. Resupplies. The IFMO will process requests for resupplies on DAPS-FH Form 5604.

f. DA locally reproducible forms are designated with the suffix "-R" as in DA Form xxx-R. AR 25-30 (The Army Printing and Publishing Program) gives the authority for local reproduction and use of DD Forms.

g. Privacy Act Statements (PAS). Under the provisions of the Privacy Act of 1974 (5 U.S.C. 552A) and AR 340-21, forms which are used to collect personal information directly from an individual must have a PAS. When personal information is taken from a higher headquarters form, a separate PAS is not required if the source document shows completion of the local action as a routine use. All forms containing personal information whether taken directly from the individual or from their records, must comply with the provisions of AR 340-21 (The Army Privacy Program) and are subject to examination by the Installation Privacy Act Official.

5-22. Training

Records Management Training is conducted monthly by G3 Training. Training schedules are published in the Computer Literacy Program schedule published by G3 Education Services Division.

5-23. Phantom Corps Library of Electronic Recordkeeping (CLERK)

Local forms are available from Phantom CLERK at <http://pclerk.hood.army.mil>.

Section V

Files Management

5-24. Purpose

To provide information concerning establishing, maintaining, and disposition of official office records.

5-25. Definitions

a. Records include all books, papers, maps, photographs, machine-readable materials, or other documentary materials, regardless of physical form or characteristics, made or received by an agency of the U.S. government under federal law or in connection with the transaction of public business and preserved or appropriate for preservation by that agency or its legitimate successor as evidence of the organization, functions, policies, decisions, procedures, operations, or because of the informational value of the data in them.

(1) Physical form or characteristics include records created on magnetic tape, punch cards, aperture cards, disks, cores, microfilm, computer printouts, large maps, and tab cards as well as paper.

(2) In connection with the transaction of public business refers to file items created during the course of business that are the property of the federal government and not of the individual.

b. Electronic records include numeric, graphic, and text information which may be recorded on any medium capable of being read by a computer and which satisfies the definition of a record.

c. Non-record material.

(1) Library and museum material made or acquired and preserved solely for reference or exhibition purposes.

(2) Extra copies of documents preserved only for convenience of reference.

(3) Stocks of publications and processed documents used for supply purposes.

(4) Letters of transmittal that do not add information to that contained in the transmittal material.

(5) Transcribed shorthand notes and stenographic material.

(6) Drafts, worksheets, and notes that do not represent significant basic steps in the preparation of the record copy.

d. Working papers are documents such as rough notes, calculations, or drafts assembled or created and used in the preparation or analysis of other documents. Working papers are considered records and are filed under the appropriate file number.

5-26. General

Areas involved in files management:

a. List of selected file numbers.

b. Files training.

c. Records Holding Area (RHA).

5-27. Selected File Numbers (FORSCOM Form 350-R)

a. The purpose of a filing system is the easy retrieval of records. AR 25-400-2 (The Modern Army Recordkeeping System [MARKS]) requires a list of file numbers when files are first created and when major changes occur. FORSCOM requires each office prepare a list on a FORSCOM Form 350-R (List of Selected File Numbers). The custodian submits this list of file numbers to the RMO for approval. After approval, the RMO files a copy and returns the original list to the submitter.

b. Each MSC RMO has approval authority for FORSCOM Forms 350-R within their command. The installation RMO within the DOIM Services Branch approves lists for Garrison and Corps activities.

c. RMOs review the list from each office of record for accuracy and proper separation of mission and housekeeping files. If changes are needed, the RMO returns the list to the submitter with recommendations. Once approved by the RMO, the list is valid until major changes occur in the filing system. RMOs maintain copies of the lists of selected file numbers they approve.

5-28. Files Training

a. Files training is conducted monthly by G3 Training. Dates and times are published in the Computer Literacy Program schedule published by G3 Education Services Division.

b. DOIM provides MARKS training sessions for separate units and activities upon request; however, RMOs should consider providing files classes for their offices of record.

5-29. Records Holding Area (RHA)

a. The RHA is located in Building 14 (52nd Street) and stores records with a retention period of 3 to 7 years. DOIM retires records having a longer retention period to a Federal Records Center (FRC). Classified material and electronic media (microfiche, etc.) are not stored at the RHA.

b. RMOs and Records Management Coordinators (RMC) transfer records to the RHA each January and October according to AR 25-400-2. DOIM may authorize accelerated transfer of records to the RHA when a unit or activity lacks storage space in their current files area. RMOs and RMCs may also transfer records to the RHA at other times during the year when fully justified.

(1) Records custodians prepare and forward an original and two copies of SF 135 (Records Transmittal and Receipt) through their RMO or RMC to DOIM Services Branch. DOIM checks the SF 135 for file title, disposition authority, disposal date, and mandatory information and assigns RHA locations for the records. DOIM returns the original and one copy of the SF 135 to the activity along with an appointment date for the RHA and a handout explaining transfer procedures.

(2) Records transferred to the RHA remain the property of the submitting activity. Appropriate activity personnel can access the records by making an appointment to review records two working days in advance. Organizations requesting the record must have the location number of the records. DOIM opens the RHA for the activity to conduct record searches. The activity completes a DA Form 543 (Request for Records) for every record pulled from the RHA.

c. DOIM pulls records eligible for destruction each January and October. The DOIM RHA database and SF 135s provide a list of records eligible for retirement to FRCs. DOIM pulls the records from the shelves and consolidates the records for shipment to either the Washington National Records Center (WNRC) or the National Personnel Records Center (NPRC).

(1) DOIM packs the records into new boxes for shipping to the WNRC or NPRC. DOIM then prepares SF 135s and forwards an original and one copy to the WNRC or NPRC for approval and assignment of accession numbers. When the FRC returns the SF 135s with the accession numbers, DOIM places a copy of the SF 135 in the first box of each series.

(2) DOIM places on the outside of each box the accession number, description of box contents, and number of boxes in the series. DOIM then coordinates with DOL Transportation for shipment of the boxes to the FRC.

5-30. Files

a. Records custodians will maintain files according to guidelines contained in AR 25-400-2.

b. Custodians will inspect records before filing to ensure all actions are completed and eliminate unnecessary attached material (such as used envelopes, routing slips which bear no essential information, and extra copies). Custodians will also identify incomplete sections to ensure that they are followed up and that the file will not be prematurely cut off. If the action is complete, but essential documentation is missing, the custodian will try to get the missing documents. If the documents are not located, the custodian will note the action taken and file it with the incomplete action.

c. Custodians will remove all cover sheets from the records before filing unless the records are in suspense files or when cases are placed in file containers pending completion of the action.

d. Custodians will staple documents if possible; however, use other fasteners when there are too many papers for stapling or physical characteristics prohibit stapling.

e. As specified in AR 25-50 (Preparing and Managing Correspondence), the action officer will add the MARKS file number when creating a document. A file number may later be placed along the right-hand edge of documents not identified with a file number at the time of creation. Posting the file number to the document is unnecessary when the physical characteristics of a document make it self-identifying for filing purposes (reference copies of publications, mail control forms, etc.).

f. Custodians will use supplies available from the federal supply schedule or an administrative self-service support center to maintain records.

g. Custodians may use guides to divide files and to identify subdivisions for easy filing and retrieval. Custodians will use folders to consolidate, retrieve, and protect the records.

h. Custodians who perform duties for more than one organization will identify the records created in each capacity and maintain them separately. Examples include a division commander who is also an installation commander and a command safety officer who is also the installation safety officer.

i. Custodians will maintain their records alphabetically, numerically, or chronologically. Only records covered by a PAS notice may be arranged to permit retrieval by personal identifiers such as social security numbers or names.

j. Custodians will file classified and unclassified documents in separate containers unless an action consists of both classified and unclassified documents. Custodians may file classified and unclassified documents in the same container when a small volume of classified material is available and it is advantageous to use otherwise empty space for unclassified material. Custodians will separate classified and unclassified material by guide cards or by placement in separate drawers.

k. Custodians will not place file numbers on folders or containers maintaining suspense documents.

l. Custodians will label all folders and containers used to store official records. The labels will include the file number, file title, PAS notice number (if applicable), year of accumulation (if applicable), and the disposition instructions. Custodians may use abbreviations for the title of a file label; however, only abbreviations authorized in AR 25-400-2 may be used in the disposition instructions.

m. The custodian is not required to post file numbers to labels when one or more file containers have records with the same file number. Only the label on the first folder of the series and the label on the first container must show the required label information. Remaining folders, drawers, or other container need only be identified by the name, number, or other features identifying the contents.

5-31. Electronic Records

a. NARA established the basic requirements for the creation, maintenance, use, and disposal of electronic records. The requirements, which include federal records created by individuals using Email applications, were published in the 28 August 1995 Federal Register.

b. Only electronic records that meet the definition of a record are preserved in a recordkeeping system (see guidance on electronic records in Appendix N).

(1) Electronic records include numeric, graphic, and text information, which may be replaced on any medium capable of being read by a computer and which satisfied the definition of a record. Agencies should preserve Email messages that document their policies, programs, and functions; however, the NARA recognizes that not all Email messages are subject to retention in most cases, drafts are not record materials that not all Email messages are subject to retention.

(2) A recordkeeping system is a system that collects, organizes and categorizes records to facilitate their preservation, retrieval, use, and disposition. Mail networks and word processors are not considered recordkeeping systems; therefore, electronic records must be transferred to an official recordkeeping system.

(3) The NARA has given authority for proponents to delete Email records from their systems only after a copy of the full message with the name of senders and addresses and date of transmission, and receipts when required, have been preserved elsewhere.

c. The NARA had issued guidance on agency recordkeeping requirements that includes a discussion of drafts and provides criteria for determining when records are records. This guidance is located on the NARA web site the address is <http://www.nara.gov/era>. Fort Hood records are maintained according to AR 25-400-2. Fort Hood guidance on electronic records is currently under development.

**Section VI
Management Information Control****5-32. Purpose**

To provide information on how units and activities at III Corps and Fort Hood process requests to establish, revise, or rescind management information requirements.

5-33. Definitions

a. Management information required in planning, organizing, directing, coordinating, and controlling an organization and its assigned mission tasks.

b. A requirement for management information to be collected, processed, and transmitting on a periodic, as required, or one-time basis. A request may be transmitted orally or in writing and may require several information products, data inputs, and data outputs. An approved controlled management information requirement is assigned a RCS.

c. A management information system is an assemblage of resources and procedures organized to collect, process, and issue data. These data are used to plan, organize, staff, direct, coordinate, and control the use of resources to accomplish missions and tasks.

d. A Management Information Control Officer (MICO) is a person assigned authority to approve, disapprove, or revise proposed management information requirements within an agency. The MICO reviews and provides jurisdictional control of management information requirements.

e. Management Information Control Liaison (MICLO). A person assigned to coordinate management information requests within the activity, assist in management information control requirements reviews, and provide technical assistance to the MICO as needed in the control of management information.

5-34. General

a. The management information control system is established to monitor requests for the collection of management data that involves extra effort by an activity to compile the requested information. These requests (information requirements or recurring reports) are monitored and controlled by the Fort Hood MICO. The Fort Hood MICO ensures only mission essential management data are requested and prevents activities from being overwhelmed by unnecessary or duplicate information requests.

b. There are two types of management information requirements: nonexempt and exempt. Nonexempt management information requirements are assigned an RCS. However, since management information requirements encompass a major part of Army communications, many common, recurring, general management information requirements are exempt from control. AR 335-15, Chapter 5, outlines the exemptions.

c. Unless exempt from control under AR 335-15 (Management Information Control Systems), management information requirements are:

(1) Established when approved by the Fort Hood MICO according to AR 335-15.

(2) Assigned an RCS by the Fort Hood MICO.

(3) Revised or rescinded when the management information requirement changes.

d. Nonexempt management information requirements are requested by a directive containing implementation instructions. The directive outlines (or changes) an information requirement, states who submits the data, and gives instructions on how and when to submit the data. If information is requested from several activities at Fort Hood, the directive may be published as a Fort Hood memorandum or message.

e. The management information control system includes ADP products processed at the installation data processing activity; however, at this time there are no identified applicable products at Fort Hood.

5-35. Management Information Control Liaison (MICLOs)

MICLOs are responsible for management information requirements control within their activity to include:

a. Identifying and reporting to the Fort Hood MICO a list of recurring reports prepared by their activity to higher headquarters.

b. Identifying management information requirements and requests their activity sends to other Fort Hood organizations to get information.

c. Determining if information requirements and requests are exempt or nonexempt.

d. Reviewing management information requirements and requests forms and packages before forwarding the information to the Fort Hood MICO for approval.

5-36. High Headquarters Report Control Systems (RCS) Reports

a. FORSCOM, DA, and most higher headquarters agencies assign a local RCS or have an RCS exempt statement for each of their controlled information requirements. An example of a higher headquarters requirement is RCS: MILPC-45, Number and Types of Decoration Approved.

b. For recurring reports submitted to higher headquarters, the Fort Hood MICO maintains a copy of each directive explaining the information requirement and correspondence or reviews regarding the requirement.

5-37. Fort Hood Report Control Systems (RCS) Reports

a. The Fort Hood MICO assigns a local RCS or RCS exemption statement for management information requirements generated by Corps and Garrison activities. MICLOs review their activity's requests for management information requirements before forwarding the request to the MICO. The MICO reviews all local publications and forms for management information requirements.

b. An example of a Fort Hood controlled management information requirement is the Command Information Summary, RCS: AFZF-DRM-01. Activities submit information to the ACofS RM. An example of an exempt requirement may be a request for nominations for an award or a request for a listing kept for operational purposes.

5-38. List of Controlled Requirements

The Fort Hood MICO periodically compiles a list of local and higher headquarters controlled management information requirements that require information from Corps and Garrison activities. III Corps and Fort Hood Memorandum 25-2 (Fort Hood Reports Control System) identifies preparing activities, RCSs, titles of report, directives, and frequency of preparation of report.

5-39. Approval of Management Information Requirements

a. Activities initiating or revising a management information requirement define the requirement in a directive. The proponent prepares, revises, or changes the directive using the format shown in AR 335-15, paragraph 2-5.1.

b. The proponent completes DA Form 335-R (Application for Approval of Management Information Requirement). Detailed instructions for form completion are contained in AR 335-15, paragraph 2-10. The proponent also prepares DD Form 67 (Form Processing Action Request) if a directive prescribes use of a new Fort Hood form.

c. The proponent then forwards the directive, DA Form 335-R, and DD Form 67 (if applicable) to the activity MICLO. The MICLO uses the checklist in AR 335-15, figure 2-1, to review the approval request. The MICLO approves the request by signing block 18 of DA Form 335-R and returns the package to the proponent for staff coordination.

d. The proponent staffs the directive, completed DA Form 335-R, and DD Form 67 (if applicable) through the affected organizations (to include DOIM) as outlined in FH Reg 1-10, page 1-16, block 1-6f.

e. After the staffed directive is approved for publication by the command group, the proponent sends one copy of the approval and two copies of DA Form 335-R through the MICLO to the MICO for RCS assignment. The directive is then submitted for editing and publication. The proponent provides the Fort Hood MICO with a copy of the published directive.

f. When the proponent feels the requirement is exempt, the proponent sends a memorandum to the activity MICLO requesting exemption. The memorandum should include the management information required and exemption paragraph number. The MICLO approves or disapproves the request and provides a copy of the correspondence to the Fort Hood MICO.

5-40. Unauthorized Information Requests

a. Unauthorized requests are requests for management information that do not have an RCS or RCS exemption furnished with the information request. Upon receiving an unauthorized information request, the activity returns the request to the originator and notifies the Fort Hood MICO of the unauthorized request.

b. Staff agencies are not required to comply with local information requests that do not cite an RCS or an exemption (AR 335-15, paragraph 1-7h(2)).

Section VII**Army Privacy Act (PA) Program****5-41. Purpose**

a. To provide information on how units and activities at III Corps and Fort Hood should respond to inquiries asking for personal type information regarding a member or former member of the Army, without violating the Privacy Act of 1974 (AR 340-21, the Army Privacy Act Program).

b. To provide information concerning collection, retention, amendment, and disclosure procedures for personal information maintained in a system of records.

5-42. Fees

a. Normally, the first copy of a record provided to an individual is free. Reproduction fees are reimbursable on subsequent copies.

b. If released to third parties under the provisions of the FOIA, use the fee schedule in AR 25-55.

5-43. Training

Privacy Act Program training is conducted monthly by G3 Training. Dates and times are listed in the Computer Literacy Program schedule published by G3 Education Services Division.

5-44. Reports

Reports are submitted annually, on a calendar year schedule.

5-45. Files

a. Policy files are incorporated in MARKS file number 100.

b. Requests and responses are maintained in 340-12a.

c. Files are maintained by calendar year.

Section VIII**III Corps and Fort Hood Office Symbols****5-46. Purpose**

To provide information concerning office symbols within III Corps and Fort Hood.

5-47. Criteria

- a. Office symbols identify the origin of correspondence and electrically transmitted messages within DA. They are also used as part of the address when forwarding correspondence and mail to, from, and within HQDA.
- b. Characters other than letters of the alphabet will not be used in official office symbols.
- c. Office symbols will be as short as possible.
- d. Changes to office symbols will be kept to a minimum.
- e. III Corps and Fort Hood office symbols are constructed as follows:
 - (1) The first two letters represent the parent agency (AF identifies III Corps and Fort Hood as part of Headquarters, United States Army Forces Command).
 - (2) Third and fourth letters represent the principal office, installation, or MSC (ZF identifies III Corps and Fort Hood and VA identifies 1CD).
 - (3) Fifth, sixth and seventh digits represent directorate or comparable element or next element below agency level and may consist of only two letters (DPW identifies Directorate of Public Works and RM identifies ACofS, Resource Management).
 - (4) Additional characters can identify the following:
 - (a) Staff division or comparable or next lower element.
 - (b) Branch or next lower element.
 - (c) Section, group, team, individual action officer.

5-48. Procedures

- a. A unit or organization requiring a new office symbol can submit written requests (memorandum format) to:

Commander
 III Corps and Fort Hood
 ATTN: AFZF-IM-SD-SB
 Fort Hood, TX 76544-5056

- b. Hours of operation are 0730 - 1630, Monday through Friday.
- c. The request for a new office symbol should contain:
 - (1) A justification for a new office symbol (e.g., reassignment of a unit or organization from one command to another or the establishment of a new unit or organization).
 - (2) A copy of the orders reassigning or establishing the unit or organization.
- d. The DOIM will forward the request to FORSCOM for review and assignment of an appropriate office symbol.
- e. The DOIM will notify the requesting unit or organization in writing of the newly assigned office symbol upon receipt of assigned office symbol for that unit or organization.
- f. Units and organizations should notify the DOIM in writing of changes in internal office symbols.

Chapter 6**III Corps and Fort Hood Printing Program****6-1. Purpose**

To provide information concerning the III Corps and Fort Hood printing program.

6-2. General Information

- a. Purchase or production of duplicating must be for the conduct of official business.
- b. Reproduction of calling, greeting, and business cards is prohibited. These items have been determined for personal use rather than for official use. However, designated military and ROTC recruiters are authorized individual business cards at government expense.
- c. Printing of invitations for official functions must be in one color ink.
- d. Printing of stationery, memo pads, and other items that contain a person's name, position, rank, and/or office title is prohibited. These items have also been determined for personal use rather than for official use. As well, units and activities are prohibited from printing, duplicating, and self-service copying these items.
- e. Advertisements inserted by or for private individuals, firms, or corporations or material implying the government endorses or favors specific commercial products, commodities, or services will not be printed.
- f. Wall and desk calendars are not printed because units and activities can purchase standard government wall and desk calendars from the GSA using local purchase procedures.

