Field Manual
No 24-17

FM 24-17
Headquarters
Department of the Army
Washington, DC, 17 September 1991

Tactical Record Traffic System (TRTS)

Contents

Unless otherwise stated, whenever the masculine gender is used, both men and women are included.

DISTRIBUTION RESTRICTION: Approved for public release; distribution is unlimited.

***This publication supersedes FM 24-17, 31 August 1987.**

Preface

Purpose and Scope

This publication provides guidance and doctrine for the Tactical Record Traffic System (TRTS). It provides signal and nonsignal personnel an overview of the TRTS. It gives the reader necessary procedures to standardize operations when processing, transmitting, and delivering tactical record traffic in hard copy and soft copy format. (Hard copy is printed copy; soft copy is data stored on magnetic disks.)

This publication covers tactics, techniques, and procedures for operating various TRTS subscriber terminals. It also provides information on the evolution of the record traffic communications system towards a totally integrated, automated, and synchronized communications system.

User Information

The proponent of this publication is HQ TRADOC. Send comments and recommendations on DA Form 2028 directly to Commander, United States Army Signal Center and Fort Gordon, ATTN: ATZH-DTL, Fort Gordon, Georgia 30905-5075. Key comments and recommendations to pages and lines of text to which they apply. If DA Form 2028 is not available, a letter is acceptable. Provide reasons for your comments to ensure a complete understanding and proper evaluation.

Chapter 1

Tactical Record Traffic System (TRTS) Fundamentals

1-1. Introduction

Record traffic is the term for messages that are permanently or semipermanently being maintained by the message originator or addressee. Record traffic is used primarily by staff organizations to conduct unit business and may exist in page form or reside on floppy disks or within computer memory. With the advent of the TRTS, users of the TRTS can process record traffic communications within an automated, decentralized, highly mobile and extended communications environment far removed from the older over-the-counter record communications services provided by the Signal Corps. In this TRTS architecture, record traffic subscriber terminals are user-owned, user-deployed, and user-operated.

The TRTS, the Army Tactical Command and Control System (ATCCS), and the Defense Data Network (DDN) are new systems systematically replacing the tactical telecommunications centers (TCC) and the over-the-counter record communications services. These new systems provide rapid flow of command and control (C^2) communications across all Army echelons of AirLand Operations. These new systems, combined with desktop and laptop personal computers (PCs), lightweight digital facsimile (LDF) machines, and digital telephones provide tactical commanders and their staff the capability to transmit and receive administrative, logistical, intelligence, and operational C^2 communications. This allows them to meet their operational and tactical mission requirements.

The TRTS is either formal or informal. Chapter 9 discusses how the two communications systems are interchangeable if procedures for message transfer are followed.

The formal TRTS uses communications terminals (CTS) as terminal devices for the transmission of properly formatted Joint Army-Navy-Air Force Publication (JANAP) 128, Allied Communication Publication (ACP) 127 GENSER, Defense Operating Instructions (DOI) 103 DSSCS messages, and US joint message text format.

The informal TRTS may use any approved subscriber terminal device available to send and receive nonformatted text, pictures, maps, and so forth. Devices include facsimile machines, PCs, and other user-owned equipment.

Transfer of record communications with tactical or garrison units is effected through user-owned and -operated terminal equipment connected to the area common-user system (ACUS) circuit and message switches.

Tactical organizations having a requirement to process record traffic between communications facilities connected by the Defense Communications System / automatic digital network (DCS / AUTODIN) message switches will receive the AN / UGC-144 CT. This user-friendly, menu-driven equipment allows the organization to prepare, transmit, and receive formal record traffic communications. Formal record traffic communications are those which comply with established procedural requirements to be processed within AUTODIN. To aid the general-purpose (GP) user, the CT has preformatted message headers and endings. Preinstalled message routing protocols allow record traffic to be properly routed to the intended addressees without delay. Two separately configured CTs provide service for either the general service (GENSER) or the Defense Special Security Communications System (DSSCS). Unit mission requirements dictate the communications environment in which the CT operates. User-owned CTs connect into the ACUS network of message switches. This provides access into the AUTODIN network of continental United States (CONUS) or overseas computerized message switching equipment.

Tactical organizations with a requirement to process message traffic which will not enter the AUTODIN message switching network will have access to the ACUS dial-up circuit switched network. This circuit switched network provides a fast, reliable, and secure means of transmitting and receiving informal tactical record traffic. Informal record traffic does not have specified procedural formats or requirements and may exist in many types of media. Connection into the informal TRTS will be extended from echelons above corps (EAC) down to battalion level.

Organizations will have access to the formal record traffic system and also to the informal record traffic system based on assigned mission and available equipment. Some units will operate in both garrison and tactical situations, while other units may use their equipment only during tactical deployments.

Communications terminals, facsimile equipment, and digital telephones may be located in tactical vans, bunkers, tents, aircraft, or buildings. This can include any associated controlled cryptographic items such as communications security (COMSEC) equipment. The equipment can easily be moved from one location or operating environment to another depending on mission requirements. Personnel operating TRTS equipment will be unit personnel normally assigned to current operations cells in tactical operations centers (TOCs), or personnel assigned to administrative, logistical, or intelligence duties where TRTS equipment is located. proper message preparation, transmission, receipt, records management, and distribution procedures must be known and adhered to regardless of where the TRTS equipment is deployed. Multilevel access and password controls make it possible to restrict access to TRTS equipment, but it is possible for almost all organizational personnel to be involved with processing formal and informal tactical record communications.

TRTS record communications pass over one or more transparent, processor-driven automatic switches. These switches include, but are not limited to the following:

- Strategic defense switched network (DSN) switches. (This system was previously known as the automatic voice network [AUTOVON].)

- Strategic AUTODIN message switches. (This system is being changed to the Defense Message System [DMS].)

- DDN system of packet switches. (Only the E-mail processing/transfer portion of DDN is part of DMS.)

- Mobile subscriber equipment (MSE) family of tactical circuit switches.

- AN/TTC-390 joint tactical communications (TRI-TAC) family of tactical circuit switches.

- AN/TYC-390 (TRI-TAC) family of tactical message switches.

Circuit and message switches form the hub of today's worldwide tactical and strategic record traffic communications networks. This network is linked globally by strategic and tactical transmission and switching systems which allow operability throughout the DCS and the ACUS. Figure 1-1 shows the CT formal TRTS architecture as it extends from division up to EAC and on to CONUS/sustaining bases throughout the world. Because the Army fights under joint, unified, or combined command authority, the TRTS extends to major forces collocated at EAC. Army forces (ARFOR), Air Force forces (AFFOR), and Marine forces (MARFOR) interconnect to the joint message switch network using either interswitch trunks or standard MODE I circuits, depending on whether or not the component has a message switch. Figure 1-2 shows how the joint forces generally are connected and have access to the TRTS.

1-2. Battlefield Automated Systems (BAS) Integration into TRTS

The modern battlefield is systematically and rapidly moving towards total automation with the application of battlefield automated systems that can and do interoperate with each other in real time. This greatly extends and enhances the commander's ability to collect, process, and distribute information to fight and win the battles of AirLand Operations.

Functional integration of BAS is becoming a reality at all echelons. The fielding of user-owned and -operated CTs that pass record traffic communications over existing communications links is an initial move toward BAS integration.

Battlefield automated systems provide interoperability across the battlefield. This continues to evolve and transition with the fielding of new equipment and systems. Tactical and strategic subscribers can communicate with each other in real time. The two record communications systems--fixed and tactical--will eventually be one worldwide record traffic system, connected by BAS, that will use common hardware and software. Record traffic communications will be passed over local and wide area networks (LAN/WAN) or through gateways to other networks. Doctrine, tactics, and techniques will be published and fielded to the user as battlefield automated systems become a total reality.

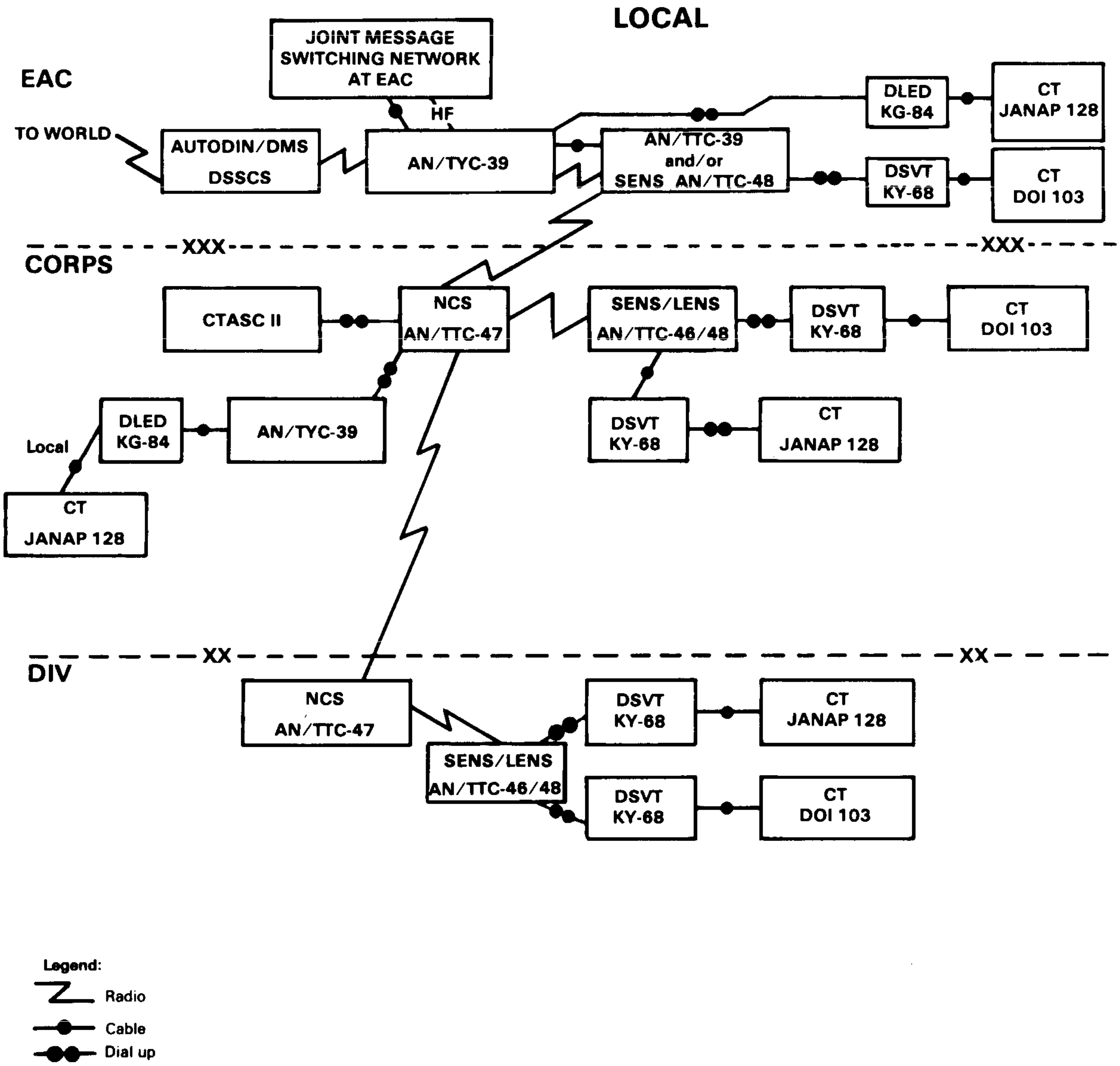


Figure 1-1. Formal TRTS architecture.