6-3. Procedures

- a. Activities prepare and submit printing requirements using a DAPS-FH 5604 (10-02). Forms are available at the DOIM printing liaison (see Table B-1).
- b. Multicolor printing is authorized only for certificates of achievement. Activities requesting multicolor printing must provide DOIM Services Branch with a memorandum that provides funding authorization, a brief justification, a print request, and camera-ready artwork. The G3/DPTM Training Support Center, provides artwork support for the camera-ready copies. Table B-1 lists Training Support Center contact data.
- c. The DOIM Printing Office reviews the printing requests for compliance with regulatory guidance. DOIM forwards approved printing requests to the Document Automation and Production Services (DAPS) Office (see Table B-1) for processing and returns disapproved request to the customer.
- d. The DAPS completes printing requests within 3 to 5 work days, when print jobs are less than 25,000 units (units are calculated as the total number of pages multiplied by the number of copies required). Print jobs exceeding 25,000 units require a longer turn around time. DAPS will provide an estimated delivery date for print requests that exceed 25,000 units if requested. Table B-1 lists contact information.

6-4. Satellite Facilities

- a. Fort Hood has satellite print facilities located in 1CD, 4ID, and 13th COSCOM. The S1 within each MSC and each tenant activity operates and manages these facilities.
- b. The satellite facilities support printing requirements within each respective MSC and tenant activity; however, the DOIM Services Branch provides printing support for the MSCs and tenant activities as needed.

6-5. Reports

DOIM provides a quarterly listing of works submitted by each unit to each activity. The report includes information on costs related to the requests.

6-6. Files

- a. Print requests and responses are maintained in MARKS file number 715.
- b. Files are maintained by fiscal year.

Section II**III Corps and Fort Hood Office Copier Management Program****6-7. Purpose**

- a. To provide information concerning how to request, relocate, turn-in, or upgrade office copiers within III Corps and Fort Hood.
- b. To provide information concerning the management, planning and control of installation office copiers.

6-8. Criteria

Activities requesting installation copier support must submit their request in writing to DOIM Services Branch according to guidelines in AR 25-30.

6-9. Procedures

- a. The DOIM Services Branch, upon receipt of a written request, evaluates the request to determine:
 - (1) Compliance with AR 25-30.
 - (2) Validity of the support requested.
 - (3) Whether existing copiers at Fort Hood can satisfy the requirement.
- b. The office copier COR initiates the following actions to validate new requirements.
 - (1) Endorses the memorandum or Email back to the requester recommending approval of disapproval of the requested action. Approvals include operation, maintenance, and reporting procedures to be followed by the request.
 - (2) DOIM reviews the COR's recommendation and then approves or disapproves the request and forwards copies of the package to the requester, appropriate program director, and to the Installation Property Book Officer. The COR maintains a record file copy until the copier is replaced or turned in.
- c. The COR conducts surveys at least every two years according to AR 25-30, to evaluate the management, efficiencies, and cost effectiveness of the office copier program. When conducting the survey, the COR:
 - (1) Revalidates initial requirements.
 - (2) Ensures that each copier is producing the range of copies recommended for the copier according to the copier contract.
- d. The COR maintains an automated inventory of copiers and updates the inventory once a month. The COR provides copies of the inventory to the Installation Property Book Officer.
- e. The contractor reads the meters for each copier once each month. After the reading, the contractor provides the COR with information on the number of copies produced on each machine. POCs for the copiers in each activity validate (with the contractor) the number of copies produced on each copier.

6-10. Training

Is conducted monthly by G3 Training. Dates and times are published in the Computer Literacy Program schedule published by G3 Education Services Division.

6-11. Reports

- a. Inventory listing. Inventory is updated monthly and forwarded to Installation Property Book Officer.

- b. Purchase Request and Commitment is prepared monthly and forwarded to Director Contracting.
- c. Cost and Production Report is prepared monthly and forwarded to Chief Services Branch, work leader Records Management Branch, and DOIM Budget Team.
- d. Office Copier Cost Charge Back Report is prepared monthly and placed in the DOIM public folders.

6-12. Relocation

- a. Copiers delivered under this contract may not be relocated from the initial delivery point without prior approval from the Copier COR.
- b. Unauthorized moves will constitute a violation of the provisions of the contract and may result in a claim against the government.
- c. Activities are responsible for damages and costs incurred from unauthorized moves.

6-13. Maintenance

- a. Activities will report maintenance or supply requirements to the copier vendor as listed in Table B-1.
- b. When reporting maintenance calls, customers will provide information on model, serial number, location, point of contact, the phone number of POC, and the information on how the copier is malfunctioning.

6-14. Files

- a. Record custodians will maintain office copiers files according to AR 25-400-2.
- b. Copier policy files are maintained in MARKS file number 1q.
- c. Office copier requests and approvals are maintained in MARKS file number 25-30zz.
- d. Copier files are maintained by fiscal year.

6-15. Fiscal Year Copier Plan

- a. The fiscal year copier plan provides quarterly cost ceilings by activities.
- b. The plan applies to units and organizations affected by the copier ceilings under the single-vendor copier contract.

Chapter 7

Command Administrative Publications

Section I

III Corps and Fort Hood Command Administrative Publications

7-1. Purpose

To provide information on the III Corps and Fort Hood command administrative publications program.

7-2. Background Information

This information applies to command administrative publications received by DOIM Services Branch for publishing. Titles are drafts until edited and authenticated according to AR 25-30 and DA Pamphlet 25-40. Each title must meet the established criteria of a regulation, pamphlet, circular, or supplement.

7-3. Procedures

a. Fort Hood uses structured writing to write administrative publications. Structured writing uses blocks of information rather than paragraphs, and offers a clear, concise, and abbreviated writing method. Authors may request an exception to a structured writing format when the content of a title requires in-depth explanation that could be lost with structured writing format.

b. Proponents must coordinate new or revised regulations, supplements, or circulars, with each III Corps and Fort Hood element that has responsibility in the policy. Staffing must include DOIM. During coordination, DOIM reviews the draft manuscript for proper media, duplication of policy, applicability, MICO compliance, and forms review. Pamphlets are informational in nature and do not require staffing.

c. The proponent of the title must type the text and provide DOIM with a hard copy and a digital copy of the draft manuscript in Microsoft® Word. All artwork must be digital. The FH Form 21 (III Corps Action Processing Form) depicting staffing and Chief of Staff approval must accompany the manuscript when submitted for editorial services.

d. During the editorial process, DOIM reviews manuscripts for spelling, grammar, format, applicability, duplication, media, compliance with governing policy, reading grade level, methodology, mood, tense, and voice and ensures all required elements appear within the title. When DOIM completes the editorial review, the manuscript is returned to the proponent for review and applicable updates. The proponent then returns the manuscript to DOIM to be published.

e. DOIM issues only two changes to a title. When a change revises more than one half of the title, DOIM suggests a complete revision. Immediate action interim changes are not a publishing medium. When a title requires a change, DOIM issues a permanent change, which remains in effect until the title is revised or the change is superseded.

f. DOIM distributes III Corps and Fort Hood command administrative publications electronically through the Phantom Corps Library of Electronic Record Keeping (Phantom CLERK) web site. DOIM no longer provides hard copy distribution. Users may retrieve copies of administrative publications from the Phantom CLERK site at <http://pclerk.hood.army.mil>. Paragraph 7-14 explains Phantom CLERK.

7-4. Caltrop Bulletin

a. The Caltrop bulletin is a weekly command information bulletin that is published once each week. The Caltrop delivers official and unofficial information of an advisory, informative or directive nature. Official information receives publishing priority. DOIM gives equal consideration to all prospective articles.

b. The Caltrop is delivered to III Corps digitally. Find it on the Services Branch website at <http://pao.hood.army.mil/dsb/caltrop.html>.

c. To submit an article for inclusion in the Caltrop, contact the caltrop editor as listed in Table B-1.

Section III Installation Publications Stockroom

7-5. General Information

a. DOIM Installation Publications Stockroom stocks DA, DD, SF, OF, accountable and sensitive and miscellaneous forms for issue.

b. Publications clerks will hand carry requests to the publications stockroom. Operating hours are Monday, Wednesday, and Friday, 0730 to 1530. In an emergency, contact DOIM Services Branch as listed in Table B-1.

7-6. Procedures

a. DOIM personnel do not require military soldiers in uniform to furnish identification before issuing forms; however, civilian personnel must show their civilian identification cards before DOIM will issue forms. The DOIM Publications Stockroom is authorized to issue blank forms to:

(1) Active duty soldiers stationed at Fort Hood.

(2) USAR personnel within Fort Hood's area of support.

(3) DA civilians assigned to III Corps and Fort Hood activities.

(4) Contractor personnel with a letter of authorization and a DA Form 1687 (Notice of Delegation of Authority – Receipt for Supplies) from the COR to validate the support requirements.

(5) Other military service agencies, such as, Air Force, Marines, non-appropriated fund instrumentalities, and AAFES services.

b. Customers may get non-stocked forms by providing information about the required form and unit name, POC, unit phone number or by special order.

c. Customers complete a DA Form 17 (Request for Publications and Blank Forms) for unit requirements.

7-7. Requesting Accountable and Sensitive Forms

AR 25-30 requires that DOIM Services Branch personnel handle accountable forms following guidelines outlined in AR 380-5. Accountable forms and sensitive forms are issued from the stockroom to battalion and division levels. To get accountable and sensitive forms activities will:

a. Provide a copy of the assumption of command order and/or delegation of authority from the commander of the activity.

b. Provide DA Form 1687, which is typed and validated by the commander of the activity requesting accountable forms and/or sensitive forms.

c. Provide a *typed* DA Form 17 to request items required by the activity. Directions for completing the DA Form 17 are on the reverse side of the form.

d. Complete a DA 410 (Receipt for Accountable Form) if the item is an accountable form.

7-8. Establishing Accounts

a. The following units and activities can have a publications account:

(1) Active army units organized under a PAC that supports battalion-size units will request consolidated publications accounts for the entire battalion, except when a unit is geographically remote.

(2) Major staff elements are authorized publications accounts.

(3) USAR and ROTC units are also authorized publications accounts.

b. To establish a publications account, complete a DA Form 12-R (Request for Establishment of a Publications Account). Take the completed DA Form 12-R DOIM Installation Publications Stockroom for signature by the Publications Control Officer. DOIM

publications stockroom personnel will forward the DA Form 12-R to the Saint Louis Distribution Center for processing.

c. Units and activities must identify the type of account being requested on DA Form 12-R. There are two types of publications accounts classified and unclassified:

(1) Unclassified accounts are the most commonly used accounts.

(2) Classified accounts are used only by units who must have classified publications to perform their mission. To qualify for a classified account, a unit must:

(a) Have a valid requirement for the material to be requested or received.

(b) Have a facilities to safeguard the materials.

(c) Have personnel cleared to handle classified materials.

d. Each publications account holder will establish initial distribution requirements for each section or unit covered under their account. These requirements should then be consolidated through the USAPA website to ensure receipt from the DA Publications Distribution Center. A copy of the Subscription Report will be provided to DOIM stockroom personnel.

7-9. Publications Management Training

Training is conducted monthly by G3 Training. Dates and times are published in the Computer Literacy Program schedule published by the G3 Education Services Division.

7-10. Phantom Corps Library of Electronic Record Keeping (Phantom CLERK)

a. Phantom CLERK is Fort Hood's electronic repository of command forms and publications. This web-based publishing system delivers command administrative publications and blank, intelligent command forms to III Corps and Fort Hood users. Phantom CLERK complies with the DA Less Paper Policy, provides timely delivery of required references, and reduces printing and warehousing costs for III Corps. Phantom CLERK does not deliver DA regulations and forms, FMs, or TMs.

b. Updated forms and publications are posted to Phantom CLERK. With electronic delivery of command titles, DOIM no longer pays printing costs associated with hard copy distribution. Users may connect to Phantom CLERK, print an entire publication or excerpts of a publication, or fill or print a form. Users who need hard copies of a digital publication must fund printing. To request reproduction, follow procedures in paragraph 6-3.

c. Intelligent command forms are fillable with Form Flow™ software. Users must have Form Flow™ software to use Phantom CLERK. Fort Hood has several Form Flow™ site licenses: contact your IMO to get a copy or get it from the DA Pamphlet 25-30 (The Army Electronic Library).

d. Access to Phantom CLERK requires a III Corps ILAN account. See your IMO to establish necessary access.

e. Finding Phantom CLERK is easy. Connect to <http://pclerk.hood.army.mil> using a web browser. Once connected, Phantom CLERK prompts you for a USERID and password: simply use the same USERID and password you use to log on to the ILAN. Once accessed, Phantom CLERK is simple and self-explanatory.

f. If you experience problems using Phantom CLERK, report them through the SUGGESTIONS AND PROBLEM REPORTING tool under CONTENTS of the Phantom CLERK menu bar, or send an Email directly to the Phantom CLERK systems administrator using the Email link on the bottom-most portion of the menu bar. The systems administrators will offer a timely resolution.

**Appendix A
References**

Section I. Required References

AR 5-9

Area Support Responsibilities

AR 5-12

Army Management of the Electromagnetic Spectrum

AR 25-1

Army Information Management

AR 25-30

The Army Publishing and Printing Program

AR 25-50

Preparing and Managing Correspondence

AR 25-55

The Department of Army Freedom of Information Act Program

AR 25-400-2

The Modern Army Recordkeeping System (MARKS)

AR 310-34

The Department of The Army Equipment Authorization and Usage Program

AR 380-5

Department of the Army Information Security Program

AR 340-9

Office Symbols

AR 340-21

The Army Privacy Program

AR 335-15

Management Information Control System

AR 380-5

Department of the Army Information Security Program

AR 380-13

Acquisition and Storage of Information Concerning Nonaffiliated Persons and Organizations

AR 380-19

Information Systems Security

DA Pamphlet 25-1-1

Installation Information Services

DA Pam 25-30

The Army Electronic Library

DA Pam 25-31

Forms Management, Analysis, and Design

DA Pam 25-33

Users Guide for Army Publications

DA Pam 25-51

The Army Privacy Program-System of Records Notices and Exemption Rules

DA Pam 25-69

List of Approved Recurring Management Information Requirements

DA Pam 25-40

Administrative Publications: Action Officers Guide

DA Pamphlet 715-15

Service Contract Administration

FORSCOM Circular 25-95-9

List of Approved Management Information Requirements

FORSCOM Supplement 1 to AR 335-15

Management Information Control System

FORSCOM Supplement 1 to AR 25-400-2

The Modern Army Recordkeeping System (MARKS)

FORSCOM Pam 25-30

FORSCOM Publications and Blank Forms Index

Fort Hood Regulation 1-10

Staff Procedures Guide

Fort Hood Regulation 25-2

Records Management Policies and Procedures

Fort Hood Regulation 380-19

Information Systems Security

Fort Hood Memorandum 25-2

Fort Hood Reports Control System

Fort Hood Pamphlet 25-1

List of Approved Recurring Management Information Requirements

Fort Hood Pamphlet 25-30

Consolidated Index of Fort Hood Publications and Blank Forms

TB 18-103

Software Design and Development

Memorandum, USAISC, ASOP-M, 4 February 1994

subject: Records Management Update, January 1994

Title 5, Code of Federal Regulations, Section 1320

41 Code of Federal Regulations, Chapter 201.

Section II Listing by Functional Area III Corps and Fort Hood Delegation of Authority

36 Code of Federal Regulations, Chapter XII, subchapter B.

Sections 3301-3314, title 44, United States Code

41 Code of Federal Regulations, Chapter 201

Sections 3301-3314, title 44, United States Code

Federal Records Act of 1950, as amended

Privacy Act of 1974 (5 U.S.C. 552a)

DISA Circular 310-130-1

Submission of Telecommunications Service Requests

DOD Directive 7750.5

Management and Control of Information Requirements

DOD 5400.11

Department of Defense Privacy Program

DOD 5400.07

Department of Defense Freedom of Information Act (FOIA) Program

OFPP Pamphlet No.4

A Guide for Writing and Administering Performance Statements of Work for Service Contracts
Contracting Officer's Representative Handbook

Army FAR Supplement, Subpart 42.90
Contracting Officers Representatives (COR)

Defense Federal Acquisition Regulation (DEFAR)

Handbook for Surveillance of Service Contracts

III Corps and Fort Hood Policy Letter Gar 380-19
Systems Security (cited in para 1-12)

Memorandum DOIM, AFZF-IM-A, 7 Mar 95
subject: FY 95 Plan - Printing Program.

Section II. Related References.

This section not used.

Section III. Prescribed Forms

DA Form 12-R
Request for Establishment of a Publications Account (LRA)

DA Form 12-99-R
Initial Distribution (ID) Requirements for Publications (LRA)

DA Form 17
Request for Publications and Blank Forms

DA Form 1687
Notice of Delegation of Authority - Receipt for Supplies

DA Form 410
Receipt for Accountable Form

DA Form 543
Request for Records

DA Form 335-R
Application for Approval of Management Information Requirement

DA Form 1687
Notice of Delegation of Authority – Receipt for Supplies

DA Form 3161

Request for Issue or Turn In

DD Form 67

Form Processing Action Request

DD Form 1494

Application for Equipment Frequency Allocation

DD Form 2085

Record of Freedom of Information Processing Cost

FORSCOM Form 350-R

List of Selected File Numbers

Fort Hood Form 21

Placeholder placeholder placeholder

Fort Hood Form 105-X1-1

Communications Service Request

Fort Hood Form 105-X1-2

Data Communications Service Request

Fort Hood Form 21

III Corps Action Processing Form

Fort Hood Form 1556

Request Authorization Agreement Certification of Training and Reimbursement

Fort Hood Form 1853

Distribution Scheme (prescribed in paragraph 5-4)

DAPS-FH Form 5604

Printing/Reprographic Request

SF Form 135

Records Transmittal and Receipt

Appendix B
Points of Contact (POCs)

Table B-1. Points of Contact (POCs)

Function	Telephone	Building and Room	Email
CAPR	287-8274 fax: 287-5530	13 Rm. 112	John.sammis@hood.army.mil
Calling Cards	287-7089	13	Sara.holt@hood.army.mil
Cable cuts	287-5600	13 Rm 115	
Caltrop weekly bulletin	287-4318 fax: 287-6509	1001 Rm. E126H	jerri.sutton@hood.army.mil
Cellular Telephones	286-6662	13 RM	Dave.Jordan@hood.army.mil
Command administrative publications program	287-4318 fax: 287-6509	1001 Rm. E126H	jerri.sutton@hood.army.mil
Commander, 1114 th Signal Battalion	287-7109	13 Rm. 156	doimadmasst@hood.army.mil
1114 th Signal Battalion S3	287-7289		
Commercial Frequencies	287-8467		Roger.deweese@hood.army.mil
Copier program	287-4794 fax: 287-6509	1001 E125A	Mac.mcclain@hood.army.mil
DITSCAP	287-3261		Michelle.berry@hood.army.mil
DMS Local Control Center	618-8496	N/a	None
DOIM	287-7109 fax: 287-5530	13 Rm. 156	none
DOIM ISM coordinator	287-1052	13 Rm. 157	Anita.natonick@hood.army.mil
DOL E and C Shop	287-1202		None
Delegation of authority	287-0220	1001 Rm. E126	
Digging permits	287-9735 (read paragraph 4-4 first)	4612	none
Document Automation Production Service (DAPS)	287-7371	1001 E134	pat.grainger@hood.army.mil
Files management (MARKS)	287-0220 fax: 287-6509	1001 Rm. E125A	Michelle.james@hood.army.mil
Forms management	287-4974 fax: 287-6509	1001 Rm E125A	Linda.Jordan@hood.army.mil

(continued on next page)

Table B-1. Points of Contact (POCs) (continued)

Function	Telephone	Building and Room	Email
FOIA	287-0220 fax: 287-6509	1001 E125A	Michelle.james@hood.army.mil
Help desk (automation)	287-7312	13	helpdesk@hood.army.mil
Leased communications coordinator	287-4500 fax: 287-5530	13 Rm. 102	Regina.long@hood.army.mil
LCC	287-2277	13 Rm. 136	Robert.cabbagestalk@hood.army.mil
Management Information Control Officer (MICO)	287-0220 fax: 287-6509	1001 Rm. C125A	Michelle.james@hood.army.mil
Official mail	287-0095	1001 Rm. E130	Michelle.james@hood.army.mil
Office Symbols	287-4289	1001 Rm. C125	Michelle.james@hood.army.mil
Pay Telephones			
Postmaster	287-7312		postmaster@hood.army.mil
Printing	287-5630	1001 Rm. C125	Debbie.locklear@hood.army.mil
Publications Stockroom	287-3995	4254	Zanna.rayner@hood.army.mil
Sprint			None
Telephone Service Center	287-8177	13 Rm. 136	Sue.chandler@hood.army.mil
Training Support Center	287-4960	229	none
Web development	287-8176	13 Rm 156	webmaster@hood.army.mil

Appendix C Capability Request (CAPR) Formats

C-1. Introduction

a. A CAPR is a document requesting authority to get information management goods and services. CAPRs support and reference information contained in an approved requirements statement (RS) (formerly known as the DOIM information management plan (IMP) and/or automation plan).

b. A CAPR action is required for legal procurement of telecommunications equipment, software, hardware or services used in one or more information sub-disciplines.