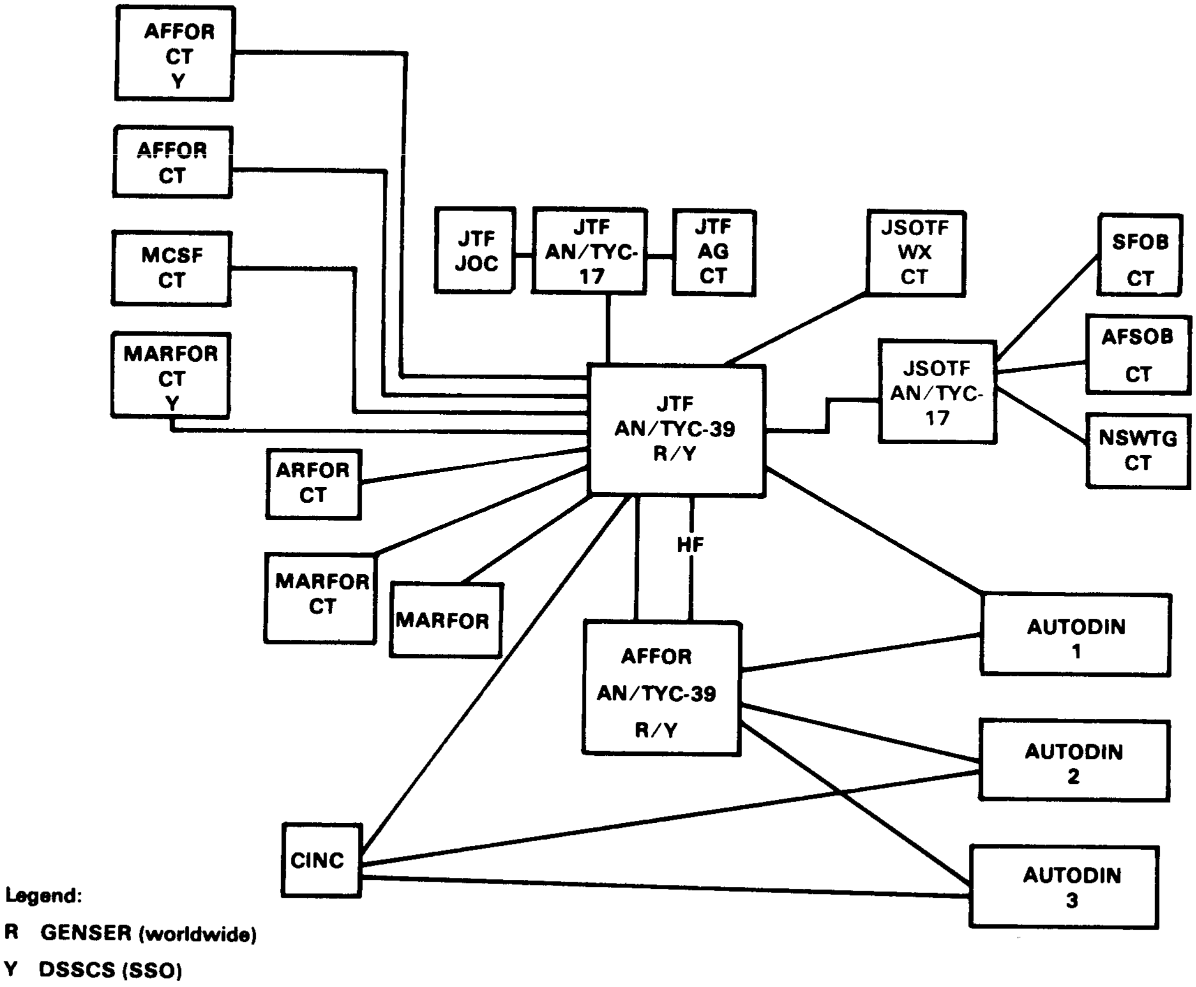


Figure 1-2. Joint message switching network at EAC.

1-3. Procedures

Procedures in this manual apply to all user-owned and -operated subscriber terminals used to pass formal or informal record message traffic by the TRTS. TCCs will adhere to established procedures in effect at tactical TCCs and as prescribed in this manual.

Procedures contained in this manual augment the procedures contained in--

- JANAPs.
- ACPs and supplements.
- DOIs.
- Critical intelligence communications (CRITICOM) operating instructions.

This manual identifies the following forms required (and recommended) to maintain an audit trail within TRTS.

- DA Form 5651-1.
- DA Form 4016.
- DA Form 4011.
- DA Form 5651.
- DA Form 1999-R.
- CT Initialization Table Entry Work Sheet. (See Appendix F.)
- CT PLA/RI Table Entry Work Sheet. (See Appendix F.)

When a CT is configured to process GENSER record communications, JANAP 128 procedures apply. At DSSCS-configured CTs, the procedures contained in DOIs are mandatory. Current ACPs and JANAPs will be procured along with Defense Information Systems Agency (DISA) and Defense Intelligence Agency (DIA) publications. Those publications may reside at the CT or be partially located at the signal office or Information Service Support Office.

1-4. Responsibilities

The TRTS operator and individuals directly responsible for the operation of TRTS equipment must be aware that TRTS literally links a soldier in the field with the national command authority (NCA).

The user is responsible for--

- Installing, operating, and completing user-level maintenance of TRTS equipment. This is accomplished in both tactical and garrison environments while in support of the unit mission.

- Maintaining liaison with the organization signal officer to ensure TRTS needs are identified and met.

- Establishing a standing operating procedure (SOP) which allows for accuracy, speed, security, reliability, and message privacy of record traffic communications. The unit SOP will augment procedures found in this manual. (See paragraph 1-3.)

- Coordinating with the supporting signal officer to ensure unit information is programmed at the unit's connected AN/TYC-39( ) message switch.

- Coordinating with the unit signal officer for employing nonstandard terminal devices on circuit and message switching equipment provided by the Signal Corps.

The organization signal officer is responsible for--

- Coordinating with user organizations to ensure the user is provided a telephone/plain language address and routing indicator (PLA/RI) directory.

- Coordinating user participation in communications training development and management of automated systems to ensure user confidence and competence in equipment and procedures.

- Providing staff management of information management areas.

- Ensuring all supported units comply with the security and operational requirements of TRTS, to include properly initializing CTs each time the terminal is deployed.

The signal unit providing AN/TYC-39( ) support is responsible for maintaining and updating PLA and RI databases.

Chapter 2

Formal TRTS Operational Concept

2-1. Introduction

This chapter describes features of the CT and associated interface equipment and systems. It also discusses operational security measures of the CT.

Formal TRTS capability will extend to independently deployed separate brigades and armored cavalry regiments through EAC. Although access is based upon AUTODIN and DSSCS user requirements, all users may communicate with other tactical users as well as strategic users since they compose a worldwide network.

Formal TRTS includes tactical and strategic/ sustaining base TCCs that process standardized formatted record communications message traffic.

2-2. Formal TRTS Equipment

The CT is a user-owned and -operated message terminal. Through menu-driven input screens and passwords, it allows composition, transmission, and receipt of formal record traffic. The CT possesses 3 megabytes internal random access memory (RAM) and 40 megabytes of hard disk storage. Each CT has a digital subscriber voice terminal (DSVT) KY-68 which provides autodial encryption capability. The CT is man-portable and can serve as a stand-alone PC. Figure 2-1 summarizes the AN/UGC-144's major operating features. See TM 11-7025-267-12 for further information on CT operations.

The CT uses an ink jet printer with a disposable printhead, a supply of fan-fold paper, and a 6-foot terminal cable.

Prompts

- Header
- Message Body

Autodial

Alarm Indicators

Emergency Erase/Purge

Service Messages

PLA/RI Security Tables

Multilevel Password Control

Self Test

Memory Load

Figure 2-1. AN/UGC-144 major operating features.

The single subscriber interface (SSI) interacts with a DSVT, a digital non secure voice terminal (DNVT) TA-1035, a dedicated loop encryption device (DLED) KG-84, or an advanced narrowband digital voice terminal (ANDVT). Three different cable assemblies are used to connect equipment to the SSI. The SSI is an internal component of the CT and has its own menu functions.

The DSVT is used for encrypting/decrypting voice traffic and provides secure digitized data capability. It operates as a full-duplex or half-duplex subscriber terminal. The DSVT provides a digital communications interface with TRI-TAC and MSE circuit switches.

2-3. Formal TRTS Switching Systems

The following overview of the automatic message switching systems, from division through corps and EAC, explains how TRTS functions with each system. Detailed information on each system is contained in the associated field manuals and technical manuals.

EAC switching systems. TRTS users should be aware that each automatic message switch central AN/TYC-39( ) is normally connected to at least two other message switches through the dual-home feature.

Message switch AN/TYC-39( ). This switch provides secure, automatic message switching of narrative record and data traffic at major corps and theater Army nodes. The AN/TYC-39( ) will automatically accept, process, store, deliver, and account for record traffic through 50 lines of narrative header and textual information.

Parent AN/TYC-39( ). A parent AN/TYC-39( ) is located at the user's parent corps (or theater). The CT user transmits messages directly by the dial-up ACUS. The parent AN/TYC-39( ) automatically routes message traffic to the intended addressees.

Alternate AN/TYC-39( ). Should the parent AN/TYC-39( ) be destroyed or become inoperable, the CT user will transmit multiple addressee traffic to an alternate AN/TYC-39( ) across corps or EAC boundaries within the ACUS network. The alternate AN/TYC-39( ) will perform message routing.

Gateway AN/TYC-39( ). A gateway AN/TYC-39( ) is normally located at EAC. The gateway AN/TYC-39( ) will provide the entry into the AUTODIN or DSSCS networks. Although any CT's parent AN/TYC-39( ) can perform as a gateway, not every switch will perform this function.

AN/TTC-39( ) and small extension node (SENS) AN/TTC-48 circuit switches. These switches provide switching and MSE network access/interface with the Secure Voice System (SVS), existing tactical switches (manual and automatic), and commercial central offices.

Corps/division switching systems. Node center AN/TTC-47 combines digital switching capability with flood search routing and subscriber management into one switching function. The SENS can interface with a node control switch (NCS) AN/TTC-47 at echelons corps and below (ECB) via CX-11230/C cable, line of sight, or tactical satellite. Additional TRTS switching to North Atlantic Treaty Organization (NATO) telephone systems and net radio interface (NRI) can be accomplished where TRTS subscribers coordinate with the supporting signal officer for these services. Along with an extension node, the AN/TTC-47 provides TRTS voice, data, and facsimile communications to corps, division, and brigade level command posts. NRI capability may be installed depending on mission and user requirements. In non-MSE divisions, the AN/TTC-41 automatic telephone central office provides automatic switching for TRTS users.

Record traffic passes over many transmission paths and through one or more circuit or message switches. The user will not normally be aware of the circuit paths as these equipments are transparent to the user. In an MSE network, tactical users may send record traffic to one or more units within a 37,500 square kilometer area. (See FM 11-30 for additional information on how record traffic passes over line of sight or cable through one or more of 42 major node centers.) Connectivity is based on close coordination with the supporting signal officer and each user making their requirements known and validated.

2-4. CT Security

AR 380-5 provides guidance pertaining to protecting and safeguarding classified material stored in the CT's memory or on the auxiliary storage cassette (ASC) or 3.5 inch floppy disks of CTs so equipped. The CT is unclassified upon receipt at the unit. (See Appendix I for factory default settings.) When classified information is stored in the CT or on an ASC or floppy disk, the equipment and disk must be protected and safeguarded as required by AR 380-5 and AR 380-19 in accordance with (IAW) the highest level of information.

As a minimum, the unit SOP should include specific guidance for safeguarding the CT and to protect the equipment before, during, and after tactical deployment. When documenting procedures for protecting the CT and associated record traffic/residue, follow procedures in AR 190-13, AR 380-5, and AR 380-19.

When operating the CT, ensure that unauthorized personnel do not gain access to the terminal, hard disk, ASCs, floppy disks, or passwords needed to access the system. The entire CT must be safeguarded IAW AR 380-5 and AR 380-19 to prevent disclosure of passwords and classified information or material to unauthorized personnel.

(See TM 11-7025-267-12 for instructions on denying unauthorized screen viewing and how to recover from a manually blacked-out terminal screen.)

Whenever the CT is unattended or not in operation, take the following precautions to prevent inadvertent disclosure of classified information to unauthorized personnel.

- All spare ASCs and floppy disks will be formatted and marked as Formatted YY MM DD (year, month, day). This is accomplished by using the FORMAT function in the CT directory. (See Appendix J for additional security and protection of ASCs and data disks.)

- All information placed on the hard disk must be saved on ASCs or floppy disks before storage. The ASCs and floppy disks must be safeguarded IAW AR 380-5 or protected under the Privacy Act of 1974. All ASCs and floppy disks containing information must be marked with the highest security classification of the information contained on them.

- Local SOP should provide disposition instructions for all message traffic, paper, and other CT generated waste. Classified waste material, such as handwritten message drafts, notes, and carbon paper will be destroyed as classified trash. Destroy classified material IAW security provisions of AR 380-5. CT users should coordinate with the unit intelligence officer and security officers for compliance with authorized destruction procedures.

The CT employs security measures within its operational software to ensure classified traffic is not transmitted to unauthorized users. The AN/TYC-39( ) will not route messages to improperly classified CTs and a CT will not allow receipt of traffic which exceeds its terminal classification.

ACUS COMSEC measures secure all TRTS traffic up to a level of SECRET. Standard COMSEC measures include radio link encryption and Protected Wire Distribution Systems (PWDS).

The following requirements provide TRTS users access to DSSCS and the capability to transmit TOP SECRET/sensitive compartmented information (TS/SCI) message traffic when authorized by the National Security Agency (NSA). (See Chapter 7 for additional guidance on actual record traffic processing procedures.)

- Compartmented key on an end-to-end basis using KY-68s (that is, S variable). (Contact the signal officer or unit COMSEC custodian for additional information on secure voice S variables.)

- Dedicated COMSEC equipment and superencryption procedures as authorized by the unit.

- A direct trunk to EAC AN/TYC-39( ) with SCI KG-84 subscribers for EAC users.

Chapter 3

Formal TRTS Message Fundamentals

3-1. Introduction

This chapter provides information on the preparation of formal messages in the TRTS.

AR 25-11 prescribes the policies, responsibilities, and procedures governing the record communications preparation, approval, and process within the Department of the Army (DA). CT users must be aware of and comply with those procedures contained in AR 25-11 and this chapter to correctly process record traffic within the formal TRTS.

Supervisors of CTs should incorporate message flow procedures from Chapter 9 and message preparation requirements from AR 25-11 into their local SOPS. This will ensure all formal TRTS record communications prepared at their CT are properly prepared and processed in an accurate and timely manner. Deviations from established procedures may result in deficiencies that adversely impact on the record traffic system (delayed, misrouted, or lost messages). Supervisors must establish, supervise, and maintain an effective quality control program that will ensure CT users are in compliance with prescribed operating procedures and practices.

Messages within TRTS will be handled with the utmost privacy. The message contents cannot be provided to anyone except by the originator or addressee.

When a message is originated from the CT, it must be entered into the CT's memory. Messages to be transmitted will be provided to the CT operators IAW the unit SOP .

> Note: For the operator to prepare and transmit a message, two different passwords must be known and used. To enter the appropriate level of classification and to enable the transmit function in the ACCESS menu, the operator must have access to two passwords.

Outgoing messages can be manually entered through the CT keyboard or, if the CT is equipped with a disk drive, the text can be delivered on a disk, inserted into the disk drive, and loaded onto the CT screen for processing. The following information must be available or known by the CT operator before composing formal record traffic into the proper format for transmission into the TRTS.

Security classification. The message writer is responsible for determining the proper security classification for each message IAW AR 380-5. A CT operator should never accept a message for transmission unless the security classification is known. The security classification must be indicated for manual message processing. Written messages will have the security classification stamped or marked at the top and bottom of the paper copy. If the message is prepared on floppy disk, the disk will be properly labeled with the security classification clearly marked. This will prevent transmission of an improperly classified message.

Releaser date-time group (DTG). This reflects the time the message was processed by the releaser and will be expressed in date/time (ZULU)/month/year. No two messages from the same office/unit should have the same DTG. (See Appendix B for construction of ZULU time and how to convert local time to ZULU.) CT users may use the internal clock time as a DTG or the user unit may assign their own.

Precedence. The precedence for the action addressee is a mandatory entry. The precedence will be used to indicate the order in which a message will be processed and the speed at which the message must be handled by the CT user and noted by the addressee. The lowest precedence should be used whenever possible. (See Appendix C for examples of precedence assignment.)

Flash (Z), CRITIC (W), and ECP (Y) messages will be handled/processed as fast as possible with an objective of 10 minutes for Flash and 3 minutes for CRITIC and ECP messages.

Immediate (0) messages should be processed within 30 minutes.

Priority (P) messages have a time objective of 3 hours.

Routine (R) messages have a time objective of 6 hours.

FROM PLA. This is normally the unit command title, location, and one office symbol which is enclosed within double slants; for example, CDR 1ST ID WASH DC//DCG//.

TO PLA. In most cases, this is the commander of the command, installation, or agency for whom the message is intended. DA Pam 25-11 contains message address designators and is used to construct the PLA/RI tables.

Office symbols will be included as part of the address designator.

Information such as ATTN MAJ SMITH or FOR COL JONES will not be used in place of office symbols. When names are required, they will be included in the internal/ handling instructions of the message text.

INFO PLA (if required).

Releaser. The releaser is designated by the unit to release messages for transmission in the TRTS. No message will be entered into TRTS without being properly released/ signed by an authorized individual. The unit SOP should state that no member will knowingly transmit or cause to be transmitted, or deliver or cause to be delivered, a false or forged message.

3-2. Preparing Outgoing Messages

Most of the information needed to compose a message was entered when the initialization table entries were made. To compose a message, the operator/CT user takes the following steps:

From the main menu, select EDIT by using the F7 key.

From the EDIT menu, select NEW MESSAGE by using the F2 key.

When the next screen appears, start typing the message text. The message text starts with the line directly after the SUBJECT line. When you reach the bottom, the screen will automatically scroll.

When the message text has been completed, select the header function using the F1 key.

If the CT is set up as a GENSER terminal. the four options for the message header are JANAP 128P, JANAP 128AP, ACP 127-1, and ACP 127-3. If the terminal is set up for DOI 103 format, the selections will be DOI 103S or DOI 103C.

After selecting the correct message format, enter information from the message form. The following prompts will appear on the CT screen. Select the appropriate entry.

- ENTER CLASSIFICATION. Enter a character U, E, C, S, or T. This entry is taken from the CLASS block of the message form. The letter must match the overall message security classification.

- ENTER THE NEXT CHANNEL SEQUENCE NUMBER (CSN). This entry only appears, and is required, if the message is ACP 127 format or MODE II of JANAP 128 and DOI 103.

- ENTER TRANSMISSION RELEASE CODE (TRC). Enter N. This will be a standard entry for this menu location.

- ENTER PRECEDENCE. Enter a character R, P, O, Z, or Y. This entry is taken from the PRECEDENCE (ACT) block of the message form.

- ENTER INFO PRECEDENCE . Enter precedence code shown on the PRECEDENCE (INFO) block of the message form. If the message is intended for a single addressee, repeat the letter previously used in PRECEDENCE.

- ENTER STATION SERIAL NUMBER (SSN). This entry is automatically placed by the CT. Press RETURN.

- ENTER SPECIAL CATEGORY (SPECAT). Enter A for TOP SECRET, B for SECRET, or N if the message is not SPECAT. This entry is taken from the SPECAT block of the message form. AR 105-31 contains additional information on SPECAT messages.

- ENTER DATE . The CT will show the current date. The DTG/RELEASER TIME (DATE-TIME, MONTH, and YR blocks from the message form) can be manually entered.

- ENTER TIME. Same as information in paragraph above.

- ENTER THE SUBJECT LINE. This entry cannot be more than one line. If the subject is more than one line, the operator must, after finishing the message, go in and EDIT the message text by adding the remaining subject lines.

- ENTER Y TO ADD PLAs/RIs. This is where the PLA/RI table is used to speed message processing. If you select Y, the CT will enter the PLA/RI table and will allow you to select the PLA and RI for the addressees. If the PLA/RI are not in the tables, then press any key and the CT will prompt you to enter the PLA and RI. After the first PLA/RI, the CT will ask if that is all. If there is an INFO addressee, continue to add PLAs/RIs. Use the PLA/RI shown on the TO line and (if required/used) the INFO lines on the message form.

After the message text has been typed, the message should be saved to an ASC or a floppy disk. This prevents having to retype the entire message should a power failure occur which would erase the message from the CT screen.

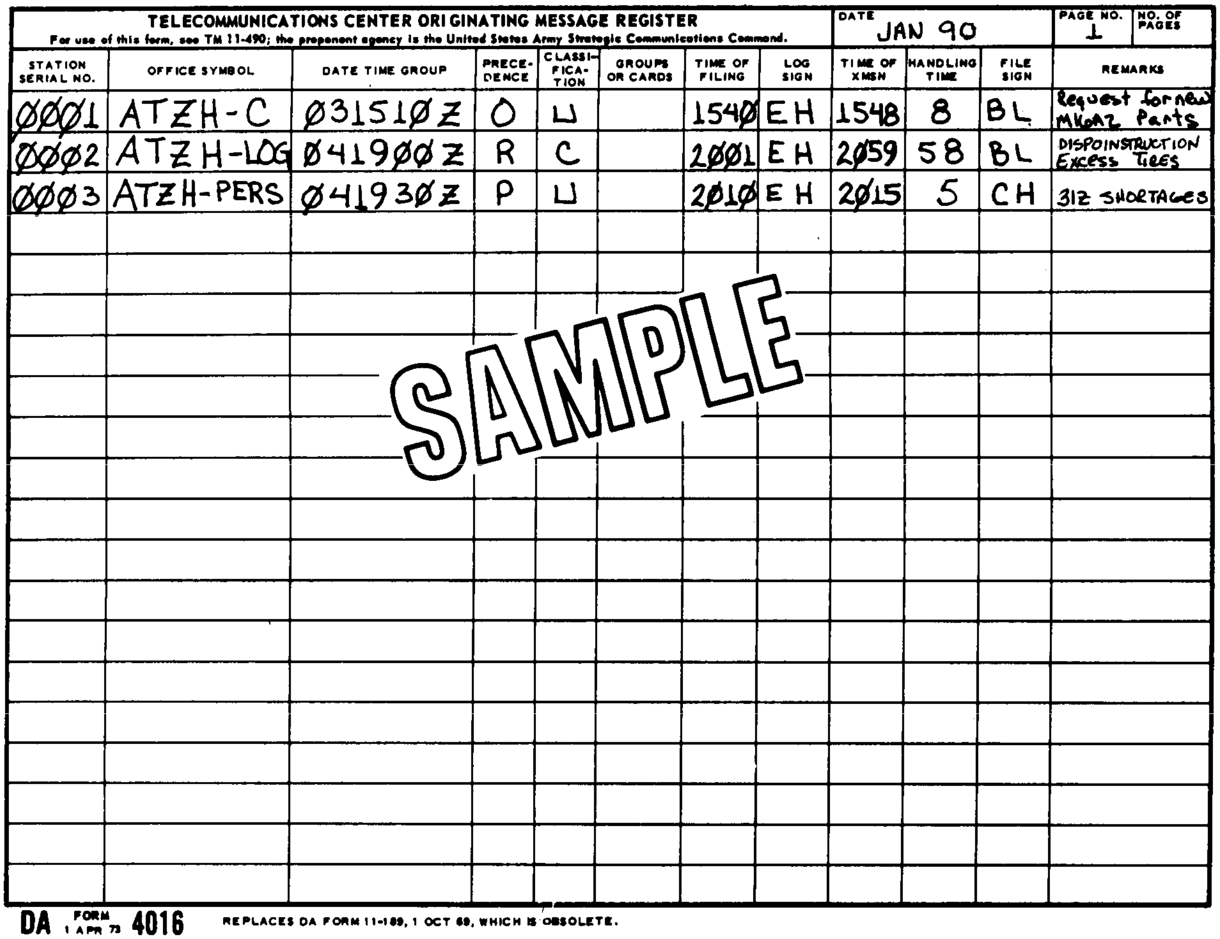
It is highly recommended that someone other than the operator who typed the message proofread the message text and initial that they have done so.