C-2. Capability Request (CAPR) Flow

a. The originator of a CAPR is the user activity with an IM requirement. The activity writes the CAPR, submits it to the DOIM, and tracks its final approval. Upon approval, the activity initiates procurement through DOL.

b. Generally, a CAPR will apply to a specific requirement at a single location. When the requestors require to CAPR to apply to more than one location, they must list locations, buildings, and other pertinent information on a separate page and attach that page to the CAPR.

c. When preparing a CAPR, the first line of assistance for the activity or organization is the IMO. The IMO checks the CAPR for format and application to the user's activity requirements. Chapter 1 lists IMO duties and responsibilities.

d. The CAPR is then signed by the activity's approving authority.

C-3. Capability Request (CAPR) Processing

a. CAPR is the document that starts the procurement of IMA equipment. CAPRs ensure that the equipment fits the installation architecture, that there is a valid justification, and that the equipment will be used for authorized government function.

b. The IMO usually prepares a CAPR, but it may be prepared by the end user as long as the IMO reviews it. A sample CAPR showing bad justifications and good justifications is at Figure D-1. This should assist you in developing an effective CAR. Two things are fundamental in the CAPR:

- (1) What do you need?
- (2) What is the mission impact on acquiring it?

C-4. Capability Request (CAPR) Format: Telecommunication Equipment

The CAPR must be generated via Email from the unit IMO and forwarded to the DOIM. The CAPR must include the items that are outlined in the example in Figure C-1. No signature block is required. The narrative should be as long as necessary to clearly state all the details of the justification. An explanation of specific CAPR items are:

1. Date of request: self-explanatory.
2. Requesting organization and location: official designation of the organization or activity requesting the computer system.
3. POC: name, telephone number and organization or office of the individual who can provide additional information concerning the justification.

Figure C-1. Sample Capability Request (CAPR)

1. Hand Held Radios for Major Construction Project Surveys
2. John Sammis, DOIM, AFZF-IM-ISD-PB, 287-8274
3. Four hand held radios for remote communications for members of the Plans Branch that are engaged in conducting surveys in remote locations.
4. In order to reduce cellular phone bills there is a requirement for hand held radios in order to communicate with personnel conducting surveys in remote locations. The expense of the radios will be over come in less than a year by the elimination of the cellular phone bills for the four instruments currently in use
5. This devices must be compatible with the current radio trunking system currently in use on the installation.
6. The only commuunication requirement is to be tied into the trunking radio network.
7. No site preparation or construction is required.
8. Since this requirement is less than \$2,500.00 it will be funded and purchased using the IMPAC credit card.

sample

Appendix D Defense Messaging System (DMS) Registration and Use Guidelines

D-1. Registration

This appendix identifies procedures for the identification and registration of distinguished names (DN), roles and responsibilities of personnel appointed duties as sub-registration authority (SRA), organization registration authority (ORA), information system security officer (ISSO), mail list manager (ML MGR) and certification authority (CA) and guidance for registering tenant activities.

a. Registration roles and responsibilities.

(1) SRA. The SRA performs administrative functions required to process registration requests and to provide registration services. Responsibilities of the SRA are:

(a) Registering individuals and organizational roles.

(b) Registering O/R addresses for organizations, application entities and users.

(c) Registering component names and coordinating PLA-to-organization mapping.

(d) Performing registration activities within a certain time frame as specified by local standing operating procedures (SOPs).

(e) If an SRA delegates authority and responsibility of sub-trees to other SRAs/ORAs for registration activities, the parent SRA must create or be aware of the identity of the child SRA or ORA that will assume that authority and responsibility.

(f) Managing (making additions, deletions, update, etc. to) the delegated sub-tree(s), to include sub-trees that the SRA further delegates.

(g) Sending SRA approved technical object registration requests to the Service/Agency Registration Authority.

(2) ORA. The ORA is the POC between users and both the SRA and CA. The ORA function will be performed normally as an additional duty and can be filled by the organization's IASO, administrative officer, or branch administrative assistant. Appointment letters should be completed and a copy furnished to the 1114th Signal Battalion DOIM Attn: DMS SRA, 52d and Support Avenue, Fort Hood, Texas. There may be as many ORAs as necessary to conduct business in a timely manner that supports DMS and organizational schedules. Responsibilities of the ORA are:

(a) Verify the identity of prospective users based on two pieces of identification (one picture identification such as a military identification card, driver's license, or passport).

(b) Ensure user connects through approved interfaces (the UAs).

(c) Assign a DN as required and verify the uniqueness of the user's DN as specified on the X.509 certificate request form.

(d) Gather user information as requested and forward any X.509 certificate request forms to the SRA and CA for registration, directory entry, and certification.

(e) Ensure that the security clearance and level of access of prospective users is specified and approved by the supervisor of the person requesting registration (for classified DMS accounts).

(3) Certification authority (CA). CA personnel generate and sign the user's X.509 certificate and programs the PCMCIA (Personal Computer Memory Card International Association) card. Ensures that PCMCIA cards are issued only to appropriately cleared and authorized individuals.

b. Tenant activities and personnel. This section provides guidance for registration of tenant activities and/or personnel assigned to Fort Hood and are afforded the use of DMS. This includes individuals and organizations located at Fort Hood who are members of a service

agency other than the Army. The Navy, Air Force, Marines, and Coast Guard register their activities that are tenants on Army sites unless circumstances exist that require having the Army perform the registration functions.

c. DN. Entries in an X.500 directory are arranged in the form of a tree called a directory information tree (DIT). Each entry in the DIT is uniquely and unambiguously identified by its DN.

(1) Construction of DNs. SRAs/ORAs construct DNs by traversing the DIT.

(a) Based on information provided by the user, the SRA will create a common name (CN) and enter it in the directory tree under the property sub-tree. For example:

cn=III CORPS G1 SAFETY(n)

(b) The current version of DMS restricts the DN to 256 characters. The number of characters from the "c" in "c=us" to the last character in the leaf entry, including spaces and non-alphanumeric characters, cannot exceed 256 characters. For example:

/c=US/o=US GOVERNMENT/ou=DOD/ou=ARMY/ou=ORGANIZATIONS/1=CONUS/1=FORT HOOD TX/ou=III CORPS/ou=3 SIG BE 1114 SIG BN DOIM(N)/cn=3 SIG BDE 1114 SIG BN DOIM CDR(N)

(2) When constructing DNs for organizational accounts, use capital letters in the DN beginning at level 8. Number abbreviations cannot be used. For example:

ou=III CORPS/ou=3 SIG BDE 1114 SIG BN DOIM(N)/cn=3 SIG BDE 1114 SIG BN DOIM CDR(N)

(3) Organizational accounts DN should be the same in both the SBU and the SECRET DIT except that the three characters "(s)" will be appended to the name in the SECRET and "(n)" in the SBU DIT.

(4) Examples:

SBU

/c=US/o=U.S.
GOVERNMENT/ou=DOD/ou=ARMY/ou=ORGANIZATIONS/I=CONUS/I=FORT HOOD
TX/ou=III CORPS/ou=3 SIG BDE 1114 SIG BN DOIM(N)/cn=3 SIG BDE 1114 SIG
BN DOIM CDR(N)

SECRET

/c=US/o=U.S. GOVERNMENT/ou=ARMY/ou=ORGANIZATOINS/I=CONUS(s)/I=FORT
HOOD TX/ou=III CORPS/ou=3 SIG BDE 1114SIG BN DOIM(s)/cn=3SIG BDE 1114
SIG BN DOIM CDR(s)

d. Unit or organization appointed ORAs/IMOs must register and/or monitor registration requests.

(1) To use DMS, an organizational user requires an O/R address, a DN, an X.509 certificate, and a PCMCIA card programmed by an authorized CA.

(2) Prior to submission of a X.509 certificate request form, the unit or organization should determine:

(a) Who will monitor or coordinate the DMS process? This person will monitor the registration process. Note: ORA/IMO.

(b) Who will authorize the creation of the accounts? Note: recommend the ORA/IMO.

(c) What units or organizations are currently using AUTODIN? What users send and receive traffic through the Telecommunication Center (TCC)?

(d) What unit or organization has a requirement for DMS? Decide if there are any offices that require DMS that do not currently use AUTODIN. This affects the number of user agents and PCMCIA cards required.

(e) Who will be the release authority for the organizational box? The release authority should somewhat correspond with the individual(s) now authorized to send messages into AUTODIN. Anyone who can release a message can send a message into AUTODIN.

(f) Who will be the reviewer(s) for the organization box(es)? This individual can be the administrative personnel in the unit. Reviewers should be able to monitor the box most of the workday. Remember that high priority traffic will come to the organizational box, not the LCC. Reviewers are people who will need to monitor the box.

(g) Who will draft message? Release authorities do not normally draft messages. Identify personnel who will perform the task. These individuals need access to a DMS user agent but not a PCMCIA card.

(h) Who will provide 24-hour notification? Decide how 24-hour notification will be handled.

(3) Registration is closely linked with other activities that need to occur to provide service to a DMS user. For this reason, some of the tasks listed below are not strictly registration activities. Tasks 1 through 8 (paragraphs *a* through *h* below) are required to provide service to a DMS user. Tasks 5, 6, and 7 (paragraphs *e*, *f*, and *g* below) do not represent registration-specific procedures, but the tasks are required to establish user service.

(a) Task 1. Identify requirement and recipient of the account and DN. Performed by: ORA/IMO.

(b) Task 2. Creation of directory entry (based on the object or user's DN). Performed by: SRA.

(c) Task 3. Registration of address. Performed by SRA.

(d) Task 4. Initialization of the PCMCIA card X.509 certificate.

(e) Task 5. Configuration of user data in the MTA and MS. Performed by the CA.

(f) Task 6. Configuration of UA. Performed by the ORA/IMO.

(g) Task 7. Testing the user configuration. Performed by the ORA/IMO/SRA.

(h) Task 8. Organizational DN added to required MLs. Performed by SRA.

(4) 3-5.3. Local registration procedures. Registration is essential to the operation of DMS. Registration provides authoritative sources of information, promotes consistency, and prevents ambiguity in naming conventions. Registration of all users and organizations is critical to ensure correct routing, authentication, and decryption of messages. Local registration procedures are:

(a) User contacts their ORA and requests a DMS organizational account. Note: Unit or organization IMOs will perform the duties as ORAs.

(b) ORA constructs and verifies DN with the DMS directory. ORA can contact the DMS LCC for assistance.

- (c) ORA contacts SRA for verification of DN (optional).
- (d) ORA submits X.509 request form to CA. Prior to submission, ensure completeness (including all appropriate signatures).
- (e) DOIM ISSO verifies clearance level of requesting user (classified requests only).
- (f) CA "cuts" PCMCIA card.
- (g) X.509/Certificate given to SRA for creating account and posting certificate. SRA will submit request for PLA-DN association, add DN to MSs as necessary, and verify account setup. *Note:* Once account is created, the SRA will forward a DMS organization account notice to the recipient and copy furnish the ORA/IMO.
- (h) CA contacts the recipient or user for issuance of card and PIN letter. CA will contact the recipient via telephone or E-mail 3-5 days after submission of the X.509 certificate request form. The user must pick up the card or PIN letter from the Fort Hood DMS LCC. Call the LCC to confirm pickup. Table B-1 lists contact information for the LCC.
- (i) User informs ORA of receipt of card. Users should immediately inform their ORA of receipt of PCMCIA card for accountability and monitoring.

(1) Note 1. Users should allow 3-5 days after submission of X.509 certification request form. If you have not been contacted by the CA, you can call the appropriate SRA (See Table B-1), or the CA to inquire about the status.

(2) Note 2. Once contacted by the CA, users should pick up the card immediately.

(3) Note 3. COL and above can authorize, by memorandum, courier to pick up their PCMCIA card and pin letter. Courier will assume responsibility of the recipient's PCMCIA card.

(4) Note 4. Users should ensure that the proper version of the MS DMS Outlook User Agent software is installed. Instructions and software can be obtained from the DOIM file server at <\\N3CDOIMFILESVR1\DMSCLIENT\DOCS>.

(j) The address registered in the DMS directory for an ML is that of the MLA that hosts the list. The ML address is always included in the TO line of a message.

D-2. Mail Lists (MLs) .

a. A ML is an abbreviated address designator that represents frequently used combinations of action and information addresses. Its purpose is to reduce the length of message headers, which decreases administrative and communications processing time. MSs are useful for, but not limited to, sending messages regarding: alerts of exercises, emergency storm warnings, intelligence summaries, operation instructions, and movement or situation reports. MLs should not be established if other means of communication are available.

b. MLs hosted by the local MLA must be registered in the DMS directory in the same manner as MLs used for organizational messaging. The addresses registered in the DMS directory would be that of the local MLA. For example, the naming convention for the lists would be ML ALL FORT HOOD(N). MLs registered for local use will not be registered as all local users and recipients should be using only DMS at that point. Local MSs will not be routed between domains.

(1) Registering local MLs. MLs are maintained by the DOIM DMS Mail list managers (MLMGR) who have SRA access and create, edit, and delete rights over the specific MLs. The MLMGR is responsible for manipulation of ML directory data at the direction of the cognizant authority for that particular ML. Cognizant authorities have control over decisions to add or delete MLs, members, or users from a mail list.

(2) Units and organizations who require local ML must submit a request to the MLMGR through their ORA for creation of a local ML. Requests should include the cognizant authority POC name, telephone number, Email address, ML name, and ML members (must be valid DMS organizational users). Forward requests to dmsmlmgr@hood.army.mil.

cn=mlmgr-1 hood doim(n)/ou=lcc hood(N)/ou=III corps/1=fort hood
tx/1=conus/ou=organizations/ou=army/ou=dod/ou=U.S. Government/c=us).

(3) Local MLs will be registered under the ML agent name, for example:

Cn=all fort hood(n)ou=mlhftz(n)/ou=iii corps/1=fort hood
tx/1=conus/ou=organizations/ou=army/ou=dod/o=u.s. governemnt/c=us

D-3. Personal Computer Memory Card International Association (PCMCIA) Cards

a. A PCMCIA card is a PC card that uses approved algorithms and procedures to provide network related security services, data integrity, access control, authentication, non-repudiation, and confidentiality of user information. PCMCIA cards are authorized to protect unclassified and SBU information. Note: The NSA has also authorized the use of these cards under certain conditions for classified (PCMCIA For Classified).

(1) PCMCIA cards must not be used as general purpose data storage devices.

(2) Upon receipt of PCMCIA cards and pin, each user must read, sign, data, and return to the CA an advisory statement or receipt.

b. PCMCIA card handling.

(1) PCMCIA cards with certificates programmed for individual messaging must not be shared.

(2) PCMCIA cards designated for organizational messaging are intended for shared use by authorized users, but such cards must not be used for individual messaging.

(3) The maximum time for renewing, re-keying, and changing a PIN for a PCMCIA card is three years or 156 weeks. The CA notifies users when their certificate or key and PIN will expire. If a user fails to present their card to the CA within the designated time period, their certificate will be added to the Certificate Revocation List (CRL) and the user alerted that their certificate is no longer valid.

(4) Before departing an organization, each PCMCIA card user must return their card to the CA or their IMO or ORA. Failure to return a card will result in the CA reporting a security compromise.

(5) Users of PCMCIA SBU cards must maintain some form of record concerning the identity of all certificates their cards contain and the identity of the CA. Users should store the certificate report (PIN letter) provided with each card, so that the information it contains will be available in case it is required for compromise recovery.

(6) A PCMCIA card disables itself after ten consecutive failed attempts to enter the associated PIN. Users of disabled cards must contact the CA to arrange for card reactivation and new PIN assignments.

(7) PINs should be memorized and should not be written down on PCMCIA cards or recorded in any manner in the vicinity of the PCMCIA workstations. Users may record their PINs, provided the PIN records are stored securely and separately from their associated cards.

(8) A PCMCIA card must be protected like credit cards or other high value items. Protection must cover periods of non-use (such as vacations and leave). Programmed cards that are not in use should not be kept in an unlocked state.

(9) Users cannot repair or reprogram damaged or inoperable PCMCIA cards. Damaged or inoperable cards should be returned to the issuing CA who will determine if the card can be reused.

c. Reportable events are events which compromise the security of the DMS account, workstation, or the organization. Users must report the following events to the CA or IASO within one working day after the event happens:

- (1) Temporary or permanent loss of a PCMCIA card.
- (2) Actual or suspected compromise of the PIN associated with a PCMCIA card.
- (3) Actual or suspected misuse of a PCMCIA.
- (4) Unauthorized modification of PCMCIA software installed on a workstation.
- (5) Actual or suspected tampering with a PCMCIA card.
- (6) Unauthorized use of an authorized duplicate PCMCIA card.
- (7) Failure to report data changes to the CA.
- (8) Detection that a user's card is disabled prior to making ten unsuccessful

consecutive attempts to unlock it.

d. Recipients can use the Fort Hood LCC incident report located on the DOIM file server <\\n3cdoimfilesvr1\dms\documentation\fort> HOOD LCC INCIDENT REPORT.DOC or submit a memorandum of record to the CA to report PCMCIA card security issues.

D-4. Completing the X.509 Certificate Request Form

When applying for a DMS account, complete the X.509 certificate request form. This form defines the security clearances and privileges you can communicate with using the X.509 certificate. It will also be used to record administrative information pertaining to the holder. A blank X.509 certificate request form and instructions are located on <\\N3CDOIMFILESVR1\DMS\DOCUMENTATION>. Users may contact the DMS LCC for assistance completing the form.

D-5. Installing the Defense Messaging System (DMS) Microsoft® Outlook® User Agent

a. The DMS version of Microsoft® Outlook® adds specific features to the commercial Outlook® technology to comply with the specifications set forth by the DOD and offers robust messaging capabilities in an integrated, easy to administer solution which supports universal connectivity.

b. Installation of the Microsoft® DMS Outlook® UA is similar to the installation of the commercial version of Microsoft Outlook. The DMS Microsoft® Outlook® UA is installed in three phases:

- (1) Phase I. Installing commercial Microsoft® Outlook® client. If you already have Microsoft® Outlook® installed on the workstation, skip this phase.
- (2) Phase 2. Installing commercial product updates.
- (3) Phase 3. Installing the DMS client extensions.

c. Instructions are available for new installation as well as upgrading from a previous version of the DMS Client software. Find installation instructions on the DOIM file server at <\\N3CDOIMFILESVR1\DMS\DOCUMENTATION>.