3-3. Originated Message Register

Use DA Form 4016 to aid the CT operator in providing an audit trail and historical information for outgoing record traffic. (See Figure 3-1.)

CT supervisors can use information from the DA Form 4016 to identify record traffic speed-of-service trends or as an aid to insecurity investigations should the need ever arise. DA Forms 4016 should be filed with individual monthly record traffic hard copies or diskettes.

Automated procedures, such as saving a message to CT memory and printing a directory listing, may meet some units' needs for maintaining an originated message register.



TELECOMMUNICATIONS CENTER ORIGINATING MESSAGE REGISTER
For use of this form, see TM 11-490; the proponent agency is the United States Army Strategic Communications Command.

DATE JAN 90 | PAGE NO. 1 | NO. OF PAGES

STATION SERIAL NO.	OFFICE SYMBOL	DATE TIME GROUP	PRECEDENCE	CLASSIFICATION	GROUPS OR CARDS	TIME OF FILING	LOG SIGN	TIME OF XMSN	HANDLING TIME	FILE SIGN	REMARKS
ØØØ1	ATZH-C	Ø3151ØZ	O	U		154Ø	EH	1548	8	BL	Request for new MKOAZ Parts
ØØØ2	ATZH-LOG	Ø419ØØZ	R	C		2ØØ1	EH	2Ø59	58	BL	DISPOINSTRUCTION Excess Tires
ØØØ3	ATZH-PERS	Ø4193ØZ	P	U		2Ø1Ø	EH	2Ø15	5	CH	312 SHORTAGES

SAMPLE

DA FORM 1 APR 73 4016 REPLACES DA FORM 11-189, 1 OCT 69, WHICH IS OBSOLETE.

Figure 3-1. Sample of DA Form 4016.

3-4. Outgoing Message Flow

Originated messages must follow a logical and established path/flow from the message originator/drafter throughout required staffing to the CT operator. The CT operator either types the message text or loads an ASC or a floppy disk containing the message into the CT memory.

Formal record traffic administrative procedures must be standardized at the user's CT to prevent message delays or losses.

Chapter 4

Transmitting Formal Messages Within TRTS

4-1. Introduction

This chapter covers how messages are transmitted by the CT and message switches within the TRTS.

Message traffic can be received and transmitted at the same time, except when the CT is connected to an ANDVT which operates in half-duplex (send or receive mode). TM 11-7025-267-12 contains the required machine functions to follow when transmitting a formal CT message within TRTS. Formal TRTS can be passed over a variety of user-owned and Signal Corps-owned equipment depending on the echelon at which the CT is located.

The CT must be enabled for transmission in the ACCESS menu. In order to transmit a message, you must have the correct passwords.

In the formal TRTS, the preferred method of message transmission between users is terminal to terminal or direct dial up using only the circuit switched network. Whenever possible, the CT operator uses the direct dial up of destination terminals. This method will greatly lessen the processing burden of the AN/TYC-39( ) message switch. The user must coordinate with the supporting signal officer to ensure the CT has been included in the parent AN/TYC-39( ) database. The following types of messages can be sent to an AN/TYC-39( ) message switch, by dial up through the circuit switched network, for delivery to required addressees.

- Multiple address messages with two or more addressees.

- Messages intended for delivery through the AUTODIN network.

- Messages that cannot be sent by terminal to terminal direct dial up after one or more attempts to transmit the message have been made.

- Messages to TRTS terminals that do not have assigned telephone numbers. Addressees in this type of message must be identified by an RI.

A CT with dial-up access to the tactical communications network is connected to the data port of the DSVT or DNVT. A station with direct access to an AN/TYC-39( ) message switch is connected through a DLED.

4-2. Transferring Formal TRTS Messages

CT to CT. Once the terminal is properly accessed and the message is formatted correctly, the CT user can transmit record traffic directly to the single addressee CT by the dial-up ACUS.

CT to multiple addressees. When sending multiple addressee record traffic, the CT user will transmit properly formatted messages directly to the user's parent corps or theater AN/TYC-39( ). See paragraph 4-3 for autodial procedures for multiple addressees.

CT to AUTODIN or DSSCS addressees. The properly formatted and addressed CT message will be transmitted to a designated gateway AN/TYC-39( ), normally located at EAC, for entry into the AUTODIN or DSSCS networks.

CT to LDF addressee. The CT user will prepare a properly formatted message for delivery by refile to an LDF. The messenger takes the message to the nearest LDF location for delivery by facsimile.

4-3. Autodialing

When a formal message is transmitted to more than one addressee, the CT operator has the option of using the CT's AUTODIAL option. This method allows the operator to manually select up to eight phone numbers (consisting of up to 10 numbers each). The CT automatically dials each phone number and transmits the properly formatted message to each of the intended addressees. CT users should be aware that when transmitting messages direct (user to user) via the circuit switching dial-up procedures, there will be no record of that message having been transmitted at the circuit switch. Therefore, if the message is lost or mishandled, it cannot be traced through Signal Corps facilities. The only messages which may be traced through the switching systems are those which transit the AN/TYC-39( ) message switch.

TM 11-7025-267-12 contains additional information on autodialing procedures.

4-4. Transmitting CT Messages by AN/TYC-39( ) Switches

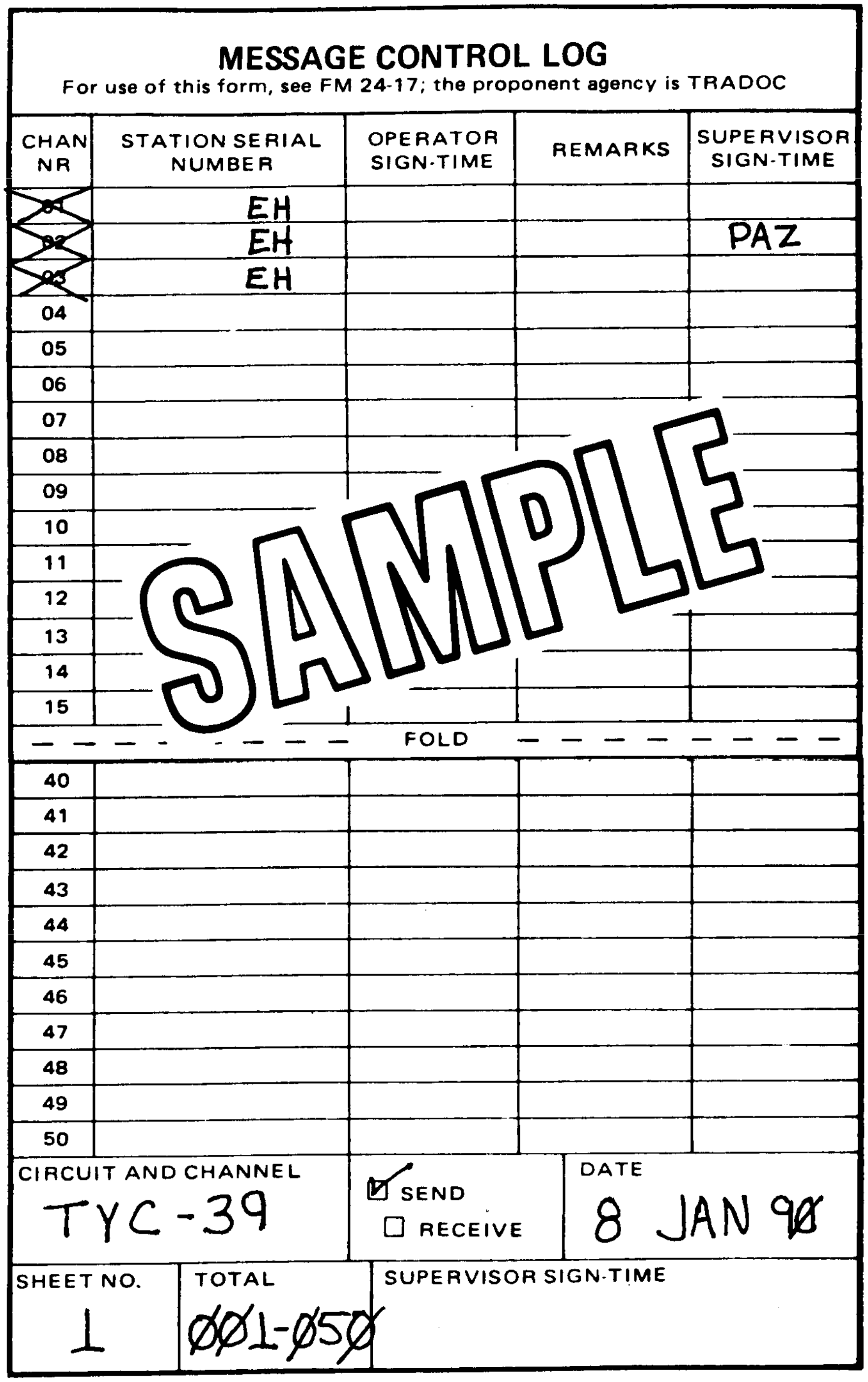
CSNs must be used when you process a message in the ACP 127-1 and ACP 127-3 formats.

CSNs must also be used if your CT is operating in MODE II. In this mode of operation, the connected message switch automatically detects a faulty CSN, header, or end of transmission situation. Since the message switch cannot stop a transmitting CT, it will send an automatic computer-generated service message to advise the CT user that the message has been rejected or accepted.

CSNs are managed by the CT operator to ensure messages are not lost or delayed at the message switch. To accomplish this, the CT operator uses DA Form 5651. To know the last CSN used and also to know what the next good CSN is, the numbers will be marked off or lined through as numbers are used for each message being transmitted through a message switch. Invalid or out-of-sequence channel numbers cause messages to be rejected at the switch and requires operator correction for retransmission. It is important to keep the CSNs correct at all times.

If the CT user has a large amount of message traffic and problems are encountered with out-of-sequence channel numbers causing message rejects, the CT supervisor of a MODE II configured CT may elect to use two separate DA Forms 5651 to keep messages separated from the switched and direct dialed networks.

Figure 4-1 shows an example of how DA Form 5651 is completed to keep track of CSNs. This example shows CSN 004 as the next valid CSN of a formal message to be transmitted through an AN/TYC-39( ).



MESSAGE CONTROL LOG

For use of this form, see FM 24-17; the proponent agency is TRADOC

CHAN NR	STATION SERIAL NUMBER	OPERATOR SIGN-TIME	REMARKS	SUPERVISOR SIGN-TIME
~~01~~	EH			
~~02~~	EH			PAZ
~~03~~	EH			
04				
05				
06				
07				
08				
09				
10				
11				
12				
13				
14				
15				
FOLD				
40				
41				
42				
43				
44				
45				
46				
47				
48				
49				
50				

SAMPLE

CIRCUIT AND CHANNEL TYC-39	☑ SEND ☐ RECEIVE	DATE 8 JAN 9Ø

SHEET NO. 1	TOTAL ØØ1-Ø5Ø	SUPERVISOR SIGN-TIME

DA FORM 5651, AUG 87

Figure 4-1. Sample of DA Form 5651.