D-6. Using the Defense Messaging System (DMS) Microsoft® Outlook® User Agent (UA).

a. The DMS version of Microsoft® Outlook® adds specific features to the commercial Outlook® technology to comply with the specifications set forth by the DOD and offers robust

messaging capabilities in an integrated, easy to administer solution which supports universal connectivity.

b. Instructions for using DMS Microsoft® Outlook® are available on the DOIM file server [\\N3CDOIMFILESVR1\DMS\DOCUMENTATION](#) and installed on a workstation during software installation..

c. Contact the DMS LCC for assistance completing the form. Contact information is in Table B-1.

D-7. After Hours Message Reception

a. It is the organization or unit's responsibility to provide alternate delivery of messages during any period in which the DMS Microsoft® UA is not operable. In DMS there are generally two types of message redirection; the originator requested alternate recipient (ORAR) and the recipient specified alternate recipient (RSAR).

b. The ORAR is used on high precedence messages. The alternate recipient is specified in a user's (recipient's) entry in the DMS directory. When the originator activates the service, the client will automatically include in your message the required information for both recipients (someone in the TO: or CC: line) as well as the alternate. This service is activated per recipient using the following instructions:

(1) Go to the DMS directory and look up the intended recipient (for example, Smith, John).

(2) Highlight the user and examine the user's attributes. The ALTERNATE RECIPIENT attribute is the recipient's alternate used for ORAR. The attribute value is a DN and will be used to look up the alternate recipient's entry in the DMS directory.

(3) Go to the DMS directory and look up the alternate recipient. Copy the entry to the personal address book and give it a name that associates it with the original recipient (e.g. Smith, JohnALT).

(4) Select all intended recipients in TO: or CC: fields(s) in the mail message.

(5) Under the PER RECIPIENT tab in military properties, highlight the name of the recipient that will have ORAR activated, in the RECIPIENTS: field, then under the ALTERNATE RECIPIENT FIELD click the SET button.

(6) Select the alternate recipient from the personal address book and click OK.

(7) Repeat steps (5) and (6) for any additional names.

(8) Click OK (return to message).

c. Setting recipient specified alternate recipient (RSAR). RSAR allows you to specify who will receive your mail when you are unavailable for an extended period. This service must be configured at the server by the DMS administrator. Consult your DMS administrator to configure this service.

D-8. Common User Terminal

a. There is a common user terminal available in the Fort Hood DMS LCC for classified users who do not have a SIPRNET connection. Users must have a valid DMS account and PCMCIA card to use the terminal.

b. Users may contact the DMS LCC (See Table B-1) for additional information.

D-9. Defense Messaging System (DMS) End User Training

The Fort Hood DMS LCC provides DMS end user training periodically. Contact the DMS LCC for a schedule of training.

D-10. Defense Messaging System (DMS) Help Desk Support

- a. Contact the Fort Hood DMS LCC for assistance in resolving DMS related problems.
- b. Table B-1 lists contact information for the DMS Help Desk.
- c. On-site assistance visits can be coordinated.

**Appendix E
Information Technology (IT) Standards****E-1. Interoperability**

- a. DOIM supports a Microsoft® operating system and Microsoft® office applications.
- b. In order to ensure interoperability, the following standard format (version) for all files shared on the ILAN must be embraced.
- c. Microsoft® Office 2000 SP1 is the standard office suite, subject to change pending future product releases.

E-2. Software standards

- a. The standard Email client is Microsoft ® Outlook® 2000. The continued use of Microsoft® Exchange® clients is discouraged.
- b. DOIM supports:
 - (1) Microsoft® Windows NT 4.0.
 - (2) Microsoft® Windows Workstation 4.0 with current service pack.
 - (3) Microsoft® Windows 2000 Professional.
 - (4) Microsoft® Office 2000 Professional.

E-3. Microsoft® Windows 2000 hardware standards

Hardware will be ordered from current Army contracts and, as a minimum, will consist of:

- a. Desktop or notebook.
- b. Pentium III 700.
- c. 128 MB Memory.
- d. 6.0 GB Disk.
- e. 24X CD-ROM.
- f. 56k modem (notebook only).
- g. 10/100 MB Ethernet Network Interface Card (NIC).
- h. Microsoft® Windows NT 4.0 or Windows 2000.
- i. PCMCIA slot.
- j. Set-D card reader.

Appendix F Information Technology (IT) Maintenance and Troubleshooting

Section I Introduction

One of the most important IMO duties is effective installation, troubleshooting (problem diagnosis) and repair automation equipment and software. The IMO is first line of support for an organization. As such, the IMO has the ability to make a significant difference. Effective installation and troubleshooting are ways to make that difference. Your abilities can reduce system down-time, improve productivity, and save the government money. The following sections will provide a basis for assisting you in these endeavors.

Section II Troubleshooting Concepts

F-1. Keep it simple and smart.

a. One of the most important concepts to remember when installing, troubleshooting or repairing equipment is “keep it simple and smart.” This concept is dedicated to the theory of starting from the basics.

b. When troubleshooting, ask yourself questions. Is the PC turned on? Is there power coming from the wall outlet? Does the same failure occur with other software or just one particular item? By remembering to start from basics and ask yourself the simplest of questions, you will be surprised at how many problems you will be able to repair without feeling overwhelmed. The tendency is to make problems much worse than they actually are.

c. The same is true for installations. Read the instructions and all updates first. Be sure to read instructions entirely, making absolutely sure that you understand them thoroughly and completely. Remember that there is nothing more frustrating than to have to start all over on something just because you forgot a step or guessed at a question. Do not be bashful. If you need help, ask another IMO or ask DOIM personnel.

Section III Diagnosis of Failures

F-2. Categories

a. Failures fall into two categories. It is very important to distinguish which type of error you are dealing with since failures often seem similar.

(1) The failure of previously working equipment or software which no longer functions properly (if at all) after installing or making changes.

(2) The failure of modified or newly installed equipment.

b. A major source of equipment related problems, especially during installations and on networks, arises from cabling. These problems include bent pins, loose connectors or improper cable type. When in doubt about the performance of a cable, swap it with a known good cable to verify failure.

c. Approximately 60 percent of all service calls placed are simple fixes that knowledgeable IMOs could have resolved.

d. In the diagnosis of software related problems, there is no substitute for familiarity and proficiency with software programs. If you are not familiar with the software, attempt to locate an individual in your office who is, or request assistance through the RSC/CSC – Information Centers and their help desks before making changes.

Section IV

The Directorate of Information Management (DOIM) Support Team

a. The DOIM Support Team provides a help desk for diagnosing software and hardware problems.

b. For all service requirements which you are unable to resolve on your own, please call the DOIM Support Team. Technicians will assist you as much as possible over the telephone or dispatch a maintenance technician to assist you. The Support Team will place a record of your call into the maintenance data base.

c. Support Team technicians require the following information to process your request:

- (1) Unit or organization name.
- (2) USERID.
- (3) Location of equipment.
- (4) IMO name.
- (5) POC at location and telephone.
- (6) Manufacturer or equipment.
- (7) Component or item name.
- (8) Serial number.
- (9) Description of the problem.

d. When providing a description of the problem, be as concise as possible. List all symptoms; write them down to prevent forgetting anything important.

e. The IMO is the focal point for installation of new equipment and software. Installation is considered the connection of peripherals to a CPU, not the installation of cards, components, or upgrades which require cover removal. Software installation is performed by the IMO in its entirety. Use only original software. It is the IMOs responsibility to complete and submit software registration and warranty cards. Keep manuals with the software. As with other problems, call the DOIM Support Team for assistance.

f. IMOs should make a reasonable effort to read documentation and other support material before calling the DOIM Help Desk. IMOs will assist end users with standard software such as Microsoft® Office 2000 and Outlook®. Training for these software packages is available through the G3 Education Center Computer Literacy Program.

**Appendix G
Excess Automated Data Processing (ADP) Equipment**

DOL will accept turn in of ADP/IMA equipment without DOIM staffing.

**Appendix H
Installation Local Area Network (ILAN)**

H-1. Installation Local Area Network (ILAN) procedures

- a. Purpose. To outline procedure for requesting Email accounts.
- b. Scope. Applicable to all personnel who are granted access to the Fort Hood ILAN.
- c. Background. Each activity has a limited number of network and mail accounts.

Individuals needing access to the MILNET for timekeeping or military pay data will be able to use the network accounts.

d. Authorized Email accounts are based on the BPA. Authorizations have already been established and provided to units and organizations.

e. Recommended distribution for accounts:

(1) Commanders, CSMs, and primary staff officers: normally 10 per battalion or 20 per brigade.

(2) Corps and Division G-Staffs

(3) Installation Directorates (for example, DPW, DOL): case-by-case.

(4) Authorized contractors: only if the COR states, in writing, that the service is within the scope of the contract.

e. Requests may be submitted electronically or by memorandum. All requests for account activation must be approved by the organization commander or director and submitted to *Postmaster - Fort Hood DOIM* (on the global address listing). Forward requests through the appropriate G6 or S6. Table H-1 lists information required for account activation:

Table H-1. Required information for account activation

Fields	Example
Last Name	Doe
First name	Jane
Middle initial	L
Rank or name title	MAJ
MSC or MACOM	DOIM
Organization, Section	1114th Signal Battalion Current Ops Div
Job title	S3
SSN	XXX-XX-XXXX
Office telephone	(254)287-1234
Office fax	(254)287-5678

H-2. Installation Local Area Network (ILAN) Deactivation Procedures

- a. Purpose. To outline procedure for removing accounts from the ILAN and Email network.
- b. Scope. Applicable to all personnel who have access to the Fort Hood ILAN.
- c. Background. Users who PCS, ETS, change duty positions, or otherwise leave the employment of the US government in the local Fort Hood area are not authorized access to the ILAN or the use of an Email account.

H-3. Installation Local Area Network (ILAN) Maintenance

- a. Purpose. To schedule normal maintenance on installation servers and other telecommunication assets.
- b. Scope. Applicable to all installation servers and infrastructure controlled by the DOIM.
- c. Background. Maintenance is required on all servers, controllers, routers, etc., managed by the DOIM. ILAN maintenance is performed each Thursday between 1600 and 1800.

**Appendix I
Internet****I-1. What is the Internet?**

The Internet, or International Network, refers to the world's largest computer network connecting thousands of networks worldwide and having a culture based on simplicity, research, and standardization based on real-life use. Much of today's leading-edge network technology came from the Internet community.

I-2. Connectivity

Access to the Internet for Fort Hood users is provided through the Non Secure Information Protocol Router Net (NIPRNET). Until such time that trunking between Fort Hood and the commercial Internet is upgraded, access to the Internet must be severely limited. IMO's can best restrict access by not loading web browsing software packages.

**Appendix J
Telephone Work Order Procedures****J-1. Introduction**

This appendix applies to all units on Fort Hood and is the primary guide for TCOs. It reiterates guidelines for requesting telephone service through unit TCOs. All telephone service fits into one of three categories; establish new service, change existing service, or fix existing service.

J-2. General

The installation telephone system is Army-owned. The telephone system provides prompt and efficient transaction of official military business. Any telephone work performed on Fort Hood, with the exception of telephone repairs, will be accomplished after a telephone work order (FHT Form 105-X1-1) has been completed by the customer or TCO, approved by the TCO, then reviewed by the Telephone Service Center. (See paragraph J-9 for instructions.) Accepted telephone work orders may not be accomplished first-come, first-serve. Due to the

nature of the III Corps and Fort Hood mission, work orders are assigned to technicians based on the work priority. Work orders must be submitted a minimum of 10 working days prior to date required.

J-3. Establish New Telephone Service

a. New telephone service requires a telephone work order (FH Form 105-X1-1) and a sketch of the building floor plan showing the exact desired location of the required instrument(s).

b. Complete blocks (b) through (E), blocks (G) through (I), block (K), and blocks (M) through (P) according to instructions in paragraph K-9 then submit the service request and floor plan to the unit TCO.

c. The TCO will check the service request(s) for accuracy, providing assistance when necessary to customers. The TCO will complete blocks (F), (Q), and (R), then submit the request and the floor plan (s) to the DOIM Telephone Service Center. Table B-1 lists contact information for the Telephone Service Center.

d. When asked and as time permits, the DOIM Telephone Service Center will assign a service order number to incoming work orders (block (A) on the Fort Hood Form 105-X1-1). The request is then part of a processing system and will be worked in due course.

e. TCOs may call or visit the DOIM Telephone Service Center during normal hours of operation (1200-1600, Monday through Friday) to determine the status of a work order. The DOIM Telephone Center will provide one of only two possible statuses for work orders establishing new service:

- (1) Assigned to Outside Plant.
- (2) Completed.

J-4. Disconnect Telephone Service

a. Although infrequent, there are occasions when units or supported organizations must depart the Fort Hood service area. TCOs must submit a work order to disconnect the telephone service.

b. Customers may complete blocks (B) through (E), blocks (G) through (I), block (K), and blocks (M) through (P) as instructed in paragraph K-9 then submit the service request and a floor plan to the unit TCO.

c. The TCO will check the service request(s) for accuracy, providing assistance when necessary to customers. The TCO will also complete blocks (F), (Q), and (R), then will submit the service request and with the floor plan(s) to the DOIM Telephone Service Center. Table B-1 lists the Telephone Service Center location and hours of operation.

J-5. Change Existing Service

Complete all information on a work order (FHT Form 105-X1-1) according to instructions in paragraph K-9.

J-6 Fix Existing Service

a. Customers can report military telephone malfunctions to the Telephone Test Desk by dialing 114 on active Fort Hood telephone lines. Repair teams will repair telephone malfunctions according to priority (for example, life or death functions such as military police, hospital emergency room, and etc.). All other repairs are first-come, first-serve.

b. Civilian telephone service.

(1) Sprint™ :Civilian repair service for any Sprint™ residential and small business users contact Sprint™ as listed in Table B-1.

(2) Report malfunctions of American Telephone and Telegraph (AT&T) pay telephones as listed in Table B-1.

J-7. Features

a. There are many telephone features available that if properly assigned, simplify the customers job. The TCO should know what these features are to help advise his or her customers.

(1) Standard features.

(a) The single line concept (SLC) is the assignment of a unique, individual, yet constant identifier telephone number to a communications instrument (telephone, computer, facsimile device, etc.). SLC provides the user a "private line" to the world:

(1) One telephone per desk.

(2) Group pickup - user can answer any incoming call in the office.

(3) Call forwarding - when user leaves the office, the telephone can be forwarded to another telephone number.

(4) Call transfer – the ability to transfer an incoming call to a different number.

(4) Three party conference- talk with two other callers simultaneously .

(5) Call hold - The user can put the current call on hold, and make a second call, then return to the previous conversation.

b. Special features include long distance civilian telephone service. Each individual is responsible for restricting long distance calls to matters that cannot be handled by electronically transmitted messages.

J-8. Pedestals

Submit request to activate or deactivate pedestals by completing a FHT Form 105-X1-1. Paragraph K-9 contains instructions to complete the FHT Form 105-X1-1.

J-9. FHT Form 105-X1-1, Communications Service Request

Customers may complete all items as required except block (A) (reserved for DOIM Telephone Service Center) and blocks (F), (Q) and (R) (which must be completed by the TCO). .TCOs must verify that all required portions of this request are completed prior to submission to the Telephone Service Center and any required floor plans are attached. Specific blocks to complete, listed by type of service required, are provided in Figure J-1.

J-10. FHT Form 105-X1-1, Communications Service Request

TCOs must complete this portion of the FHT Form 105-X1-1 (referred to as a telephone work order) .All information is required.

(a) The Telephone Service Center will enter the date submitted. The date service required should be at least 2 weeks after request was submitted. Remember that waiting to deliver a completed request does not count as submitting a request.

(b) Enter the name and telephone number of the person who has knowledge of the requirements.

(c) Specify the Division, Brigade, Battalion, and company if known.

- (d) Check the appropriate block: inside move means only the inside location of the telephone line will be changed. outside move indicates that the telephone instrument must be moved from one building to another.
- (e) Enter the telephone number for existing service. Leave blank for new service.
- (f) Current location of telephone line(s). Leave blank for new service.

Figure J-1. Sample FHT Form 105-X1-1 (Communications Service Request)

SUBSCRIBER IS REQUIRED TO ATTACH COMPREHENSIVE FLOOR PLAN OF FACILITIES. ALL COPIES TO BE SUBMITTED TO 1114TH SIG / DOIM - FORT HOOD SERVICE ORDER SECTION.		SERVICE ORDER NUMBER (FOR USE BY TELEPHONE SVCS CTR ONLY)	
DATE REQUEST SUBMITTED / DATE SERVICE REQUIRED 12MAR01/28MAR01		POC WITH EXACT LOCATION (TELEPHONE, BLDG, ROOM NUMBERS) Should be someone who will be at the location	
TO: TELEPHONE SERVICE CENTER 1114TH SIG / DOIM - FORT HOOD BLDG 13 FORT HOOD, TEXAS 76544		FROM: (UNIT / ACTIVITY) 1BN, 2BDE/4ID	UIC _____ SEQ # _____
(CHECK ONE ONLY)	<input checked="" type="checkbox"/> NEW SERVICE	TELEPHONE NUMBER XXX-XXXX	CLASS OF SERVICE REQUESTED <input checked="" type="checkbox"/> A2 <input type="checkbox"/> A3 <input type="checkbox"/> A6 <input type="checkbox"/> C <input type="checkbox"/> OTHER
	<input type="checkbox"/> DISCONNECT	OLD LOCATION (BLDG, ROOM)	NEW LOCATION (BLDG, ROOM)
	<input type="checkbox"/> INSIDE MOVE	PRESENT DIRECTORY LISTING	PROPOSED DIRECTORY LISTING Enter Accurate and Descriptive -Directory-Listing
	<input type="checkbox"/> OUTSIDE MOVE <input type="checkbox"/> OTHER		
SPECIAL FEATURES REQUESTED <input type="checkbox"/> CALL FORWARD - BUSY TO _____ <input type="checkbox"/> CALL FORWARD - NO ANSWER TO _____ <input type="checkbox"/> CALL FORWARD - INTRAGROUP <input type="checkbox"/> CALL PICKUP WITH _____ <input type="checkbox"/> SPEED CALLING		SPECIAL REQUESTS, SPECIAL EQUIPMENT, JUSTIFICATION, REMARKS, ETC. <div style="text-align: center; font-size: 2em; opacity: 0.5;">sample</div>	
FOR USE BY SUBMITTING UNIT COMMUNICATIONS CONTROL OFFICE			
NAME OF REQUESTER Name of the Requester should match the POC		CONTROL NUMBER	SIGNATURE OF TELEPHONE CONTROL OFFICER TCO must be on orders with the Telephone -Service Center
FOR USE BY TELEPHONE SERVICE CENTER PERSONNEL			
BLDG NUMBER	TERMINAL NUMBER	TERMINAL COUNT	CABLE PAIR

Appendix K Dynamic Host Configuration Protocol (DHCP) Configuration

K-1. Server properties.

Set conflict detection to "2." Setting the detection to "2" ensures that any IP address assigned dynamically by DHCP is checked twice before being assigned to ensure the IP address is not already in use. This limits conflicts on the network.

K-2. SCOPE Setups.

Scopes are based on the IP addresses and the sub-net mask used for creating the scope. Contact the DOIM Support Team for scope information. When creating the sub-net masks, balance the scopes between the two DHCP servers. Contact the DOIM Support Team for scope information.

K-3. Dynamic Host Configuration Protocol (DHCP) Client Settings in locations where DHCP scopes are assigned.