Chapter 5

Formal TRTS Message Receipt Fundamentals

5-1. Introduction

This chapter presents procedures for processing received record traffic messages. It provides instructions relating to procedures, security, privacy, and maintenance of an audit trail.

The unit SOP provides local procedures to enhance accountability and privacy within the organization. The CT user/operator is held personally and legally responsible for the initial accountability, security, and privacy of received messages until properly delivered to the authorized and intended addressee.

The CT supervisor must coordinate with the organization signal officer to have a terminal/unit routing guide published. This aids the CT operator in determining the proper routing and delivery of incoming messages. Routing guides should include action and information addressees for specific subject areas and number of copies to be delivered.

As a minimum, the CT operator should process received formal record traffic messages as shown below.

The CT operator visually scans all received messages. This ensures the message is in fact intended for that terminal, is not garbled, is not incomplete, and is not misrouted. See Chapter 6 for processing misrouted messages.

The CT operator processes messages by precedence. Higher precedence messages are processed ahead of lower precedence messages. In most cases and depending on organizational mission, an incoming IMMEDIATE precedence message is processed and delivered before an outgoing IMMEDIATE precedence message. The local SOP indicates if received messages take precedence over outgoing messages. A received PRIORITY precedence message always takes precedence over a received ROUTINE precedence message.

Received service messages take priority over outgoing service messages and outgoing record traffic of the same or lower precedence.

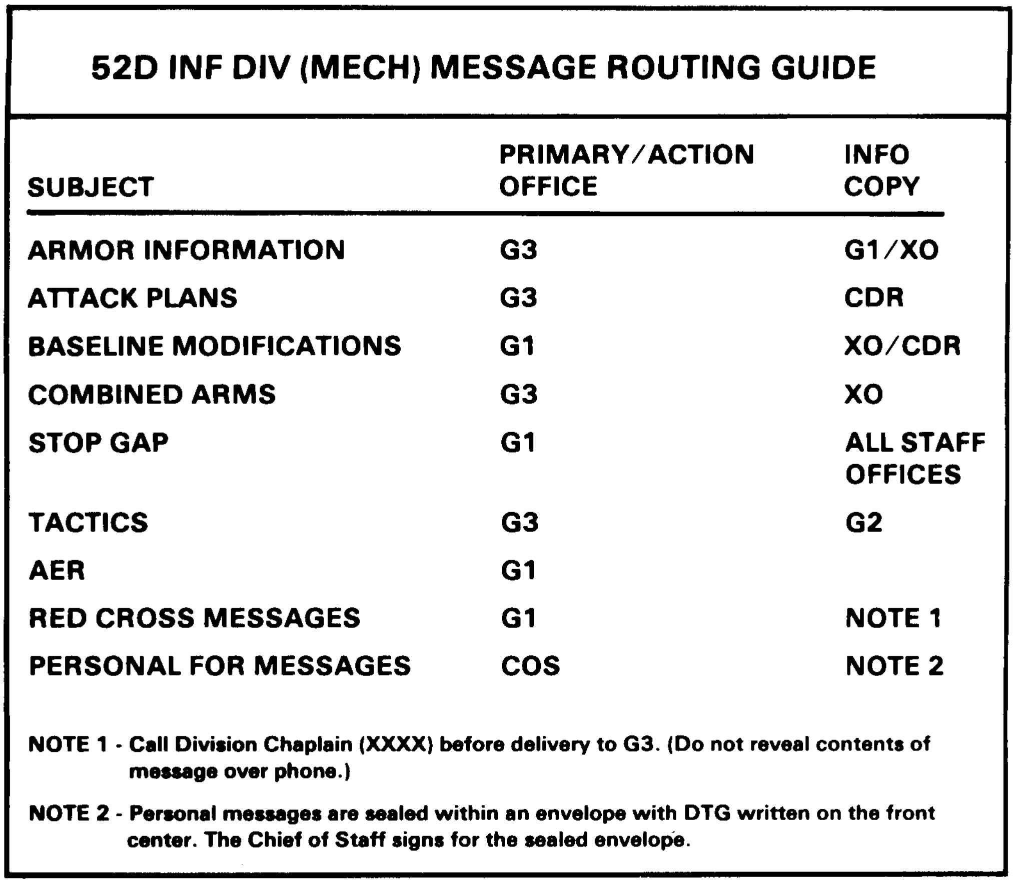
Signal officers will not conduct internal distribution. They write the policy and procedures that staff or CP sections use in the field which govern both electronic and manual means. Individual staff sections generate their own copies and transport them using their own resources to selected distribution points (that is, drop boxes if applicable). Each staff section picks up its own distribution per the unit SOP. If the Army or a unit resources the signal brigade/battalion with messengers and transportation, signal will publish a messenger service plan. Signal organizations are not resourced with messenger augmentation. Individual staff sections coordinate their own resources for transporting messages. The signal officer coordinates with supported staff elements to develop an internal distribution routing guide. This routing guide shows CT operators how to make the required number of copies. Figure 5-1 shows an example of a message routing guide. Individual units develop their own procedures to accomplish the commander's intended mission. This routing guide enables personnel to effectively deliver or make the required notification when receiving sensitive/important record traffic communications at the CT.

High precedence (IMMEDIATE and FLASH) delivery instructions should be provided to the CT operator. This speeds delivery service to the intended addressee and ensures that messages are acted on by the correct office/section.

The unit security officer provides the CT operator with a current security clearance roster. This roster identifies personnel authorized to receive classified messages.

- A classified message is never released to an unauthorized person. A SECRET message is never released to an individual with less than a SECRET security clearance. A classified message is never delivered to an individual until his security clearance is verified or known.

- All classified messages are delivered with the appropriate level classified cover sheet attached.



52D INF DIV (MECH) MESSAGE ROUTING GUIDE

SUBJECT	PRIMARY/ACTION OFFICE	INFO COPY
ARMOR INFORMATION	G3	G1/XO
ATTACK PLANS	G3	CDR
BASELINE MODIFICATIONS	G1	XO/CDR
COMBINED ARMS	G3	XO
STOP GAP	G1	ALL STAFF OFFICES
TACTICS	G3	G2
AER	G1	
RED CROSS MESSAGES	G1	NOTE 1
PERSONAL FOR MESSAGES	COS	NOTE 2

NOTE 1 - Call Division Chaplain (XXXX) before delivery to G3. (Do not reveal contents of message over phone.)

NOTE 2 - Personal messages are sealed within an envelope with DTG written on the front center. The Chief of Staff signs for the sealed envelope.

Figure 5-1. Message routing guide.

Received messages are the responsibility of the CT operator until delivered to the addressee or placed into internal distribution center distribution boxes. The signal officer and his staff is responsible for internal unit distribution boxes.

5-2. Message Privacy Requirements

CT operators are not to discuss or to reveal the contents of a received message except to the addressee or to an authorized representative.

A strict need-to-know policy is followed and documented as directed in the SOP. Personnel, regardless of rank or position, are not given access to information copies of messages unless authorized by the addressee. CT operators release messages only to those organizations or individuals as stated in the CT routing guide. The addressee makes all additional distribution as required.

5-3. Message Retention/Audit Trail

The CT operator can store a record of message transactions (sent and received messages) in the terminal's HISTORY file. In some CT configurations, this function is automatic. To have an audit trail of received messages, the CT operator should print a HISTORY file as indicated in the unit SOP.

HISTORY files do not show the subject matter of a message. To assist in locating or retrieving a received message, the CT operator should keep a copy of each message received. (See paragraph 5-4.) A copy of the HISTORY file and a copy of each received message should be kept on file in the CT area for a period of time determined by the unit SOP. This speeds up message retrieval and service action should a service message be received requiring action to be taken on a previously received or transmitted message.

Classified messages must be filed and protected IAW AR 380-5.

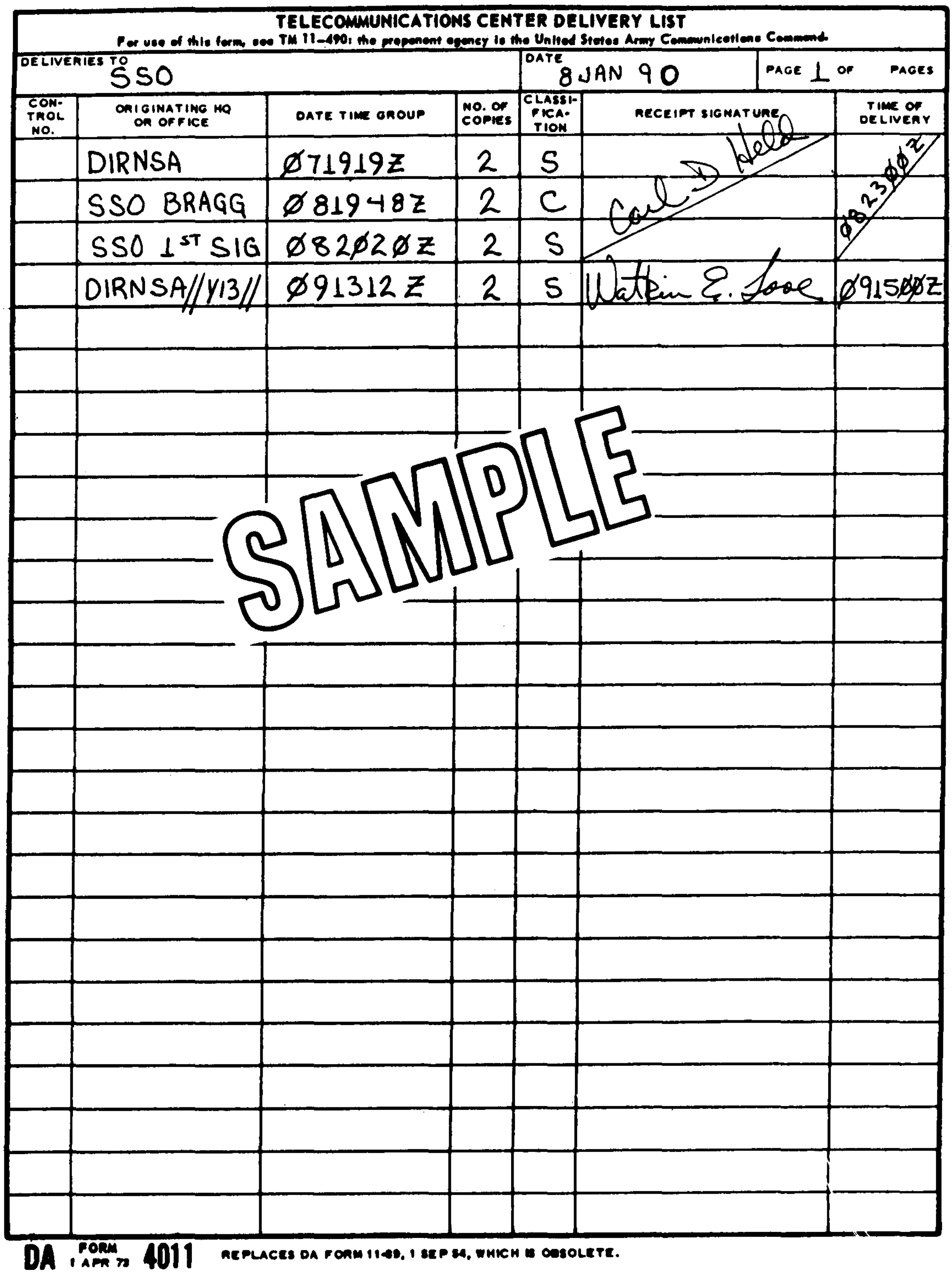
All files must be maintained IAW AR 25-400-2. CT operators are to maintain an internal records system to support the TRTS mission and information mission area requirements as published by the signal officer.