Windows™ 9x (where x is the version), Windows™ NT Workstation, and Windows™ 2000 Professional clients will configure their TCP/IP setup to use DHCP unless they are authorized to use a static IP address assigned to them by the Networking Section. File servers, print servers, application servers, network monitoring servers, and domain controllers will use static IP addresses and sub-net masks assigned by the networking section.

Appendix L Open Database Connectivity (ODBC)

L-1. Installing Open Database Connectivity (ODBC)

ODBC is a standard application programming interface (API) for accessing data in both relational and nonrelational database management (DBMSs). Using the ODBC API, applications can access data stored in a variety of personal computer, minicomputer, and mainframe DBMSs, even when each DBMS uses a different data storage format and programming interface. Users who need connectivity to production SQL Server databases, loaded on the DOIM server in building 13, must have ODBC software installed on their PCs. ODB is available from a number of vendors. This pamphlet assumes you will use Microsoft® Access version 7.0.

L-2. Before You Begin

- a. When asked for the `DATA SOURCE NAME` enter `HOODSQL1`.
- b. The `DATABASE NAME` will depend on which database you want to access.
- c. You must have a `USERID` and password to connect to the production database. The database name, `USERID`, and password can be obtained by having your IMO contact the Fort Hood Database Administrator (see Table B-1).
- d. Follow the instructions in paragraph L-2e, or use the step-by-step instructions on installing ODBC that is available through the help tool of your Access® program.
- e. To use the help tool in Access®:
 - (1) Open Access® on your PC.
 - (2) Click `HELP` on the Access® toolbar.
 - (3) Click `ANSWER WIZARD`.
 - (4) Type `ODBC` and click `SEARCH`.
 - (5) Click `INSTALL ODBC DRIVERS AND SET UP ODBC DATA SOURCES`.

L-3. Installing ODBC Drivers and Setting Up ODBC Data Sources

- a. When you installed Microsoft® Access, if you chose the custom installation option in the Microsoft® Access Setup program and left the data access option and the Microsoft® SQL server ODBC driver option under the data access option checked, then ODBC support and the Microsoft® SQL Server driver were installed on your workstation. If you did not, or if you chose typical installation, reinstall Access® and choose to add this component.
- b. You can install the Microsoft® SQL Server driver using the setup program, then use the ODBC manager (called the ODBC Administrator if you are using Microsoft® Windows NT) to specify data sources. You can also use the ODBC manager (or ODBC Administrator) to specify data sources for other installed ODBC drivers.

L-4. Installing the Microsoft® SQL Server Driver Supplied with Microsoft® Access

- a. To install the SQL server driver, run the setup program then click `ADD/REMOVE`.
 - (1) Click the `START` button.
 - (2) Choose `RUN`.
 - (3) Type `drive:setup.exe` then click `OK`. If you are installing from a network drive, click the `BROWSE` button, then use the `LOOK IN BOX` to locate the setup file.
 - (4) In the setup program, click the `ADD/REMOVE` button.
 - (5) Select `DATA ACCESS`.

(6) Click CHANGE OPTION.

(7) Click CONTINUE and follow the instructions in the remaining setup dialog boxes.

a. The Microsoft® SQL Server Driver Help file (Drvssrvr.hlp) provides detailed information on using Microsoft® SQL Server driver and setting up data sources for SQL Server databases.

b. The ODBC manager help (Odbcist.hlp) explains how to use the ODBC Manager (called the ODBC Administrator if you have Microsoft® Windows NT) to add, modify, and delete ODBC drivers and data sources.

c. Because the ODBC Help files are separate from the Microsoft® Access Help files and are meant to be used with a number of Microsoft® applications, you should keep the following information in mind when you use these files:

d. The Microsoft® SQL Server driver and ODBC Control Panel Option Help files are installed on your computer only if you have installed ODBC.

e. You cannot use the BACK button at the top of the help window to return to Microsoft® Access Help from one of these help files. You must reopen Microsoft® Access to return to the original Microsoft® Access help window.

f. The Microsoft® Desktop ODBC driver option of the setup program installs ODBC drivers for Microsoft® Access, FoxPro, dBASE, Paradox, Excel®, and text data. However, these drivers are not for use with Microsoft® Access®: they are supplied so that other applications such as Microsoft® Query can use them. To install drivers other than the Microsoft® SQL Server driver, get the files and documentation for that ODBC driver from the vendor of the data format. Microsoft® Access® requires 32-bit ODBC drivers that are in compliance with ODBC Level 1. Each ODBC driver has specific requirements for installing and setting up data sources. Refer to the driver's documentation for more information.

g. After the driver is installed, set up data sources using the ODBC manager according to the instructions below.

L-5. Setting Up Data Sources

a. If you installed the Microsoft® SQL Server ODBC driver when you ran the setup program, use the 32-bit ODBC Manager (or the ODBC administrator for Windows™ NT) to set up new data sources or modify existing data sources.

b. When you start the ODBC Manager (or the ODBC Administrator), click the help button in each dialog box to get help on how to enter the information in that dialog box.

c. In Microsoft® Windows 95, click the START button, point to settings, click CONTROL PANEL, then double-click the 32-BIT ODBC ICON.

d. In Microsoft® Windows NT, double click the ODBC ADMINISTRATOR ICON in the ODBC program group, or run the Odbcad32.exe program installed in the \WINDOWS\SYSTEM directory.

(1) To define a new data source for a currently installed driver, click ADD.

(2) To modify the definition of an existing data source, click a name in the USER DATA SOURCES LIST, then click SETUP.

L-6. Add data source Dialog Box

a. The ADD DATA SOURCE dialog box asks you to select an ODBC driver for which you want to add a data source. The installed ODBC drivers list contains the names of currently installed drivers. Additional ODBC drivers can be added through an ODBC application setup program. From the INSTALLED ODBC DRIVERS list, select the name of the driver that the data source will use (SQL server).

- (1) Choose the OK button.
- (2) Enter information about the data source.
- (3) The data source name can be anything that will help you remember what database this data source connects to. However, we strongly recommend that you use the actual database name here.
 - (a) The description may be left blank or you can enter a description of this data source.
 - (b) The server should be HOODSQL1
 - (c) NETWORK ADDRESS and NETWORK LIBRARY are blank.
 - (3) Click on the OPTIONS button.
 - (4) Enter information about the database.
 - (a) The DATABASE NAME must be the specific database you want to connect to. If the instructions are followed, this will be the same as the DATA SOURCE NAME.
 - (b) There can be only one database per data source.
 - (c) Obtain this information from the Fort Hood database administrator.
 - (5) Leave the LANGUAGE NAME blank.
 - (6) Click the OK button.
 - (7) Click the CLOSE button.
- b. The ODBC and at least one data source should have been successfully installed. If you require further assistance, contact the database administrator.

Appendix M
Digital Rules of Engagement (ROE)

Each end user should use these digital rules of engagement (DROE) to manage their ILAN-attached PC. Consider the edicts articulated in paragraphs *a* through *t* as the basic starting point in managing your portion of the Fort Hood information architecture.

- a. Do not store private data in public folders.
- b. Do not "reply all" unless necessary.
- c. Email attachments must not exceed 5MB.
- d. Email messages should not incorporate a background wallpaper option.
- e. Local data file backup and recovery is the end user responsibility.
- f. Mission essential video clips only.
- g. Must have current anti-virus signatures and definitions on computer to use Email.
- h. Must log into the Fort Hood to access Email.
- i. No chain letters.
- j. No jokes sent via Email.
- k. No signature blocks with pictures.
- l. Only trusted domains will be allowed to access HOOD domain resources.
- m. Send links to files instead of actual files.
- n. Set option to delete DELETED MAIL when you log off Outlook®
- o. Standard desktop operating system will be Windows™ 2000 Professional.
- p. Standard Email editor is Microsoft® Word 2000.
- q. Store all mail to a personal folder if at all possible.
- r. When forwarding a message delete unnecessary addresses.
- s. Zip or compress large files.
- t. Use common sense to preserve the information resources at your disposal.

Appendix N
Terminal Server Access Controller System (TSACS)

N-1. Terminal Server Access Controller System (TSACS)

- a. TSACS is a method for personnel to access their ILAN from remote locations for official government purposes. TSACS will not be used as a local Internet Service Provider (ISP)
- b. This guide assists you in establishing a connection to the network via a modem (dial-up) and the TSACS. This guide assumes you already have a TSACS account, a local USERID and password for the hood network, PCMCIA card and cable, telephone line, and your computer has the required software for an internet connection.

N-2. Setting up a Terminal Server Access Controller System (TSACS) Connection / Dial-up Networking.

Start the Windows™ 95/98 system. Double click on MY COMPUTER, then on the DIAL-UP NETWORKING icon that looks like figure Q-1:

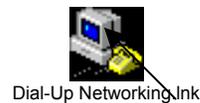


Figure N-1. Dial up networking icon

In the DIAL UP NETWORKING dialog box, double click on MAKE NEW CONNECTION

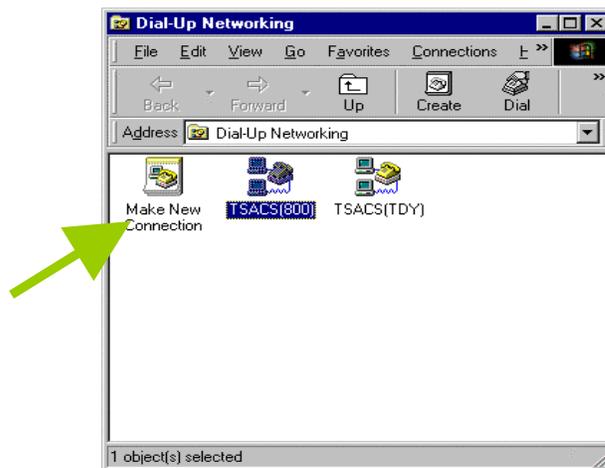


Figure N-2. Make new connection

In the make new connection dialog box, enter a name for the connection (use any name, i.e., TSACS, LOCAL, ETC...) (for illustration purposes, the name "local" is used).

Your modem will automatically display in the SELECT A DEVICE path. Now, click the NEXT button.



Figure N-3. Name the connection

Type the entire telephone number in the telephone number field. Do not put the area code in the area code box. Enter the number without dashes or spaces (i.e., 9,18006320196). See N-4 for a list of correct telephone numbers. The CONUS country code must be UNITED STATES OF AMERICA (1). OCONUS users must choose the appropriate country code.

Click on the NEXT button.

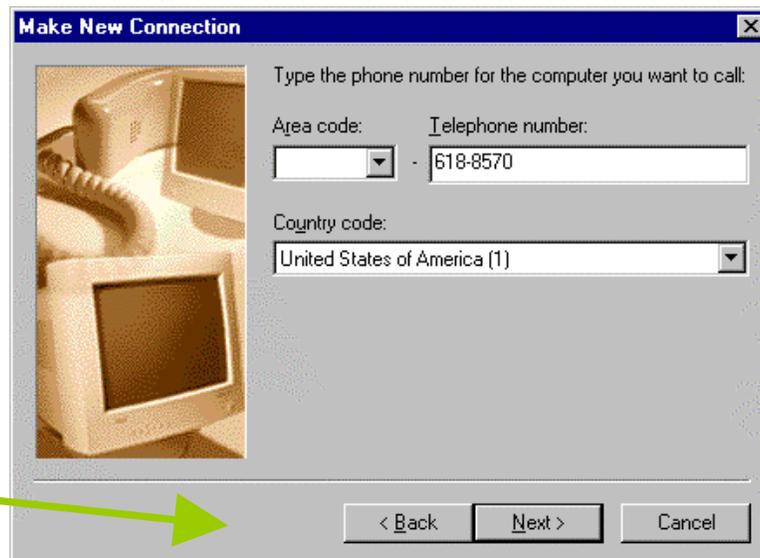


Figure N-4. Telephone number and country code

Click the FINISH BUTTON. In the DIAL UP NETWORKING BOX there should now be an icon for the new connection you just created.

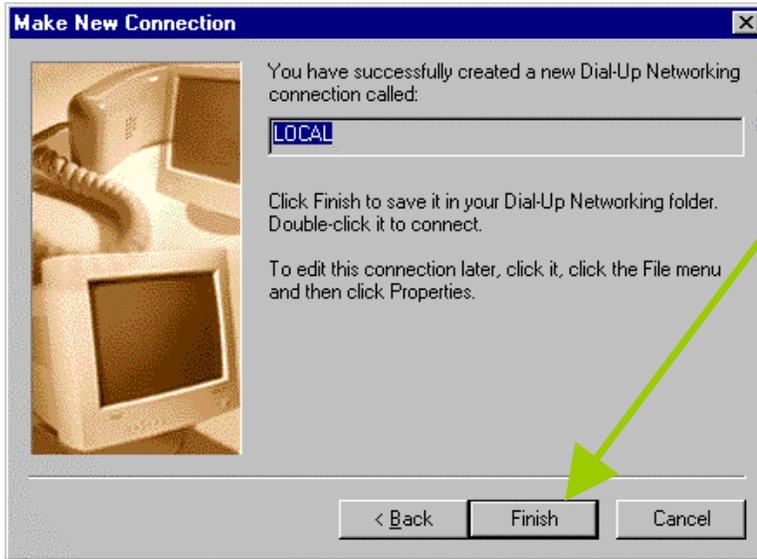


Figure N-5. Complete dial up networking

N-2. Setting Up Adapters and Protocols

Highlight the new connection icon by clicking on it once.

Select FILE then PROPERTIES from the menu items

or

while the cursor points to the icon, click the right mouse button, then click PROPERTIES.

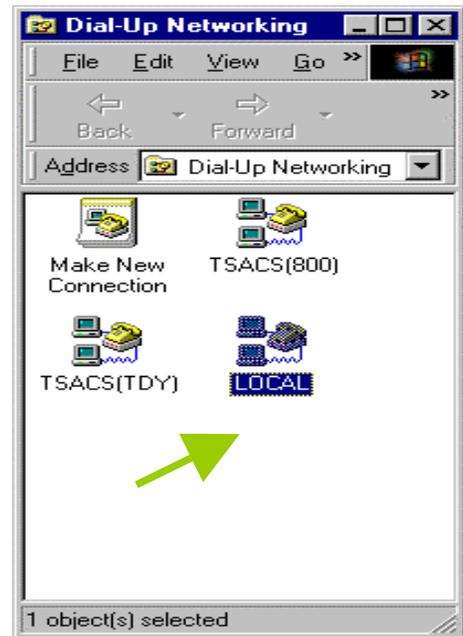


Figure N-6. Dial up networking properties

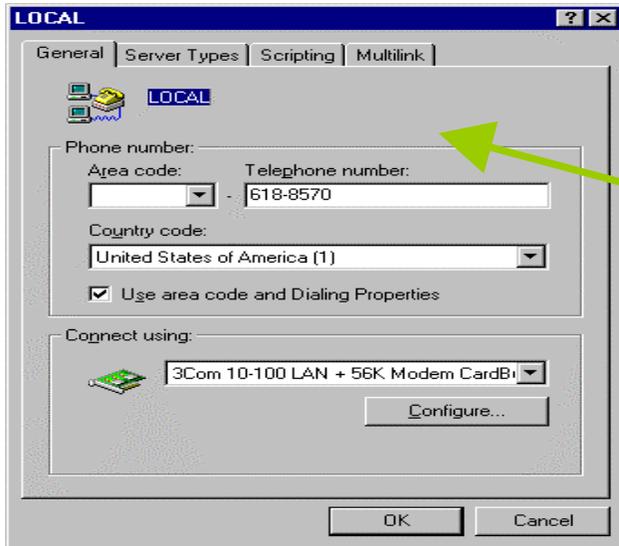


Figure N-7. Terminal server dialog box

In the TYPE OF DIAL UP SERVER: field, select PPP, INTERNET NT SERVER, WINDOWS 98

Under ALLOWED NETWORK PROTOCOLS make sure there is a check mark in front of TCP/IP

Click the TCP/IP SETTINGS BUTTON as shown in Figure N-8

In the TERMINAL SERVER DIALOG BOX, click the SERVER TYPES tab as shown in figure N-7.



Figure N-8. Server types

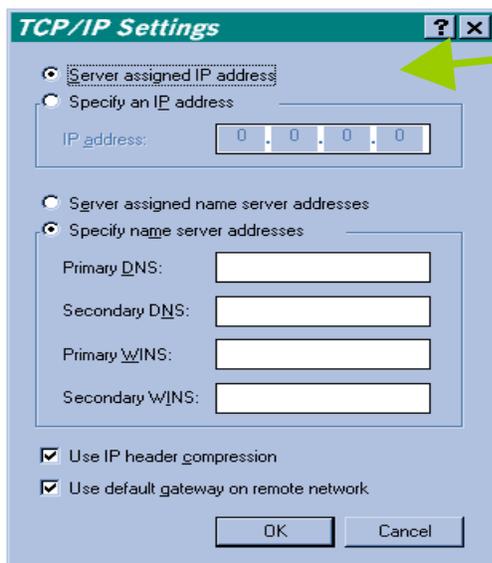


Figure N-9. TCP/IP settings

Select SERVER ASSIGNED IP ADDRESSES

Select SPECIFY NAME SERVER ADDRESS then type the DNS and WINS settings*:

Note: Contact the DOIM Support Team for current DNS and WINS settings.

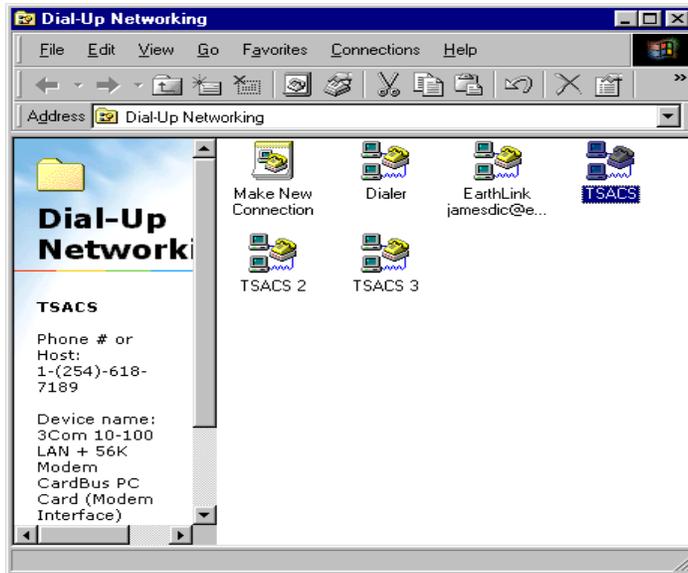
Make sure that there is a check mark in THE USE IP HEADER COMPRESSION and USE DEFAULT GATEWAY OR REMOTE NETWORK blocks.

Click the OK button

Congratulations. You have just created a dial-up connection to the terminal server.

N-3. Connecting to the Terminal Server

To make a connection to the terminal server, double click on MY COMPUTER



The MY COMPUTER dialog box displays. Click the DIAL UP NETWORKING icon.

When the dial up networking dialog box displays, double click the terminal server dial-up icon you created in section N-2.

Figure N-10. Selecting TSACS icon

In the connect to dialog box, enter your TSACS user name (see paragraph N-1b) and password then click on the CONNECT button.

Note: usernames always begin with HOD and the password must be lowercase



Figure N-11. Connecting to the terminal server

The CONNECTING TO TSACS dialog box appears and lists the status of the connection

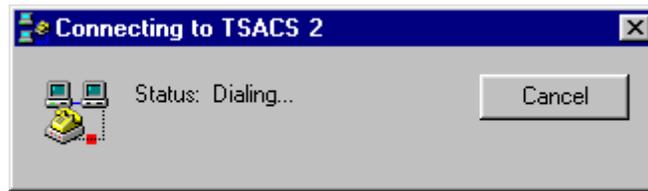


Figure N-12. Dialing status

Another CONNECTING TO TSACS dialog box appears and says that TSACS is verifying your user name and password

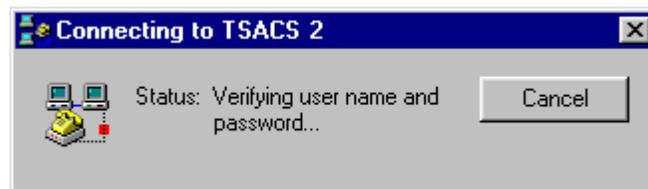


Figure N-13. Password verification

If prompted, enter your user name and password to the hood domain (the same user name and password you use when you connect to the ILAN.)

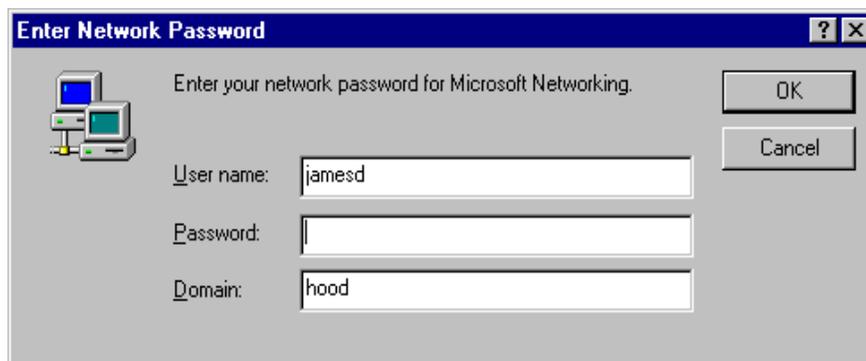


Figure N-14. Enter your ILAN password

A CONNECTION ESTABLISHED dialog box will appear as in figure N-15 that tells you the connection is complete.

You are now logged on to the HOOD domain. You may now launch your Email program the same way you do when you are in your office.



Figure N-15. Connection established

N-4. Points of Contact by Location

See <https://www.tsacs.army.mil/both/telephones/phony.html> for a complete listing of all available CONUS and OCONUS TSACS telephone numbers.

Appendix O Information Assurance (IA)

O-1. Information Assurance Security Officer (IASO) Responsibilities

- a. The IASO ensures IS under his or her purview is operated in a manner consistent with system accreditation, local policies, and AR 380-19 (Information Systems Security).
- b. The IASO must be appointed in writing, down to and including company-level, to monitor unit compliance. MSCs, division, staff offices, and garrison directorates will designate a lead IASO to be the POC to consolidate reporting requirements, receive information and disseminate information. Provide a copy of the lead IASO appointment orders to the appropriate III Corps and Fort Hood IAM.
- c. Protect IS under his or her control through cost effective physical security measures.
- d. Conduct IA security awareness training to include initial security awareness training to new users prior to issuance of password, quarterly reminder of consent to monitoring, and annual refresher IA training.
- e. Ensure IASO and SAs are certified according to AR 380-19
- f. Report vulnerabilities, security breaches, or virus attacks through channels to the unit IASO immediately. The unit IASO will telephonically report the incident to the III Corps and Fort Hood IAM and begin preparing an incident report in the format shown at figure O-1. If required, the DOIM will provide technical assistance to the IASO for the completion of the incident report.
- g. Conduct a risk management review to achieve the most effective safeguards against unauthorized disclosure of information, denial of service or use, and unauthorized use of IS.
- h. Takes physical and personal security measures to safeguard IS and information processed.
- i. Establish a vehicle for software control and accountability to prevent copyright violations according to AR 25-1.
- j. Ensure personnel out-process through their appropriate IMO or IASO to ensure DOIM receives notification to close Email accounts for departing personnel.
- k. Ensure commercial Internet services are not used for the conduct of official business.
- l. l. Ensure the proper destruction of non-functional computer hard drives.

O-2. Individual User Responsibilities

- a. Individual users may not transfer SBU information from the ILAN to any non-DOD system or network. SBU is that information dealing with logistics, medical care, personnel management, privacy act data, contractual data, For Official Use Only information, and certain categories of financial data. The III Corps definition of SBU is any DOD information on the ILAN that is generated for government purposes. Do not release government information to persons or agencies not affiliated with DOD. Protect SBU information to ensure confidentiality, availability, and integrity, and protection from foreign intelligence services or unauthorized personnel.
 - a. Safeguard government IA hardware, software and information.
 - c. Restrict unauthorized access to IS by safeguarding passwords and entry procedures. Password protected screen savers that lock the screen after seven minutes or less of inactivity will be used
 - d. Report vulnerabilities, security breaches, intrusion, monitoring, or anomaly and virus activity to the unit or activity IASO immediately.

e. Before using IS to process classified information, ensure that the IS is accredited to process classified information.

Figure O-1. Sample Incident/Intrusion Checklist

PROCEDURES FOR INCIDENT/INTRUSION HANDLING:

If you suspect that your system may be compromised take the following procedures and complete this form.

DO

- Disconnect the system from the network, contact your IASO, and the installation IAM.
- Access the system as root and perform a complete system backup to tape or CD.
- Confirm the integrity of the system backup and place in a restricted access location.
- Restrict physical access to the system until ACERT and CID can be contacted.
- Complete the following in detail and notify the Regional CERT and your local CID.
- Disable associated user accounts, if known, until CID determines investigative status.

DON'T

- Turn the system off or reboot the computer.
- Finger or attempt to contact the source directly.
- Alter or change the system files on the suspicious system.
- Connect to the system over the network.
- Allow any suspected individuals access to the system.

POC Name: SSG Jane Smith

Phone Number

DSN: 555-1234

Commercial: 212-555-1234

RANK/GRADE: SSG

Position: IASO

Unit: 4ID, DIVARTY

MACOM: FORSCOM

Installation: Ft Hood

Email address: jane.smith@hood.army.mil

ONLY INVESTIGATE THE CONFIGURATION OF THE SYSTEM ONCE A COMPLETE BACKUP HAS BEEN ACCOMPLISHED.

FHT Form 25-X28, March 2002 (DOIM) – page 1

sample

Figure O-1. Sample Incident/Intrusion Checklist (continued)

TARGET INFORMATION

Security classification: SBU

IP Address of the targeted system(s): IP 150.114.12.12 (even on DHCP, put the IP address of the system at the time of the incident. PORT: _____

OS of the targeted system: Win NT Version: 4.0/SP6.a

Domain Name of the Targeted system (ie worksta1.greedy.army.mil) n4iddivartysupoff.hood.army.mil

Date and/or level of Latest patch: 28Feb; Application – Office updates

System Hardware: (ie SUN/COMPAQ/DELL) Dell Optiplex

If web server, publicly accessible?: N/A

Security Mode of operation (dedicated/system high/multilevel etc) _____

Other software installed on the system? Office 2000/Adobe Acrobat Reader/IE 6.0/Formflow/WinZip

Unauthorized software installed on the system? YES
If yes, what type (IRC, Napster etc?) Morpheus

What AV product is installed on the system: Norton Corporate, 7.6

What was the latest AV update: 28 Feb 02

Were there any alerts from the AV product: NO
(if yes, identify the alert/warning: _____)

sample

Accreditation date: SSAA still being approved (Contact your IASO if this is unknown)

Trusted Host: (What other systems are trusted?) (What systems trust this host?)

IP address: _____ IP address: _____
IP address: _____ IP address: _____
IP address: _____ IP address: _____
IP address: _____ IP address: _____

Is there an approved login warning banner: YES

Information contained on the system: Admin/alpha rosters, supply orders, ncoers, email

Information available on the network: forms, manifests, publications

Figure O-1. Sample Incident/Intrusion Checklist (continued)

What was the system used for? Admin/Supply

Is there an Intrusion Detection Sensor monitoring this network: YES

If yes, what type? Real Secure

Are IDS logs available? YES

Can they be provided/accessed? Yes – contact the DOIM IA team

Is there a firewall protecting this system? YES

(If yes, what type? Cisco Pix 535

(Sidewinder/Raptor/Gauntlet/etc)

Are firewall Logs available? YES

Can they be provided/accessed? Yes – contact the DOIM IA Team

How was intrusion detected? What suspicious activity caused the investigation?

Individual had been on a 4-day pass; upon return, noticed files had been deleted and some changed. Event log (security) showed users logging in that should not have been. IE home page was changed, as well.

sample

What actions did the system administrator/security specialist take in this incident to date?

System was immediately disconnected from the network. User notified me, the IASO, and I notified Michele Berry, the IAM. Upon her direction, this report is being filled out. No one is being allowed to access the computer. Awaiting CID direction for a backup to be done.

THE BELOW INFORMATION WILL BE FILLED OUT AFTER THE INCIDENT IS REPORTED AND AN INVESTIGATION INTO THE BACKUP CAN BE DONE.

Has the site been blocked at the controllable security routers? YES NO

(If yes, how: _____)

How was the intruder able to access the system? _____

What was the exploit used if identified? _____

Figure O-1. Sample Incident/Intrusion Checklist (continued)

Level of access gained by the intruder? _____ (root/user level)

Was the system used to target another site? _____

Commercial/civilian: _____ (IP)
 Military _____ (IP)

Security status: Offline? YES NO
 (if no, why is the system still on line? (PDC/BDC/exchange server etc):

Has the system had a vulnerability assessment conducted in the past? YES NO
 (if yes, when? _____)

Has the system been compromised previously? YES NO
 (if yes, when? _____ How? _____)

Was the IP changed as a result of the previous compromise: YES NO

Has the password file been accessed or copied? YES NO
 (if yes, when? _____)

Has the system administrator changed root password for other systems? YES NO
 (if yes, when? _____)

Were files uploaded to the target system? YES NO
 (if yes, what type? _____)
 (names of files identified: _____)
 (can the files be provided: YES NO)

Has the system been scanned after the backup was conducted? YES NO

Have the results been provided? YES NO

Counter measure installed on the system? _____
 (ie TCP wrappers/shadowed password files/etc)

IMPACT: _____
 (ie compromised/denial of service/altered data/loss of server/etc)

Manhours involved: _____ (investigation)
 Manhours involved: _____ (recovery)

Any suspicious emails sent from the users account YES NO
 If Yes, what was the destination address? _____ (include copy)

sample

Figure O-1. Sample Incident/Intrusion Checklist (continued)

SOURCE INFORMATION

IP Address identified as potential sources (from files or logs):

IP: _____(PORT) _____

IP: _____(PORT) _____

IP: _____(PORT) _____

Source country: _____

Domain Name if available or resolved: _____

DATE/TIME of the session START: _____ STOP: _____

Attack Method: _____

Type of protocol: TCP UDP ICMP OTHER(_____)

Did a commercial entity provide notification to the POC: YES NO
(attach comments)

Did a commercial entity provide logs or files to the POC: YES NO
(attach comments)

sample

FHT Form 25-X28, March 2002 (DOIM) - page 5

Appendix P Information Mission Area (IMA) Training

Section I Information Mission Area (IMA) Training

P-1. Basic Training

Basic training to the new IMO starts with this handbook and attendance at the DOIM IMSC meetings. The IMO should read each issue of the *Bits and Bytes* newsletter (see Appendix T) to ensure he is on the mailing list. Additionally, training classes with various functional areas are offered. The IMO should select which classes may provide useful information. Functional area

P-2. Computer Assistance

The Support Team is the source for a variety of computer support services. Services include assistance in installing and configuring devices help in troubleshooting problems. The Support Team can provide assistance with many common PC components and COTS software products. While the level of knowledge varies between products and devices, many times a Support Team technician can provide useful insight and experience.

P-3. ACofS, G3 Education Services NCO Lead Computer Literacy Courses

The ACofS, G3 Education Services provides formal classes in computer related subjects and provides open computer labs to active duty military and others on a space available basis. The most current schedule is in the ACofS G3 public folder and provided through unit training coordinators.

P-4. Office Copiers Management

DOIM conducts training on management of office copiers as part of the quarterly Records Management Training class. The ACofS G3 announces the class on the Computer Literacy Schedule and assigns spaces for attendance. The class is open to both civilian and military personnel. DOIM Services Branch provides specialized sessions for TOE units upon request.

Section II Systems Administrator (SA) Training

P-5 Systems Administrator Certification

SAs must be level II certified. Information can be found on the Fort Hood home page (<http://pao.hood.army.mil>) under SYSTEM ADMINISTRATION AND NETWORK MANAGEMENT SECURITY COURSES.

**Appendix Q
 Directorate of Information Management (DOIM) Proxy Server**

Q-1. The proxy server

The DOIM proxy server makes the most efficient use of available bandwidth. This is accomplished by caching sites as they are requested on the proxy server's hard drives, then providing those sites to subsequent requesters at a much greater rate without having to use more bandwidth. Furthermore, the proxy server service prevents outside sources from identifying internal IP addresses, thus hiding the III Corps internal network from potential hazards and gaining the benefits of a domain name system (DNS) registered address. Instructions follow for configuring Internet Explorer™ versions 4.0 and 5.0, and Netscape™ Navigator version 4.6. If further instructions are needed, contact the DOIM Support Team at the contact information in Table B-1.

Q-2. The DOIM Proxy Service

- a. Instructions to use the DOIM proxy service are provided in paragraphs Q-3 and Q-4.
- b. Figures Q-1 through Q-7 depict steps necessary to configure a client machine to use the DOIM proxy service to access the Internet. The three most common browsers used on Fort Hood are illustrated in these instructions: Internet Explorer™ 4.0, Internet Explorer™ 5.0, and Netscape™ Navigator 4.6.

Q-3. Netscape™ Navigator 4.6 Proxy Service Instructions

Open Netscape™ Navigator.



Figure Q-1. Netscape Navigator open preferences

In the browser toolbar, click on EDIT then PREFERENCES.

Click ADVANCED.

Click PROXIES

Note: website appearance may differ from those shown in this pamphlet.

Next, click **MANUAL PROXY CONFIGURATION** as seen in Figure Q-2.

Click **VIEW**

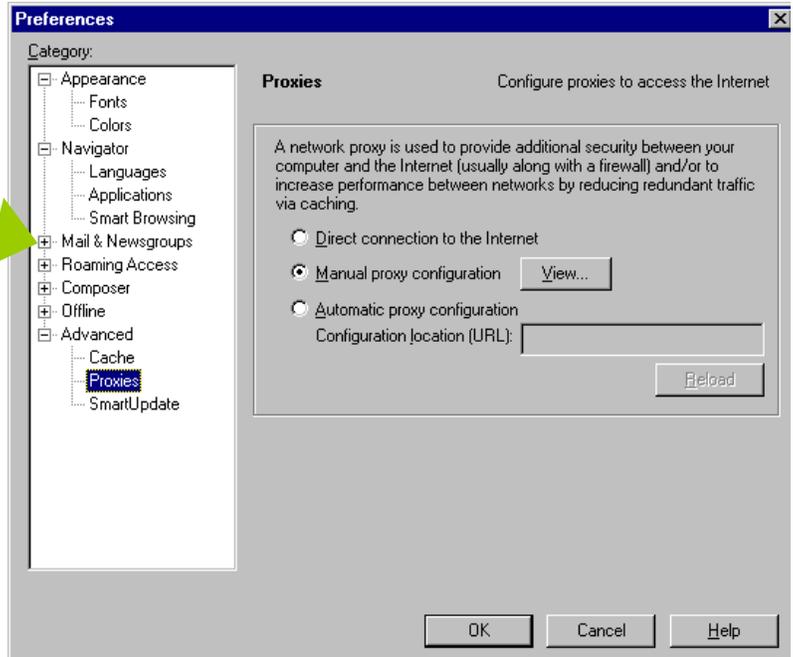


Figure Q-2. manual proxy configuration

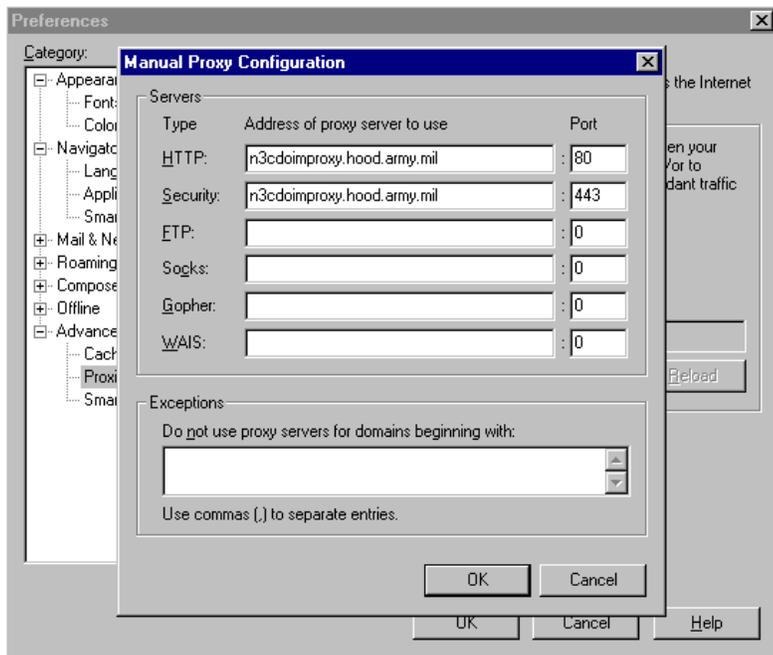
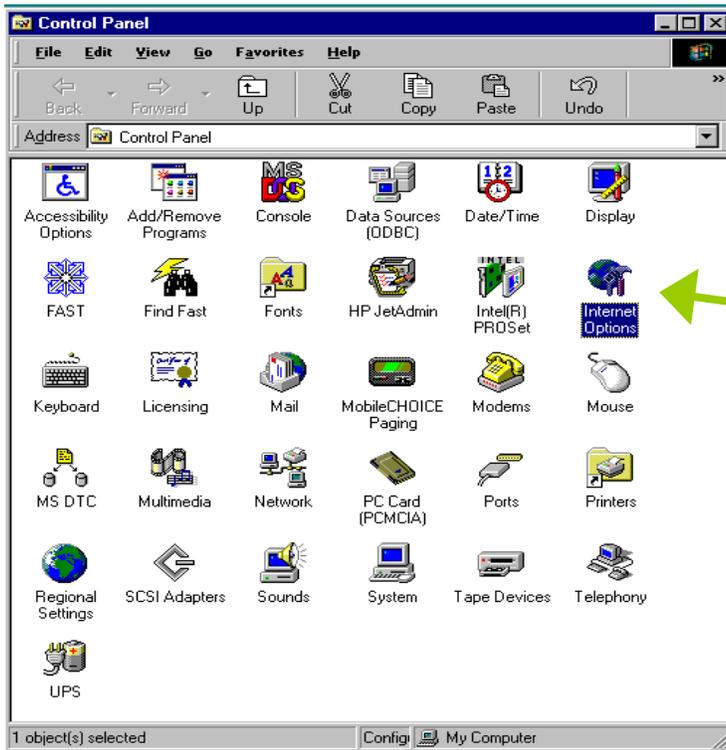


figure Q-3. Netscape™ Navigator exceptions

Enter the appropriate exceptions in the exception field (remember to use commas to separate the entries). Call the DOIM Support Team for current exceptions.

Notice that there is no entry for pclerk.hood.army.mil. This site can only be accessed using Internet Explorer 4.0 or greater.