The unit commander or signal officer may require additional internal logs, records, and files to be maintained in support of the CT. These may be historical or reference files and must be maintained IAW AR 25-400-2.

To assist in an audit trail, the CT operator releases received messages to the addressee or a designated representative on DA Form 4011. Figure 5-2 shows a sample of DA Form 4011 with required entries.

Personnel signing for messages are to sign their payroll signature and place a time and date next to their name.

CT operators must initial the DA Forms 4011 to indicate which messages they released to addressees.



TELECOMMUNICATIONS CENTER DELIVERY LIST

For use of this form, see TM 11-490: the proponent agency is the United States Army Communications Command.

DELIVERIES TO SSO | DATE 8 JAN 90 | PAGE 1 OF PAGES

CONTROL NO.	ORIGINATING HQ OR OFFICE	DATE TIME GROUP	NO. OF COPIES	CLASSIFICATION	RECEIPT SIGNATURE	TIME OF DELIVERY	
	DIRNSA	Ø71919Z	2	S	Carl D Hell	Ø823ØØZ	
	SSO BRAGG	Ø81948Z	2	C			
	SSO 1ST SIG	Ø82Ø2ØZ	2	S			EL-1
	DIRNSA//Y13//	Ø91312Z	2	S	Watkin E. Sooe	Ø915ØØZ	EL

DA FORM 1 APR 73 4011 REPLACES DA FORM 11-69, 1 SEP 54, WHICH IS OBSOLETE.

Figure 5-2. Sample of DA Form 4011.

5-4. Record Traffic Journal

The record traffic journal can be maintained as a multipart folder or three-ring binder. This journal keeps the oncoming shift informed of ongoing actions and serves as a quick information source for the command/staff personnel. The CT operator arranges the journal as follows:

- Copies of outgoing record traffic.

- Copies of incoming record traffic.

- Copies of delivery lists showing when and to whom record traffic was delivered.

- DA Form 1594 may be used to provide detailed information the CT operator wants to document.

Retain messages in accordance with established records management procedures. Journals may be of significant historical value or as documentation of lessons learned on particular tactical deployments. CT operators should protect journals and message retention files IAW the highest level of classified messages contained in the file.

Chapter 6

Formal Service Message Fundamentals

6-1. Introduction

This chapter presents information regarding service messages, the use of operating signals, and service message logs .

Service messages are short concise messages between CTs, switches, or TCCs requesting action be taken on a previously sent or received message. For example, service messages are sent to request RETRANSMISSION of a received and garbled message or to advise a CT they have sent a message to the wrong addressee/CT.

Service messages contain one or more combinations of letters called operating signals (or Z signals). Operators use Z signals instead of lengthy message text to state a problem or request certain action be taken. Z signals represent questions, answers, or requests for information over communications paths.

ACP 131 ( ) contains hundreds of Z signals that can be used in JANAP and DOI 103 messages. Normally, only a few Z signals are used frequently in message switching networks. CT users must be familiar with the more commonly used Z signals so as to provide a quicker response time on serviced messages. Appendix E contains a list of commonly used operating signals and their meanings.

One copy of each service message received or transmitted is attached to the original message being referenced in the service message. Any action that is required must be processed and the message delivered to the intended addressees within the speed-of-service requirements of each precedence level.

Incoming service messages are an indicator of operator training requirements and levels. Supervisors should closely monitor the number and types of service messages and ensure all assigned CT operators are aware of service message procedures and requirements. When CT operators know what actions are required for various service messages, writer-to-reader processing times are decreased.

6-2. CT Preformatted Service Messages

The CT has built-in preformatted selections for service messages which the operator can call up from the EDIT menu. These are listed in a subsequent paragraph. In most cases, these preformatted service messages will meet the CT operator's needs in accomplishing service actions. The CT operator calls them up and uses them in the following manner.

- From the MAIN menu, select the EDIT menu.
- From the EDIT menu, press SERVICE function key. Either the GENSER or DSSCS service message menu is displayed depending on the terminal network.
- Move UP and DOWN arrow keys to highlight the service message needed.
- Press SELECT function key. A prompt to select a service message appears.
- Press SELECT function key to extract data service message or NO MSG to manually enter information.
- Enter service information/action/Z signal as needed. When you are finished, the service message is displayed.
- Press MENU key to return to service menu and prepare to send the service message as an outgoing message.

The following preformatted service messages are available:

- Voluntary Correction of Transmitted Message

  -Portion of message
  -Entire message

- Misrouted Message

  -Corrected and resent (relayed)
  -Unable to relay

- Missent Message
- Suspected Duplicate
- Receipt of Unmarked Duplicate Messages
- Notification of Garbled Message
- Request Retransmission
- Retransmission
- Readdress Multiple Page

The service messages that an operator can select are explained below.

Voluntary correction (VOL CCN) of transmitted messages.

For Portion of Message

```
RTTUZYVW RADADAAO03 0012109-UUUU--RAASSAA.
ZNR UUUUU
BT
UNCLAS SVC NON-INTELLIGENCE
ZUI RADADAA0002 0011837 0118372 JAN 90
VOL CCN CHANGE LINE SEVEN WORD SIX TO READ
FOXTROT
VICE GOLF .
BT
#0003
```

--OR--

For Entire Message

```
RTTUZYVW  RADADAA003  0012109-UUUU--RAASSAA.
ZNR UUUUU
BT
UNCLAS SVC NON-INTELLIGENCE
VOL CCN RADADAA0002 0011837Z JAN 90
R 011837Z JAN 90
(ORIGINAL MESSAGE TEXT WITH CORRECTIONS MADE)
BT
#0003
```

A VOL CCN of a transmitted message saves time by correcting a portion of a message that was already transmitted. When you select this service message, you add your change after VOL CCN.

VOL CCN service messages are used when significant errors which affect the substance of a message are detected after transmission.

An entire message may be corrected by using the procedures shown in the example above.

After receiving a VOL CCN service message, the CT operator processes the service message ahead of outgoing messages of the same or lower precedence.

The CT operator takes the following actions:

- Retrieves the original message received from the received message file.
- Makes the necessary corrections.
- Marks the corrected message as a CORRECTED COPY .
- Redistributes the message to the original addressee(s).

  Optionally may add CORRECTION UNDERLINED.
- DESTROYS ALL OTHER COPIES.

Misrouted message.

Corrected and Resent (Relayed)

```
RTTUZYVW RADADAA0004 0012114-UUUU--RAASSAA.
ZNR UUUUU
BT
UNCLAS SVC   NON-INTELLIGENCE
ZUI RADADAA0002 0011837 011837Z JAN 90
ZEQ-3 RUADAAA 0211734
BT
#0004
```

--OR--

Unable to Relay

```
RTTUZYVW RADADAA0004 0012114-UUUU--RAASSAA.
ZNR UUUUU
BT
UNCLAS SVC NON-INTELLIGENCE
ZUI RADADAA0002 0011837 011837Z JAN 90
ZEQ-4
BT
#0004
```

A service message for a misrouted message informs the sending terminal that the receiving station is not the addressee on the message, and that the wrong RI has been used.

Upon receiving a misrouted message, the receiving CT is responsible for one of two actions.

- Relay the message and inform sending station of action taken. The ZEQ-3 example informs the sending station of the message being received at the wrong station and the receiving CT relaying the message to the correct CT. The time of relay is placed after the correct CT's RI to alert the sending CT of the time relayed.

- Notify originating station that message has been misrouted and no other action taken. The ZEQ-4 service message is sent to the originating CT to inform the terminal that the message has been misrouted, the correct RI is unknown, the addressees correct RI must be determined, and the message must be retransmitted to the correct RI.

The receiving CT is responsible for delivering a received message or notifying the originating CT that the message has not been delivered because an incorrect RI has been used.

A copy of the service message is attached to the original misrouted message and is placed in the RECEIVED MESSAGE FILE .

Missent message.

```
RTTUZYVW  RADADAA0005  0012116-UUUU--RAASSAA.
ZNR UUUUU
BT
UNCLAS SVC NON-INTELLIGENCE
ZUI RAASSAA0002 0011837 011837Z JAN 90
ZEQ-1 TOR 0212321Z
HEADER FOLLOWS
RTTUZYUW  RADADAA0002  0011837-UUUU--RADFDAA.
#0005
```

A missent message is a message that has the correct RI but has been inadvertently transmitted by the automated message switch.

The receiving CT is responsible for relaying a missent message as a suspected duplicate (ZFD) and sending a service message (ZEQ-1) to the originating CT to inform them of the time of relay.

Suspected duplicate.

```
RTTUZFDY RADADAA0002 0011837-UUUU--RAASSAA.
ZNR UUUUU
R 011837Z JAN 90 ZFD
FM CDR 5TH CORPS FRANKFURT GE//IAESA//
TO RAASSAA/CDR FT HOOD TX//AEBADT//
BT
UNCLAS NON-INTELLIGENCE
(ORIGINAL MESSAGE TEXT)
BT
#0002
```

A suspected duplicate message is sent out when one or more addressees claim they never received the original transmission, or if the CT operator is relaying a missent message.

- The message is resent because the addressee claims the message was never received.

- The Z signal ZFD tells CT addressees that they may have already received the message.

- After the message has been selected from the MSG directory, the CT automatically makes the changes to the header. No further changes are required by the CT operator.

The CT operator processes and delivers messages marked as SUSPECTED DUPLICATE to alert addressees that the message may have already been received.

Receipt of unmarked duplicate message.

```
RTTUZYVW  RADADAA0006  0012119-UUUU--RAASSAA.
ZNR UUUUU
BT
UNCLAS SVC NON-INTELLIGENCE
ZUI RAASSAA0002 0011837 0118372 JAN 90
RECEIVED UNMARKED DUPLICATE
TOR 0119012 AND 0119122
HEADER FOLLOWS
RTTUZYUW  RAASSAA0002  0011837-UUUU--RADADAA.

#0006
```

A service message showing receipt of an unmarked duplicate message informs the sending CT that a message has been received twice.

When a CT receives a service message reporting receipt of an unmarked duplicate, the CT operator checks the HISTORY file to ensure the message has not been retransmitted twice by mistake. If only one transmission has been made, the CT user sends a routine message to the connected message switch/parent or alternate AN/TYC-39() and cites the--

- Complete header of the message.

- Time transmitted.

- Information to identify the CT who received the duplicate messages.

- Time of receipt of both messages.

Duplicate messages will be delivered to the addressee as a SUSPECTED DUPLICATE. The addressee, not the CT operator, makes the final determination as to what (if any) action is required, or if the message has already been received and action taken.

A copy of this service message is attached to the previous service message to indicate the completed action.

Notification of garbled message.

```
RTTUZYVW  RADADAA0007  0012121-UUUU--RAASSAA.
ZNR UUUUU
UNCLAS SVC NON-INTELLIGENCE
ZUI RAASSAA0002 0011837 0118372 JAN 90
ZES-2
BT
#0007
```

The garbled message (ZES-2) service message informs the originating CT that you have received the message and the text is unreadable.

A copy of this service message must be kept in a suspense file until a readable copy of the message is received for delivery. Appropriate follow-up action must be taken periodically until the suspense action is cleared. Follow-up action will be taken based on the precedence of the garbled message.

After a corrected copy is received, the original message, the service message, and the correct copy will be attached and placed in the RECEIVED MESSAGE FILE.

Messages having a precedence of PRIORITY and above will be delivered as received with the message marked DELIVERED SUBJECT TO CORRECTION. Garbled or incomplete high precedence messages will not be held by the CT operator for service actions.

Request retransmission.

```
RTTUZYVW RADADAA003 0011839-UUUU--RASSAA.
ZNR UUUUU
R 0118382 JAN 90
FM CDR 5TH CORPS FRANKFURT GE//IAESA//
TO RAASSAA/CDR FT HOOD TX//AEDBA//
BT
UNCLAS NON-INTELLIGENCE
ZUI RASSAA0005 R 010848Z JAN 90. ZES-2 INT ZDK
(ORIGINAL MESSAGE TEXT)
BT
#0003
```

A request retransmission message asks the distant terminal to complete an action. INT means REQUEST.