Q-3. Internet Explorer Proxy Settings Instructions



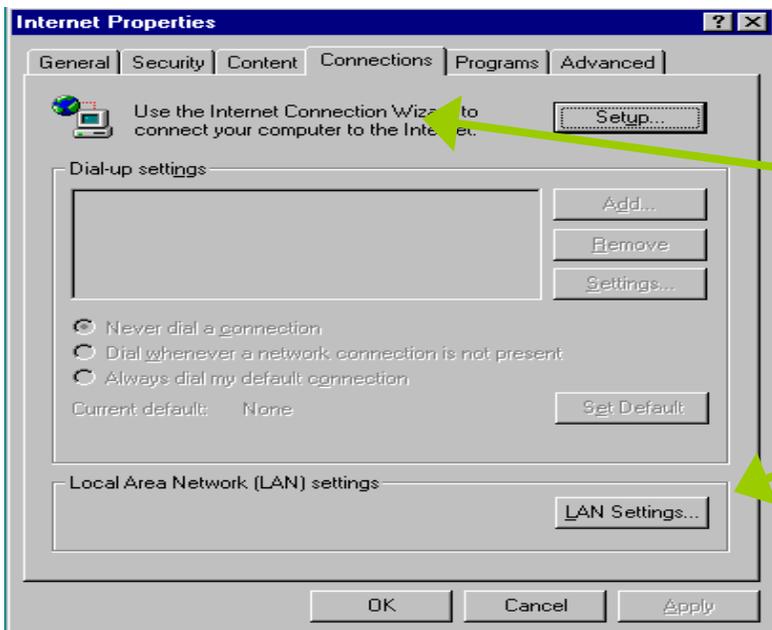
Go to CONTROL PANEL

Click START
Click SETTINGS
Click CONTROL PANEL

Click INTERNET OPTIONS

there is more than one way to do this, however these instructions provide the most direct route

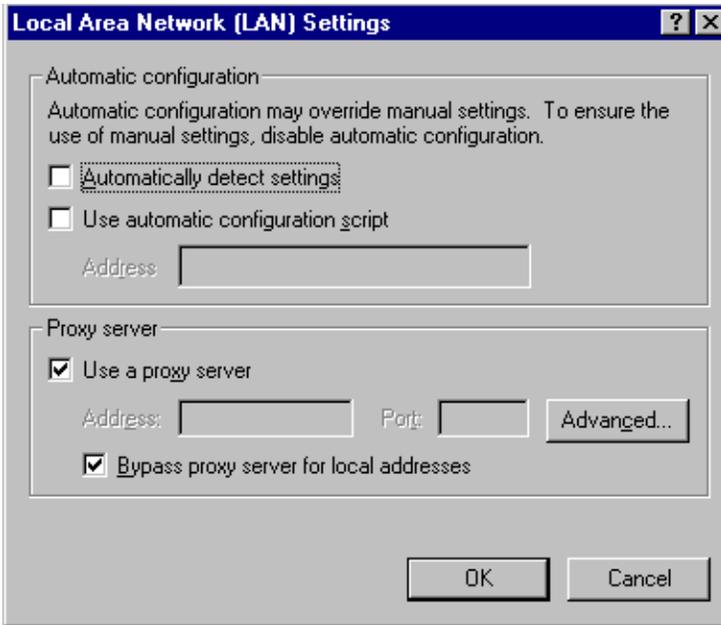
Figure Q-4. internet options



Click CONNECTIONS tab

Click LAN SETTINGS button

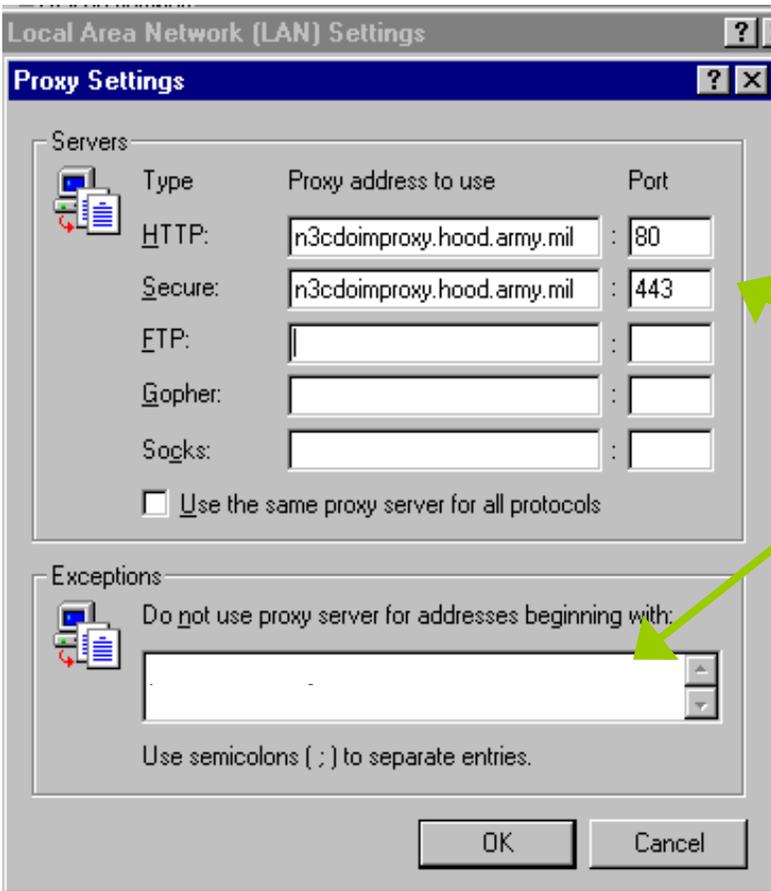
Figure Q-5. LAN settings



click the
ADVANCED button on
the LAN settings dialog
box as in figure Q-6.



Figure Q-6. advanced



type

n3cdoimproxy.hood.army.mil

in the HTTP and SECURE paths *only*

Type 80 in the port for HTTP

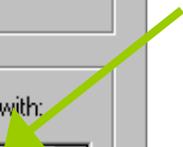
Type 443 in the port for
SECURE



in the exceptions box, type the
exceptions*.

*Call the DOIM Support Team for the
current exceptions.

remember to use semicolons as
separators.



Your proxy settings should look like
figure Q-7. Click OK three times:
Internet Explorer is set.

Figure Q-7. Complete Internet Explorer proxy settings

Appendix R
Leased Communications Lead times

Table R-1. Leased communications lead times

TYPE OF SERVICE	DISA LEAD TIME CONUS/ALASKA	DOIM LEAD TIME	TOTAL LEAD TIME	EXPEDITE CHARGES
	<i>calendar days</i>	<i>calendar days</i>	<i>calendar days</i>	<i>calendar days</i>
Point-to-point long haul circuits **includes exercise circuits	120	30	150	90 (variable)
All changes	70	30	100	90
FTS-2001				
Initial service to a new location—install new facility	120	30	150	n/a
800 service	30	15	45	N/a
Local service				
Telephone lines	N/a	30	30	N/a
Local leased (on Ft. Hood) Point-to-point circuits	45	15	60	N/a
Telephone calling cards	N/a	5	5	N/a

Note 1: Most actions can be successfully completed with the above timelines. Some actions may take longer.

Note 2. Lead times for OCONUS point-to-point circuits is 270 days.

Appendix S Shared Files and Shared Directories

S-1. Introduction

a. This appendix provides information on where and how to find shared information within the ILAN. Two sources of shared information are addressed in detail:

- (1) Public folders accessed through the ILAN Email system.
- (2) Shared directories accessed through the NETWORK NEIGHBORHOOD program within Windows™.

b. Now that computer connections to LANs are fully integrated into Fort Hood's daily routine, more ways are found to increase their efficiency. Shared directories and shared folders are valuable because they save space. As files are sent through Email to many recipients, server memory or the user's computer memory is used and sometimes used up to accommodate the duplication of each file. Each time an update is required, more memory is used to resent the update to all who need it. Shared directories and folders however, use one portion of memory and everyone accesses the folder to get the most up-to-date version.

S-2. Public folders.

Public folders may be accessed through your Outlook® 2000 client. The folders are categorized by unit or directorate under the Fort Hood public folders section.

S-3. Shared directories

The availability of any shared directory may be limited based on the administrator of the directory, the type of the computer used, the type of software used, or other factors. Shared directories may be found on the installation file server \\N3CDOIMFILESVR1\ which is accessible through a computer's NETWORK NEIGHBORHOOD applet.

- a. Right click on NETWORK NEIGHBORHOOD.
- b. Select FIND A COMPUTER.
- c. Type [\\N3CDOIMFILESVR1\](\\N3CDOIMFILESVR1)

Appendix T *Bits and Bytes* Newsletter

T-1. Introduction

Bits and Bytes is a quarterly newsletter published for the general Fort Hood community. This newsletter provides insight into IMA issues.

T-2. Distribution

Bits and Bytes is published electronically by the DOIM/1114th Signal Battalion Operations Officer and sent to IMOs. To receive a direct copy on the day of publication, send an Email request to the DOIM Help Desk (see Table B-1).

T-3. Archives

Volume 1, Issue 1 was published in July 1995. DOIM maintains up to 12 months of back issues in the DOIM public folder under *Bits and Bytes*. IMOs are encouraged to print and file issues of the *Bits and Bytes* with their copy of the IMO handbook.

Appendix U Public Key Infrastructure (PKI) – Medium Grade Services (MGS)

U-1. Requesting PKI MGS Certificates

Requests for PKI MGS “soft” certificates for Fort Hood personnel are limited to Army senior leadership (General Officers, Senior Executives, and selected senior staff members). Requests for all other personnel will be accepted pending the implementation of the Common Access Card (CAC). Ensure that the requestor has an Army Knowledge Online (AKO) Email address (for example, first.last@us.army.mil).

a. Submitting requests. Personnel requesting PKI/MGS certificates must complete the PKI certificate request form and forward to dmshelpdesk@hood.army.mil. The request form is located on the DOIM File Server (N3CDOIMFILESVR1/DMS/PKI/PKI Information).

(1) The application is forward to the Army PKI Local Registration Authority (LRA) for creation of the certificates.

(2) The LRA forwards the certificate registration Instructions to the Fort Hood PKI Trusted Agent (TA) who downloads the certificates and place them on diskette.

(3) Individuals are contacted for delivery or pick-up of certificates and coordination for installation.

(4). This process may take 4-5 days.

b. Lost and misplaced passwords. If password is lost or forgotten, request for new certificates must be submitted.

c. Certificates should be installed on any workstation (PC) that the individual uses for Email.

U-2. Export Certificates

a. If you lose your disk and have installed the certificates on one workstation, certificates can be exported from that workstation and installed on another.

(1) Open the Microsoft® Outlook® application. From the TOOLS menu, select the OPTIONS.

(2) The OPTIONS window will be displayed. Click the SECURITY tab. Click the SETTINGS ... button.

(3) Under the Digital IDs (certificates) section, click the IMPORT/EXPORT button.

(4) The Import/Export ID window will appear. Select EXPORT YOUR DIGITAL ID TO A FILE.

(5) Click the SELECT button and select the certificates you which to export.

(6) There should be three certificates listed. To identify the certificates, highlight the certificate and click the VIEW CERTIFICATE button.

(7) The certificate window will appear. Select the DETAILS tab and scroll down the field list to KEY USAGE. If the value of the Key Usage field is KEY ENCIPHERMENT(20), then the selected certificate is the encryption certificate. If the value IS DIGITAL SIGNATURE, NON-REPUDIATION(C0), then the certificate is the signature certificate. The third certificate listed with DOD CLASS 3 CA-3 is the ID certificate.

(8) Click OK to close the window.

(9) Select the certificate. Click the BROWSE button and select where you want the certificates stored. Ensure that you save the certificates as *.p12 files (ie. ID.p12).

(10) Enter the password that you used to store the certificates on the workstation. Click OK.

(11) You will need all of the certificates if you are planning to install them on another workstation. You must perform Section U-2, paragraph a., steps 1-10 for each certificate.

U-3. Installing DOD Class 3 Certificates for use with Microsoft® Products

a. Before installing the DOD Class 3 Certificates on the workstation, verify that the diskette (received from the DMS LCC) contains the correct files. The diskette should contain five files; one Identity certificate, one email signature certificate, one encryption certificate, and two root certificates.

b. Installing root certificates (*.p7b files).

(1) Double click (or right click) INSTALL CERTIFICATE DODROOT.p7b file to start the certificate manager import wizard. Click the NEXT button to continue.

(2) Accept the default option in the SELECT A CERTIFICATE STORE window. Click the NEXT button to continue.

(3) Click the FINISH button when the COMPLETING THE CERTIFICATE MANAGER IMPORT WIZARD window displays.

(4) Click the YES button when the ROOT CERTIFICATE STORE window displays. If the ROOT CERTIFICATE STORE window is not displayed, the root certificate has previously been installed. Proceed to step 6.

(5) Click the OK button when the IMPORT WAS SUCCESSFUL message displays.

(6) Repeat steps 2 through 5 to install MEDROOT.p7b.

(7) It is very important to install the Medium Assurance Root Certificate because many certificates have already been issued by the previous DOD PKI version and will not expire until their life span has expired.

c. Installing Identity and Email Certificates (*.p12 files)

(1) Double click (or right click INSTALL CERTIFICATE) file ID.p12. This will restart the *Certificate Manager Import Wizard*. Click the NEXT button to continue.

(2). You are prompted to select a file to import. Choose the default file name, which is the file you double clicked. Click NEXT to continue.

(3) Enter your Portable Security Password. This is the password that was given to you by the DMS LCC when your certificates were downloaded to your floppy. If you have forgotten the password, you must contact the DMS LCC to get new certificates.

(4) Check the ENABLE STRONG PRIVATE KEY PROTECTION and the MARK THE PRIVATE KEY AS EXPORTABLE boxes. Click the NEXT button to continue.

(5) Choose PLACE ALL CERTIFICATES INTO THE FOLLOWING STORE then click BROWSE .

(6) The SELECT CERTIFICATE STORE WINDOW appears. Highlight the personal folder. Click OK . The SELECT CERTIFICATE STORE window closes and the personal folder is automatically inserted into the certificate store field.

(7) Click NEXT to continue. The COMPLETING THE CERTIFICATE MANAGER IMPORT WIZARD window displays.

(8) Click FINISH .

(9) The default setting is MEDIUM. Change the security level by clicking SET SECURITY LEVEL.

(10) Set the security level to HIGH. Click NEXT to continue. Private keys secured with the medium setting are easily compromised. The MGS Program Office only recommends the high security setting. With this setting (high), your key will only be accessible with the appropriate password. Individuals who do not know your password are unable to use your key. In MGS terms, those individuals will not be able to read your encrypted e-mail or send e-mail

using your DOD PKI digital signature.

(11) After selecting the `HIGH SECURITY` option, label your key with the label `DOD PKI CERT`.

(12) Set a key usage password. To avoid confusion, it is recommended to use the password can be the one given to you by the DMS LCC. Click `FINISH` to continue.

(13) You will complete the installation process by using your private key for the first time. Enter your key usage password (step 12) and then click `OK`.

(14) Confirmation is received when you see `THE IMPORT WAS SUCCESSFUL` message. Click `OK` and you will return to the workstation's desktop.

(15) Finish installing your certificates by repeating steps 1-14 with the `EMAILID.p12` and `ENCRYPTID.p12` files. When you get to Step 11, simply make sure that `USE THIS PASSWORD TO ACCESS THIS ITEM` is selected and click `FINISH`. Skip Step 12, and go to Step 13.

(16) Selecting `USE THIS PASSWORD TO ACCESS THIS ITEM` enables you to keep the same password for all of your DOD PKI Certificates.

U-4 Configuring Microsoft Outlook 98/2000 to use DOD PKI Class 3 Certificates

a. You must have Internet Explorer 5.5 SP2 (128-bit encryption) and Microsoft™ Outlook 2000 SR1 SP2 loaded on the workstation/laptop.

(1) Open Internet Explorer and select `INTERNET OPTIONS` from the `TOOLS` menu.

(2) The `INTERNET OPTIONS` window will appear. Select the `CONTENT` tab and then select the `CERTIFICATES` button.

(3) The `CERTIFICATE MANAGER` window will appear. Before configuring Microsoft™ Outlook, verify that *all* certificates were loaded. The following certificates should appear under the `PERSONAL` tab:

2 -E-mail Certificates (DoD Class 3 Email CA-3)

1- Identity Certificate (DoD Class 3 CA-3)

(4) Once verification is complete, click `CLOSE` to exit window.

(5) Open the Microsoft™ Outlook application. From the `TOOLS` menu, select the `OPTIONS` item.

(6) The `OPTIONS` window will be displayed. Click the `SECURITY` tab. Click the `SETTINGS` button.

(7) The `CHANGE SECURITY SETTINGS` window will be displayed. Enter a name to label your security settings. Next, click the `CHOOSE` button to the right of the `SIGNING CERTIFICATE` field.

(8) There are two (2) certificates used for signing. Highlight the certificate that is issued by the `DOD CLASS ? EMAIL CA-?`. Click `OK`. Expand the `ISSUED BY` field (by clicking on the line to the right of the issued by and dragging) to ensure that you select the correct certificate.

(9) The `SELECT CERTIFICATE` window closes and you are returned to the `CHANGE SECURITY SETTINGS` window. The signing certificate is automatically inserted into the `SIGNING CERTIFICATE` field. The Hash Algorithm is `SHA-1`.

(10) Next, click `CHOOSE` to the right of the `ENCRYPTION CERTIFICATE` field.

(11) The `SELECT CERTIFICATE` window re-appears. There is one (1) DOD Class 3 Certificate used for encryption. Highlight that certificate and then click `OK`.

(12) The `SELECT CERTIFICATE` window closes and you are returned to the `CHANGE SECURITY SETTINGS` window. The encryption certificate is automatically inserted into the `ENCRYPTION CERTIFICATE` field. The Encryption Algorithm should be `3DES`. If `3DES` is not the default and is not in the drop down box notify your System Administrator. Your workstation

requires a 128-Bit Encryption pack.

(13) Check all the boxes in `CHANGE SECURITY SETTINGS` window to make sure your DOD PKI Certificates are your default settings for MGS.

(14) Once all the fields in the `CHANGE SECURITY SETTINGS` window are filled, click the `OK` button to accept the entered information and close the window.

(15) You will be returned to the `OPTION` window. Click the `OK` button to close. When you are back to your inbox. You can begin using MGS.

U-5 Sending and Receiving Messages

Note: To encrypt a message, the addressee must be pulled from the contacts folder.

a. Add the Signed/Encrypt Buttons to the toolbar

(1) Launch Outlook™. Select for `NEW MESSAGE` Item.

(2) On the toolbars, select `VIEW` then `TOOLBARS` then `CUSTOMIZE`.

(3) In the `CUSTOMIZE` window select the `COMMANDS TAB`.

(4) Scroll down the `CATEGORIES` column to `STANDARD`.

(5) In the `COMMANDS` column scroll down and highlight `ENCRYPT MESSAGE CONTENTS AND ATTACHMENTS`. Drag and drop it on your toolbar. Repeat this for `DIGITALLY SIGN MESSAGE`.

(6) Close the `CUSTOMIZE` window.

(7). Close the message.

b. Sending Signed or Encrypted Message To Contact

(1) Launch Outlook™. Select for `NEW MESSAGE` Item.

(a) `TO:` address must come from the contacts folder – Select contacts addressee

(b) Type message. Select `ENCRYPT AND DIGITALLY SIGN` (these are the blue lock and red ribbon/ink pen icons on the toolbar).

(2) Select `SEND`. Enter private password key to release secure message. Click `OK`. Blue lock seal is on the envelope of the sent message (check `SENT ITEMS` to confirm) Recipient *must* open with their private password key and must have the sender's public key imported into Outlook™ contacts.

c. Receiving Signed or /Encrypted Messages.

(1) From Outlook™, double click to open the mail message. A window opens and prompts for *your* private password key

(2) Enter your password.

(3) Click `OK`. The mail can now be read. Blue lock icon (on envelope) represents encrypted and red ribbon (on envelope) represents digitally signed.