The example above shows a CT requesting retransmission of a message from CDR FT HOOD CT due to receiving a garbled message (ZES-2) in Germany.

Had the received message been incomplete, the Z signal ZES - 1 would have been used.

Retransmission (of a previously transmitted message).

```
RTTUZDKW RADADAA0002 0011837-UUUU--RASSAA.
ZNR UUUUU
R 0118372 JAN 90
FM CDR 5TH CORPS FRANKFURT GE//IAESA//
TO RAASSAA/CDR FT HOOD TX//AEDBA//
BT
UNCLAS NON-INTELLIGENCE
(ORIGINAL MESSAGE TEXT)
BT
#0002
```

Retransmission of a previously transmitted message is used to resend a message in response to a request retransmission request by a distant CT. The example above indicates that the message has been corrected and retransmitted in response to a ZES-2 request.

Upon receipt of a ZDKW message, the CT operator must determine if a service action (ZES-2) has been originated by the CT. If the ZDKW is in response to your ZES-2 service, pull the service, process, and deliver the ZDKW as a CORRECTED COPY. Attach a copy of the service message to the garbled message and the ZDKW message for file.

If the receiving CT did not request a retransmitted message (ZES-2 action not originated by your CT), deliver the ZDKW as a SUSPECTED DUPLICATE to the addressee.

Readdressing messages (single page or multiple page).

```
RTTUZYUW  RADADAA001l  0081949-UUUU--RAASSAA.
ZNR UUUUU
R 081948Z JAN 90
FM CDR 5TH CORPS FRANKFURT GE//IAESA//
TO RUSNBAA/CDR 19TH CORPS SEOUL KOR//ITIT//
BT
UNCLAS NON-INTELLIGENCE
(ORIGINAL MESSAGE TEXT)
BT
#00ll
```

A readdressed message is a message that needs to be sent to an addressee that was originally listed on the message, but the RI was not included in the original transmission.

The above example shows a message that was sent to a different addressee than was originally transmitted. The original header remains on the message so that all personnel are aware of who has received the message.

Single and multiple page readdressals look the same and the same information is needed for both.

6-3. CT to CT Service Message Procedures

To send a service message to another CT, use the EDIT menu, select new message, and type what type action is needed and on what message. Select the JANAP 128AP for the header.

Supervisors should ensure training covers service message actions to enable improved speed-of-service to CT addressees.

6-4. CT to TCC Service Message Procedures

To send a service message to a TCC, use the appropriate operating signals and procedures found in Chapter 4 of JANAP 128.

6-5. Automatically Generated Service Messages

The AN/TYC-39( ) and AUTODIN message switches have the capability to automatically generate service messages on messages that have been transmitted by the CT. These service messages are sent to the CT when there is an error in the message header or end of a message which does not allow the message to pass through the AN/TYC-39( ) or AUTODIN.

Examples of automatically generated service messages and the required operator responses follow with a brief explanation. It is important that CT users are familiar and comply with the required actions to process automatically generated service messages. Failure to respond within speed-of-service requirements may adversely impact on the owning organization's mission.

Format or MODE II in JANAP 128 and DOI 103 format.

```
PTTUZYVW RUEBCSD0002 0081948 -UUUU--RUEBDEA.
ZNR UUUUU
UNCLAS SVC RUEBDEA 12340081947
INVALID CSN EXPECTED DEA125 RCVD DEA129 ACC
#0003
NNNN
```

This service message is received when a message with the incorrect CSN has been received by the connected AN/TYC-39( ). If the incorrect CSN has a higher out-of-sequence number than the next-in-sequence CSN expected, the AN/TYC-39( ) will accept the message and process it. Your next CSN would be DEA130.

```
PTTUZYVW RUEBCSD0002 0081948-UUUU--RUEBDEA.
ZNR UUUUU
UNCLAS SVC RUEBDEA1234 0081946
INVALID CSN EXPECTED DEA145 RCVD DEA129 REJ
#0002
NNNN
```

This service message is received when a message with the incorrect CSN has been received by the AN/TYC-39( ). The message switch will reject the message and the CT operator will have to resend the message using the next CSN of DEA146. In both examples above, the automatically generated service message was a result of the CT operator not monitoring the DA Form 5651 and crossing out the CSN number that corresponds to the next outgoing message being sent to or through a message switch.

Open CSN.

```
OTTUZYVW RUEBCSD0042 0081945-UUUU--RUEBDEA.
ZNR UUUUU
UNCLAS SVC
ZFX DEA015 THRU DEA023
#0042
NNNN
```

This service message is received by the CT when a message with an invalid CSN has been received by the AN/TYC-39( ). If you have transmitted a message using the CSN's DEA015 through DEA023, then you must retransmit the messages with a new CSN starting with the next valid CSN from the DA Form 5651.

Invalid security field.

```
OTTUZYVW RUDOCSD0008 0081948-UUULJ--RUDDABA.
ZNR UUUUU
UNCLAS SVC ABA008 RUDOABC1234 0081944
INVALID SECURITY FIELD REJ
#0008
NNNN
```

This service message--a reject--is received when an error occurs with the operating signals ZNR or ZNY and security redundancies codes not matching. The CT operator must correct the error and retransmit the message into the TRTS .

Invalid header.

```
RTTUZYVW RUCLCSD0004 0091948-UUUU--RUCLABA.
ZNR UUUUU
UNCLAS SVC ABA004 RUCLABC1234 0091947
INVALID HEADER REJ
#0004
NNNN
```

This service message--a reject--is received when there is an error in the header of the message. An extra space or one in the wrong location will cause the message to be rejected. The CT operator must correct the error and retransmit the message.

Invalid routing.

```
RTTUZYVW RUCLCSD00005 0091948-UUUU--RUCLABA.
ZNR UUUUU
UNCLAS SVC ABA004 RUCLABC1234 0081948
INVALID ROUTING REPROTECT TO: RUCLAAA
#0005
NNNN
```

This service message is received when an incorrect RI is used. If the RI was obtained from your PLA table, contact your supporting signal officer for updating of the PLA tables.

Note that the invalid routing message will in most cases inform you of the correct RI to be used to retransmit the message.

High precedence message accept.

```
OTTUZYVW RUFTCSD0059 0081920-UUUU--RUCLAI3A.
ZNR UUUUU
UNCLAS SVC R Z ABA009 RUFTABC2012 0081919
#0059
NNNN
```

This service message is received by the CT operator as an acknowledgement of receipt for a message transmitted from the CT with a precedence of FLASH or higher.

R Z means the message was received at the AN/TYC-39( ) for forwarding to the intended addressee.

6-6. Service Message Logs

Incoming and outgoing service messages should be controlled by the CT operator in a manner that will allow for the clearing or timely follow-up of service actions. A service suspense file of terminated and originated service messages is to be maintained until requested or required actions are completed. DA Form 4016 can be adapted to serve as incoming and outgoing service message logs.

All actions relating to a service message must be filed with the original message to give a complete historical picture of the message and actions taken to properly and correctly deliver the message. If the CT operator receives a garbled message, a copy of the outgoing service message and the corrected copy will be attached to the original message received prior to placing in the file. Only the marked corrected copy will be delivered to the addressees.

Chapter 7

Defense Special Security Communications System CT Facilities

7-1. Introduction

This chapter prescribes security procedures in addition to those procedures and requirements found in DOI 101 and DOI 103. When CTs process DSSCS messages, additional security precautions must be afforded to preclude adverse impact upon national security.

Units which have CTs that process DSSCS record traffic present lucrative and vulnerable targets for espionage and enemy operations. The Director, NSA/Chief, Central Security Service (CSS) have prescribed special rules and procedures for handling and reporting loss, storage, and access to DSSCS record traffic and associated communications equipment. DSSCS terminal supervisors must be aware of and enforce required security measures to protect record traffic from loss or compromise.

7-2. Responsibilities

The unit/organization automated message processing special security officer (AMPSSO) is responsible for overall CT security. The AMPSSO receives guidance from the local special security officer (SSO) and is the security controller for the DSSCS CT.

7-3. Special Procedures

Two-person integrity. National policy requires two people working near each other to provide mutual support in maintaining the integrity of the CT processing/storing DSSCS communications. The two-person integrity is in effect at all times when processing and storing TS/SCI defense information. AR 380-5 contains additional information for the implementation requirements for two-person integrity, while the unit's AMPSSO provides local guidance.

Physically separate. DSSCS and GENSER record traffic will be physically separated at all times. (This also includes physical separation of CTS.) Each CT maintains separate files and records. The provisions of DOI 103 for file copies, ASCs, and floppy disks of DSSCS messages are in effect.

ASCs and floppy disks are never to contain both DSSCS and GENSER messages.

ASCs and floppy disks containing SCI messages will be controlled and stored by the SSO.

Entry to processing or storing DSSCS record traffic on the CT is restricted to--

° Personnel whose duties justify their access.

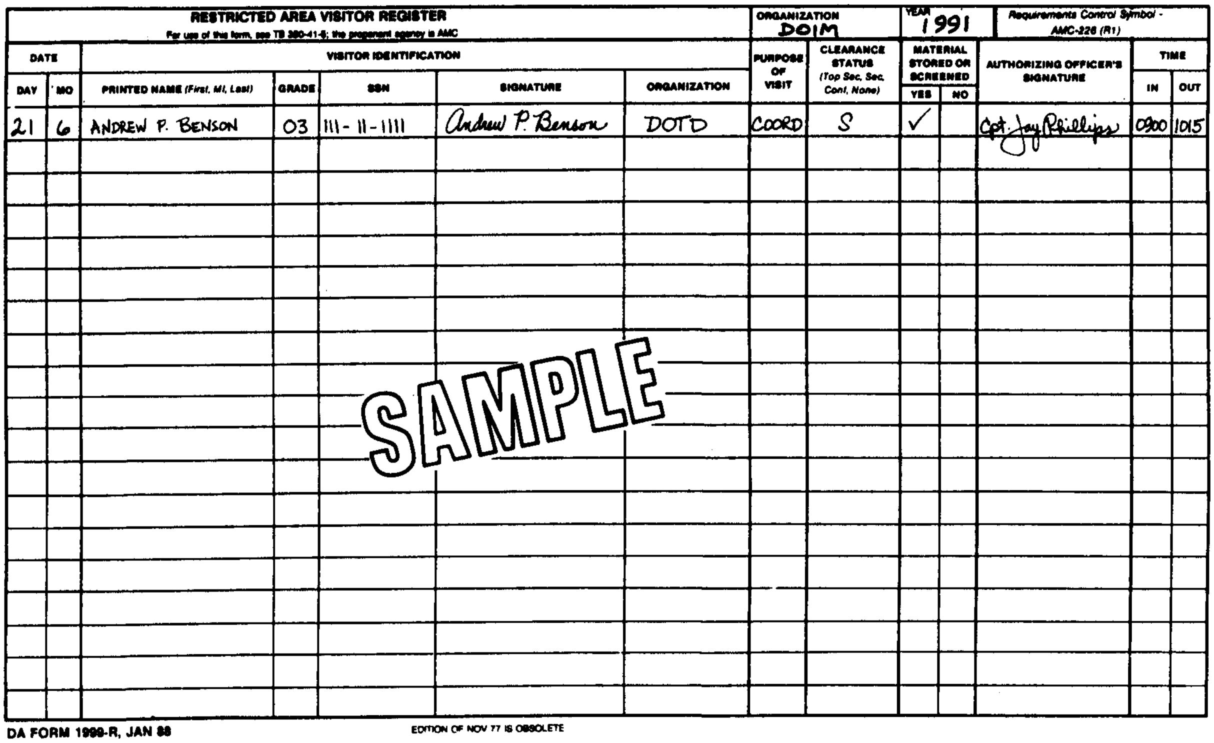
° Personnel who have had their security clearances to SCI defense information verified by the SSO.