(4) Right click on `FROM` address and `ADD TO CONTACTS` (if needed).

d. 5-4. Sending signed *only* messages

(1) Launch Outlook™.. The `TO:` address can be from the global, personal or contacts addresses. Type the message.

(2) Select to digitally sign (Red Ribbon or Ink Pen icon button). Select `SEND`. Enter private key to release if correctly set for a high security level.

(3) Click `OK`. Both PKI and non-PKI recipients can read digitally signed *only* messages like unencrypted emails

e. Retrieving PKI Email "Public" Certificates from signed and/or encrypted message. A received PKI signed message displays a red ribbon icon in the right margin of the window header (a blue lock indicates encrypted).

(1) Open the message.

(2) Right click on the sender's name (`FROM` line).

(3) From the pop up menu, select `ADD TO CONTACTS`.

(4) A contact window will appear with the individual's information. Click the `SAVE AND CLOSE` button on the toolbar.

(5) This adds a PKI Email "public" certificate to an existing contact or to a new contact addressee.

f. Verifying Valid Certificate (optional)

(1) Select the individual's contact from the contacts list.

(2) The contact window will appear with the individual's information. Additional information (phone numbers, job title, etc.) can be added.

(3) Select the `CERTIFICATES` tab. If the individual have valid certificates, the name and `USERID` will be displayed in the `CERTIFICATES (digital Ids)` block.

(4) Highlight the entry and press the `PROPERTIES` button.

(5) The `CERTIFICATE PROPERTIES` window will appear.

(6) Select the `DETAILS` tab and scroll down. The field `SUBJECT ALTERNATIVE NAME` will display in the Value field the Email address linked to the certificate. The `KEY USAGE` field should indicate `KEY ENCIPHERMENT(2)` in the `VALUE` column.

(7) If the key usage value does not indicate key encipherment(20), you do not have the individual's public key. You will need to add it again from a signed message from the individual or directly from the directory.

U-6 Section 6 Forwarding Army Knowledge Online (AKO) Email

a. Modifying your AKO account to forward all mail received requires that you access only the local `Microsoft™ Exchange` mailbox.

(1) Start your web browser and connect to the AKO web page at

<http://www.us.army.mil>.

(2) Login with your user name and password.

(3) Click the `PERSONALIZE` link on the right side of the web page. The `ARMY KNOWLEDGE ONLINE: PERSONALIZE YOUR PORTAL – INTERNET EXPLORER` window will appear.

(4) Click the `USER PROFILE` button. THE `ARMY KNOWLEDGE ONLINE: VIEW AND CHANGE YOUR USER PROFILE – INTERNET EXPLORER` window will appear.

(5) Enter your local email address in the `FORWARDING EMAIL ADDRESS` field.

(6) Click the `SUBMIT` button. You should receive an `UPDATE SUCCESSFUL!` dialog box.

(7) Click `OK`.

b. When a user sends mail, the recipient will see the `@us.army.mil` address when they reply to the sender's e-mail message.

c. The Exchange Site System Administrator will also add your AKO email address to your local account and set it as the reply address. This allows recipients of your signed or encrypted mail to retrieve the correct certificate. The recipient will also see your `@us.army.mil` address when they reply to your message.

d. Users on the same Exchange™ site or on sites that perform directory replication with the local site will, by default, route mail to the recipient's local address and not the SMTP address of `@us.army.mil`.

U-7 Importing Contacts List

Contacts lists provide an easy way for individuals to transmit signed and/or encrypted email to addressees. Currently, there are two contacts list provided to assist users; the `GO Contacts`

List, which is maintained by PM SET-D and USAISEC and forwarded to the FORSCOM PKI PM for dissemination, and the Hood PKI Directory Contacts List, which is maintained by the Fort Hood DMS LCC (TA). Both contacts lists are updated as needed. Updates to these lists will be forwarded via email as required. Contacts lists (.pst files) are located on the DOIM File Server (N3CDOIMFILESVR1\DMS\PKI\CONTACTS) Note: The .pst file name will contain the date (i.e. PKI Directory 141201.pst). Any corrections or modifications to the Hood PKI Directory can be sent to dmshelpdesk@hood.army.mil.

a. Hood PKI Directory and GO PKI Contacts List

(1) Copy the most recent .pst file to your hard drive. Do not select the desktop because the file will remain in use and you will not be able to delete it.

(2) Highlight the contacts entry in the folder list of Outlook.

(3) Go to FILE/IMPORT OR EXPORT.

(4) The IMPORT AND EXPORT WIZARD window will open. Select IMPORT FROM ANOTHER PROGRAM OR FILE .

(5) Select NEXT.

(6) Select PERSONAL FOLDER FILE (.PST) from the IMPORT A FILE window. Select NEXT.

(7) In the IMPORT PERSONAL FOLDERS window, select browse for the file to import.

(8) Highlight the .pst file that was previously saved on the hard drive.

(9) Click OPEN. Ensure replace duplicates with items imported is selected. This will allow any new information or certificates to replace the old.

(10) Select NEXT.

(11) Select PERSONAL FOLDERS. Ensure that you click on both INCLUDE SUBFOLDERS and IMPORT ITEMS INTO THE SAME FOLDER IN YOUR MAILBOX.

(12) Click FINISH. A new subfolder named Hood PKI Directory or GO PKI is added under contacts.

(13) Right click on the Hood PKI Directory or GO PKI Contacts and select PROPERTIES.

(14) In the DIRECTORY PROPERTIES window, select the OUTLOOK ADDRESS BOOK tab and check the box for SHOW THIS FOLDER AN E-MAIL ADDRESS BOOK.

(15) Click APPLY then OK.

U-8 Downloading Addresses from the Directory using Lightweight Directory Access Protocol (LDAP)

a. Configuring the user's Microsoft™ Outlook client for LDAP allows the user the convenience of populating or updating a contacts folder with the most commonly addressed PKI users and to allow real-time access to the DOD PKI directory to address recipients not currently in the contacts folder.

b. Microsoft™ Outlook 2000 with SR1 and SP2 is required to provide CRL checking for non-repudiation and LDAP functionality.

c. Configure Outlook

(1) If open, close Outlook.

(2) On the desktop, right click on the Outlook icon and select PROPERTIES.

(3) At the Microsoft™ Exchange Settings Properties window

(a) Click ADD.

(b) Select MICROSOFT LDAP DIRECTORY and click OK.

(c) Enter the following LDAP lookup properties:

Directory Service Account: DoD PKI Release 2
Server Hostname: email-ds-3.c3pki.chamb.disa.mil
Server Port Number: 389
Search Base: ou=pki, ou=dod, o=u.s. government, c=us

(4) When you are finished, close all windows.

(5) The creation date of the certificate identifies the certificate release. Each directory list contains entries of various releases. If you do not know which release an individual may have and/or you do not find the entry that you are searching for, search another directory.

b. Using LDAP to query directory.

(1) Open Outlook.

(2) Open Personal Address Book.

(3) In the SHOW NAMES FROM THE: FIELD, click the drop down arrow to display all address lists (the LDAP entries will be at the bottom of the list).

(4) Select the email-ds-3.c3pki.chamb.disa.mil entry

(5) Click the FIND ITEM button. Enter the individual's name.

(6) When results are found, all entries meeting the search criteria entered will display.

The SHOW NAMES FROM THE: field will display Search Results.

(7). The information found would also be kept and displayed the next time you select the LDAP address list.

(8) You can right click the entry and select ADD TO PERSONAL ADDRESS BOOK or FILE/ADD TO PERSONAL ADDRESS BOOOK. Reminder: Addresses for sending encrypted mail must be maintained in your contacts list.

Glossary

Section I. Abbreviations

AA

Automation architecture

AAFES

Army Air Force exchange service

ACP

Allied communication publication

ADP

Automated data processing

ADPE

Automated data processing equipment

AE

Automation equipment

AGP

Accelerated graphics port

AIG

Address indicator group

AKP

Army knowledge online

AMHS

AUTODIN mail host server

AMME

AUTODIN multi-media exchange

AMS

AUTODIN mail server

API

Application programming interface

APO

Army post office

ASC

Automatic switching center

ASEMH

Army standard Email host

ASIMS

Army standard information management system

AT&T™

American Telephone and Telegraph™

ATM

Asynchronous transfer mode

AUTODIN

Automatic digital network

BASOPS

Base operations

BPA

Blanket purchase agreement

CA

Certification Authority

CAC

Common access card

CALC

Computer assisted learning center

CAMO

Corps automation management officer

CAPR(s)

Capability request

COMOPS

Communications operations summary

COMSEC

Communications security

CONUS

Continental United States

COOP

Continuity of operations

15 OCTOBER 2001

III CORPS & FH PAM 25-5

COTS

Commercial off-the-shelf

CQ

Charge of quarters

CRI

Collective routing indicators

CSA

Chief of Staff, Army

DA

Department of the Army

DASD

Direct access storage devices

DBM(s)

Database management

DCO

dial central office

DCP

Directorate of Civilian Personnel

DD

Defense Department

DDN

Defense data network

DDN/TAC

Defense data network/terminal access controller

DHCP

Dynamic host configuration protocol

DII

Defense information infrastructure

DISA

Defense Information Systems Agency

DIT

Directory information tree

DITCO

Defense Information Technology Contracting Office

DOD

Department of Defense

DOIM

Directorate of Information Management

DOL

Directorate of Logistics

DMS

Defense messaging system

DN

Distinguished names

DNS

Domain name system

DOL

Directorate of Logistics

DPW

Department of public works

DROE

Digital rules of engagement

DSN

Defense switched network

DTG

Date time group

Email

Electronic mail

FA

Functional Area

fax

Facsimile

FM

field manual

15 OCTOBER 2001

III CORPS & FH PAM 25-5

FMC

Forms Management Coordinator

FMO

Forms Management Officer

FOIA

Freedom of Information Act

FORSCOM

Forces Command

FRC

Federal records center

GFE

Government furnished equipment

GO

General officer

GWACS

Government agency contracts

HMW

Health, morale, welfare

IA

Information assurance

IASO

Information assurance security officer

IAVA

Information assurance vulnerability

IDIQ

Indefinite quantity

IEEE

Institute of Electronic and Electrical Engineers

IFMO

Installation Forms Management Officer

ILAN

Installation local area network

IM

Information management

INMARSAT

International maritime satellite (service)

IMA

Information mission area

IMO

Information management officer

IMRB

Information management review board

IMPAC

International Merchant Purchase Authorization Cards

IMSC

Information management support council

IP

Internet protocol

IPBO

Installation property book officer

IRHA

Installation records holding area

ISA

Industry standard architecture

ISDN

Integrated services digital network

ISM

Installation support module

ISSO

Information System Security Officers

IT

Information technology

ITS

Information transport system

JANAP

Joint Army, Navy, Air Force AUTODIN policies and procedures

JTA

Joint technical architecture

KVDT

Keyboard video display terminal

LAN

Local area network

LATA

Local access and transport area

LCC

Local control center

LCR

Least cost routing telephone system

LEC

Local exchange carrier

MACOM

Major Army command

MAD

Message address directory

MCA

Military construction Army (projects)

MDT

Message distribution terminal

MEDDAC

Medical Department Activity

MICO

management information control officer

ML

Mail list

MLMGR

Mail list manager

MMCA

minor military construction army

MODEM(S)

Modulator(s), demodulator(s)

MPD

message preparation directory

MGS

Medium grade service

MICO

Management Information Control System

MICLO

Management Information Control Liaison

MSC

Major subordinate command

MVS

Multiple virtual storage

NARA

National Archives and Records Administration

NIC(S)

Network interface card(s)

NIPRNET

Non-secure internet protocol network

NPRC

National Personnel Records Center

OCONUS

outside continental United States

ODBC

Open database connectivity

OF

Optional Form

15 OCTOBER 2001

III CORPS & FH PAM 25-5

OPA

other procurement Army

ORA

Organization registration authority

ORAR

Originator requested alternate recipient

OTC

Operational Test Command

OWA

Outlook® Web Access

PA

Privacy act

PACS

Pentagon automated communications subsystem

PAO

Public Affairs Officer

PAS

Privacy Act Statement

PC

Personal computer

PCI

Peripheral control interface

PCMCIA

Personal computer memory card international association

Phantom CLERK

Phantom Corps Library of Electronic Recordkeeping

PIN

Personal identification number

PLA

Plain language address

PKI

Public key infrastructure

POC

Point of contact

PM

Project manager

PSN

Packet switching node

PSTN

Public switched telephone network

PTCS

Pentagon telecommunications centers system

RACS

Remote automated communications system

RCS

Report Control System

RFS

Request for service

RHA

Records holding area

RI

Routing indicator

RLM

Remote line module

RMC

Records Management Coordinator

RMO

Records management officer

ROTC

Reserve Officer Training Corps

RSAR

Recipient specified alternate recipient

RSC

remote switching center

15 OCTOBER 2001

III CORPS & FH PAM 25-5

OCONUS

Overseas continental United States

OMA

Operation maintenance Army

SBU

Sensitive but classified

SES

Senior executive service

SF

Standard Form

SIPRNET

Secure internet protocol network

SLC

Single-line concept

SOP

Standing operating procedure

SRA

Sub-registration authority

STAMIS

standard Army management information system

STARPUBS

standard Army publications system

TASO

terminal area security officer

TCC

Telecommunications center

TSACS

terminal server access

TCO

telephone control officer

TCP/IP

Transmission Control Protocol/Internet Protocol

TDC

Tactical document copier

TM

technical manual

TPN

Tactical packet network

TSR

Telecommunications service request

TTY

Teletypewriter

UFR

Unfinanced requirement

USAR

United States Army Reserve

US

United States (of America)

USC

United States Code

USERID

User identification

USMTF

United States message text format

VTC

Video teleconference facility

WAN(S)

Wide area network(s)

WINS

Windows Internet Name Service

WNRC

Washington National Records Center

WWW

World wide web

15 OCTOBER 2001

III CORPS & FH PAM 25-5

1CD

1st Cavalry Division

4ID

4th Infantry Division

13th COSCOM

13th Corps Support Command

Section II. Terms

This section not used

Index

This index is organized alphabetically by topic and by subtopic within a topic. Topics and subtopics are identified by the paragraph number.

1-800 service. See Toll Free Services

800 Service. See Toll Free Services

Army Applications System, 9

Army Standard Information Management System, 9

ASIMS. See Telecommunications Center

ATMs (Asynchronous Transfer Mode), 8

AUTODIN. See Telecommunications Center

Automation

Architecture, 5

Plan, 5

Overview, 7

Beepers. See pagers.

Bits and Bytes, 85

Back issues, 85

Distribution, 85

Cables, 5

Cabling, 8

Calling Cards, 15

Caltrop Bulletin, 52

Car phone. See Cellular Telephone Service.

Cellular Telephone Service, 13

Distribution plan, 13

Command Administrative Publications, 51

Commercial radios, 16

Computer

Maintenance, 10

Software, 10

Computer center, 9

Consultant support, 6

Copiers, 50

Office Copiers, 50

Relocation, 51

Maintenance, 51

Data Networks, 9

Data Processing Center, 9

Dedicated Circuits, 5, 14

Defense Data Network, 9

Connectivity, 9

Defense Information Switching Network, 9

Desktop Interface to AUTODIN Host, 7, 17

Directorate of Information Management, 1

Distribution. See Distribution Center

Handbook of, 1

Center, 18

DOD Mega-Centers, 9

DOIM. See Directorate of Information Management.

DPC. See Data Processing Center

Duties. See Responsibilities

File Sharing, 7

Forms Management, 39

Forms Manager, 39

Design, 40

Forms Management Officers and Coordinators, 39

Training, 40

Freedom of Information Act (FOIA) Program, 37

Fees, 38

Requests, 38

Frequency Management. See Commercial Radios

hardware, 7

health, morale and welfare (MHW) calls, 3

hubs, 8

IEEE, 6

IMA Devices, 5

IMO, 1

Liabilities, 2

Limitations, 2

IMSC. See Information Management Support Council

Index, 20

Information Management Support Council, 1

Meetings, 1

Information System Security Officer, 9

Infrastructure

network, 8

INMARSAT. See International Maritime Satellite Service

Installation Local Area Network. See Appendix I

Installation Support Modules. 5, 9

Institute of Electrical and Electronic Engineers. 6

Integrated Service Digital Network. 5, 6

Inter-LATA. 14

International Maritime Satellite Service. 14

Internet. 9

Access. 10

Internet Protocol

Address. 8

Intra-LATA. 14

IP. See Internet Protocol

ISDN. 6, 7

LATA. 14

Leased Communications. 14

Lead times. 83

Local Leased Communications Services. 15

Long –haul circuits.14

Mail. See Official Mail

Management Information Control Officer (MICO), 44

Military Construction Army (MCA) projects. 5

Mission. 1

Commander, 1114th Signal Battalion. 1

Directorate of Information Management, 1

Mobile Phone Service. See Cellular Telephone Service. 7

Newsletter. See Bits and Bytes.

NIPRNET, 9

Office Copiers, 50

Office Symbols, 47

Official Mail, 18

Distribution, 36

Federal Express, 37

Certified Mail, 37

Registered Mail, 37

Mail Scheme, 36

Official Use

Electronic Mail. 4

Employee's own time, 3

General. 2

Government property.3

Interpretations. 3

References. 3

Subordinates' time. 3, 7

Packet Switching. 8

Pagers. 16

Passwords. 9

Pay Telephone Service. 15, 7. Appendix J

Peacetime to Wartime. 6, 7

Personal Computer. 7

Phantom CLERK, 40, 52, 54

Point-to-Point Lines. 14

Portable Phone. See Cellular Telephone Service

Printing, 48

Procedures, 49

Satellite Facilities, 49

Projects

Automation. 5

Management. 5

Telecommunication. 5

Proponent. 1

Privacy Act Program, 47

Publications Management, 53

Establishing Accounts, 53

Training, 54

Publications Stockroom, 52

Purpose

Handbook. 9

Radios. See Commercial Radios

Records Management, 36

Report Control System, 46

Training, 38

References. Appendix A

Relocation. 5

Renovation. 5

Reports Control System (RCS), 46

Responsibilities

IMO. 1

Information Processing Division. 1

Information Support Division. 1

Routers. 8

Satellite Phone. See International Maritime Satellite Service

Security

ADP. 9

Servers. 7

Shared Directories. 84

Shared Files. 84

Ship-to-shore phone. See International Maritime Satellite Service. 7

Software

and CAPR. 38

and registration and warranty cards. 48

as an IMA asset. 3

Base-line survey. 2

Basic Instructions. 81

CSS. 30

development. 2

DINAH-MITE. 17

evaluation. 1

Software (continued)

- evaluations. 1
- IMO Support Duties. 1
- inappropriate use. 3
- installation assistance. 6
- must use original. 48
- ODBC. 67
- removal for turn-in. 51
- repair matrix. 47
- troubleshooting. 45
- turn-in. 2
- updates. 55
 - excess. 51
- exempted from CAPR. 73
- Overview. 7
- Upgrade Instructions. 81

STAMIS. 5**Standard Army Management Information Systems (STAMIS). 9****Stovepipe. 5****Subnet mask. 8****TCC. See Telecommunications Center****TCO. See Telephone Control Officer.****TCP/IP**

- and X.25 protocol. 6
- Setting Adapters and Protocols in Windows™. 48
- Upgrading Instructions. 81

Telecommunications Center. 16**Telephone Calling Cards. 15****Telephone Control Officer**

- Duties. 2
- Responsibilities. 2

Telephone Service

- Pay Telephone Service. 15

Telephone Work Orders. 5**Telephones. See Cellular Telephone Service. See INMARSAT.****Terminal Server Access Control System. 10. See TSACS****Termination Boxes. 5****Toll Free Service. 14****TSACS. 10**

- Example Request. 63

User Identification. 7, 9

This page intentionally left blank

find this title at <http://pclerk.hood.army.mil>