Cleared CT operators processing SCI will ensure that noncleared personnel are not allowed in or near the CT until all record traffic processing is completed. (A strict need-to-know policy will be enforced at all times.) Access rosters will be provided by the SSO and maintained next to the CT. Personnel not listed on access rosters will be required to sign DA Form 1999-R.

CTs that have processed SCI must be sanitized after the message processing is completed and before the next non-SCI multilevel user is permitted to operate the terminal. Cleared personnel will make a thorough security check of the area to ensure all SCI-related material, including classified trash, is removed from the area and properly secured.

Use DA Form 1999-R to record personnel authorized by the commander/SSO to have access to the CT. The SSO should sign as the authorizing officer. Figure 7-1 is a sample of a completed DA Form 1999-R. TB 380-41-5 contains a blank form and instructions for use.

All DSSCS messages, except service messages, are processed and delivered to the SSO who is responsible for reproduction and dissemination. DA Form 4011 is used to control DSSCS message delivery to the SSO. The SSO may direct additional delivery instructions for SCI record traffic.



RESTRICTED AREA VISITOR REGISTER

For use of this form, see TB 380-41-5; the proponent agency is AMC

ORGANIZATION DOIM | YEAR 1991 | Requirements Control Symbol - AMC-226 (R1)

DATE		VISITOR IDENTIFICATION					PURPOSE OF VISIT	CLEARANCE STATUS (Top Sec, Sec, Conf, None)	MATERIAL STORED OR SCREENED		AUTHORIZING OFFICER'S SIGNATURE	TIME	
DAY	MO	PRINTED NAME (First, MI, Last)	GRADE	SSN	SIGNATURE	ORGANIZATION			YES	NO		IN	OUT
21	6	ANDREW P. BENSON	03	111-11-1111	Andrew P. Benson	DOTD	COORD	S	✓		Cpt. Jay Phillips	0900	1015

SAMPLE

DA FORM 1999-R, JAN 88 EDITION OF NOV 77 IS OBSOLETE

Figure 7-1. Sample of DA Form 1999-R.

Compromise, possible compromise, or any security violations involving DSSCS/SCI material will immediately be reported to the SSO.

7-4. Security Indoctrination and Training

Organizations with DSSCS CTs must have a supervised and documented training program to indoctrinate CT user personnel in their individual security responsibilities. This training will include the following:

- Safeguarding the CT and associated ASCs and floppy disks from unauthorized access.

- Basic emergency planning for emergency destruction, evacuation, and storage.

- Reporting procedures, channels, and time frames to report any incidents of compromise or insecurities involving the CT, ASCs, floppy disks, or record traffic files.

SSOs will conduct and document security briefings to provide CT users with a clear understanding of what is expected and required to protect the DSSCS message equipment and system. Briefings will be conducted at least quarterly or as prescribed by DSSCS regulations.

The DSSCS CT supervisor/SSO will conduct an ongoing training program for the preparation and transmission of CRITIC messages IAW DOI 103. Assistance in establishing or conducting a CRITIC program can be provided upon request to: Director, NSA/CSS, ATTN: DDT, Fort George G. Meade, Maryland, 20755-5000. Normally, the SSO will be the CRITIC control officer who will monitor the level of CRITIC message processing proficiency at consolidated CTs.

7-5. Tactical Sensitive Compartmented Information Facilities (SCIFs)

CTs initialized for and processing DSSCS tactical record traffic must be located in a SCIF. While in a garrison environment and depending upon the unit's formal record traffic requirements, the CT may be utilized either within an accredited fixed SCIF or inside a tactical vehicle collocated with an accredited SCIF. The tactical vehicle must be parked near or, if possible, collocated next to the garrison SCIF. If the CT is not used in garrison for record traffic or training, the CT must be purged of all memory and the tactical vehicle completely sanitized of all DSSCS files and associated administrative documents. Upon deployment to an exercise or tactical location where the CT will be initialized, a tactical SCIF must be formally established prior to the CT processing DSSCS record traffic. Refer to Defense Intelligence Agency Manual (DIAM) 50-3 for the required information to be forwarded through command channels to establish a tactical SCIF.

A tactical SCIF is defined as, but not limited to, one of the configurations listed below. The exact type of tactical SCIF depends primarily upon the commander's requirements for DSSCS record traffic and the tactical situation.

- Tactical vans, shelters, or closed-in vehicles.

- Tents or operations in vacated civilian or military buildings. (See first paragraph under DSSCS Tactical Security Considerations below.)

- Aircraft (fixed or rotary) or bunkers.

The following are examples of tactical SCIFs.

- TOCs.

- Special security communications and information processing vans.

- Telecommunications facilities used for processing SCI voice and data traffic.

- Airborne and ground command posts or emergency relocation activities used for command, control, communications, and intelligence operations.

DSSCS tactical security considerations.

Operation of a tactical SCIF and associated CTs requires continuous 24-hour per day operation for the entire period of operations/activation. Two indoctrinated individuals will be present for duty within the tactical SCIF. These individuals must be armed at all times if the tactical SCIF is located in a tent.

Overall security of a tactical SCIF is not at the same degree as at fixed (sustaining/strategic) SCIFs. To enhance security in a tactical situation, the SCIF, where operationally possible, will be located within the supported headquarters defensive perimeter and as close to the TOC as the tactical situation dictates.

Tactical SCIFs will be located within an area that uses a physical barrier around the SCIF and provides for a single access point. An armed guard will be on duty at all times to limit access to the area. Strict access control procedures will be used to restrict unauthorized personnel from gaining access to the SCIF or security perimeter. Personnel who may enter the tactical SCIF area without escort will be identified on a current access roster provided to the guard by the SSO.

Record traffic produced within the tactical SCIF, both in paper copy and the information/data maintained on ASCs or floppy disks, will be limited to that needed to support, sustain, and document tactical operations. CT-produced paper copy, ASCs, and floppy disks will be afforded a rapid and thorough means of destruction under tactical conditions or hostile actions.

CT users will ensure large volumes of DSSCS traffic, ASCs, and floppy disks do not accumulate within the tactical SCIF.

AMPSSO/SSOs will coordinate with the supporting information service support officer (ISSO)/signal officer to ensure that a system of controls are established to monitor and control the paper and disk holdings produced by the CT and maintained within the tactical SCIF. The Modern Army Recordkeeping System (MARKS) will be used to identify procedures for maintenance, retirement, and destruction of CT record traffic files.

Chapter 8

Informal TRTS

8-1. Introduction

This chapter covers informal record traffic- - what equipment is used, how it's accounted for, how it's transferred across the system, how it interfaces with formal record traffic systems, and how it's passed to strategic and tactical packet networks. Also covered is the role of personal computers and the interconnection with the ATCCS.

Informal record traffic capability is primarily limited to users within combat net radio (CNR) and the ACUS. The informal record traffic capability is implemented from maneuver battalions through EAC for users who have a requirement to send C^2 information but not authorized access to formal TRTS. (See Figure 8-1.)

Informal TRTS allows commanders and their staffs to originate and terminate narrative text, map, graphic, and operational overlay messages which support battlefield missions. No specific format for informal record traffic exists. An example of informal record traffic is a photograph with comments handwritten on the document surface, then transmitted over the tactical circuit switched network. Another example is narrative text prepared by the battalion S3 and transmitted by the circuit switched network to the brigade S3.

8-2. Informal TRTS Message Equipment

The LDF serves as the user's primary input/output device for informal message traffic. To transfer an informal message, a user connects the origination LDF to the destination LDF by the dial-up ACUS, CNR, or interfaces between the two systems. Figure 8-2 shows examples of LDF connections. Once connections are complete, the user coordinates the transmission, transmits the record traffic, and terminates the call. Acknowledging the receipt may or may not be required.

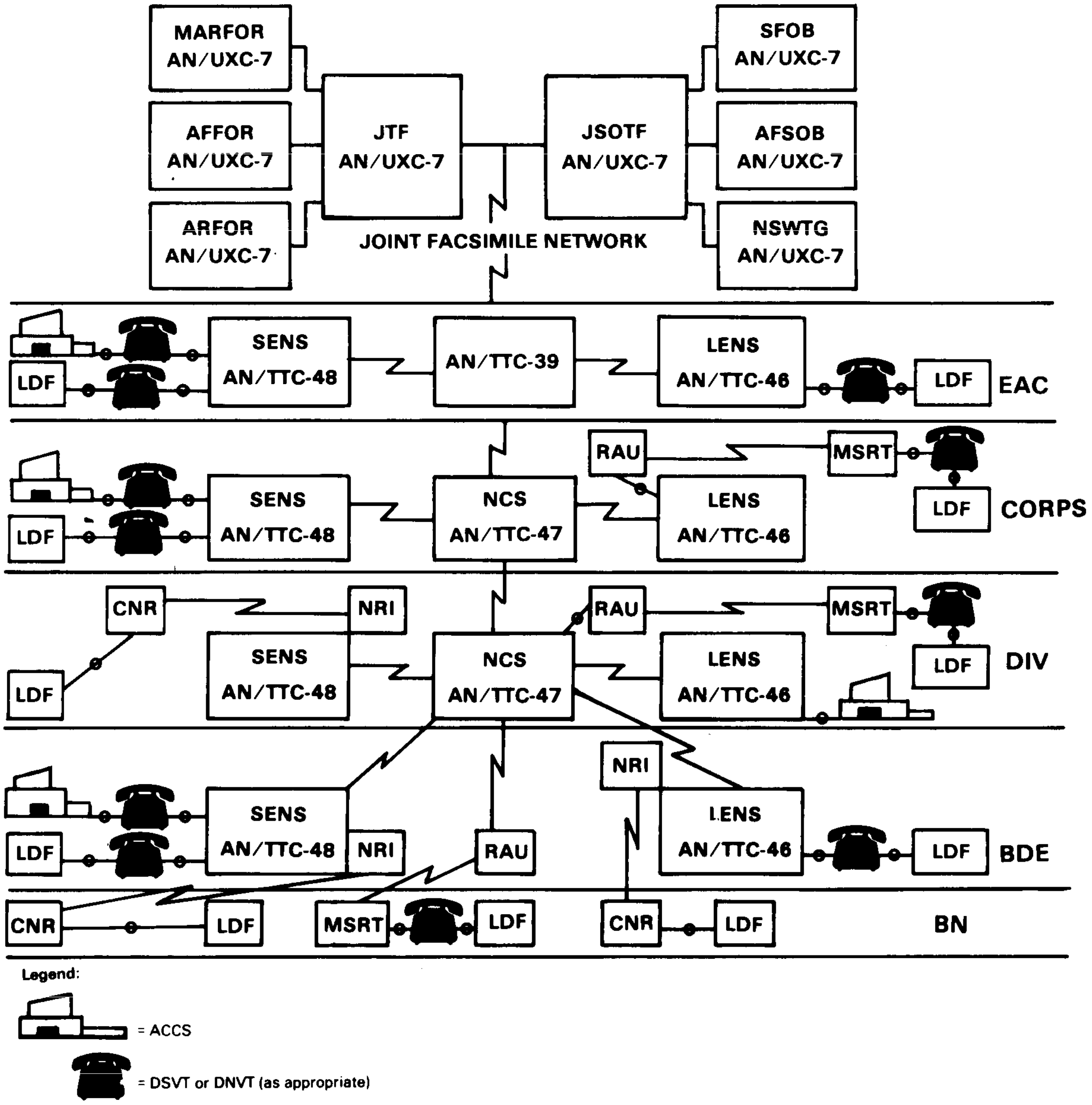
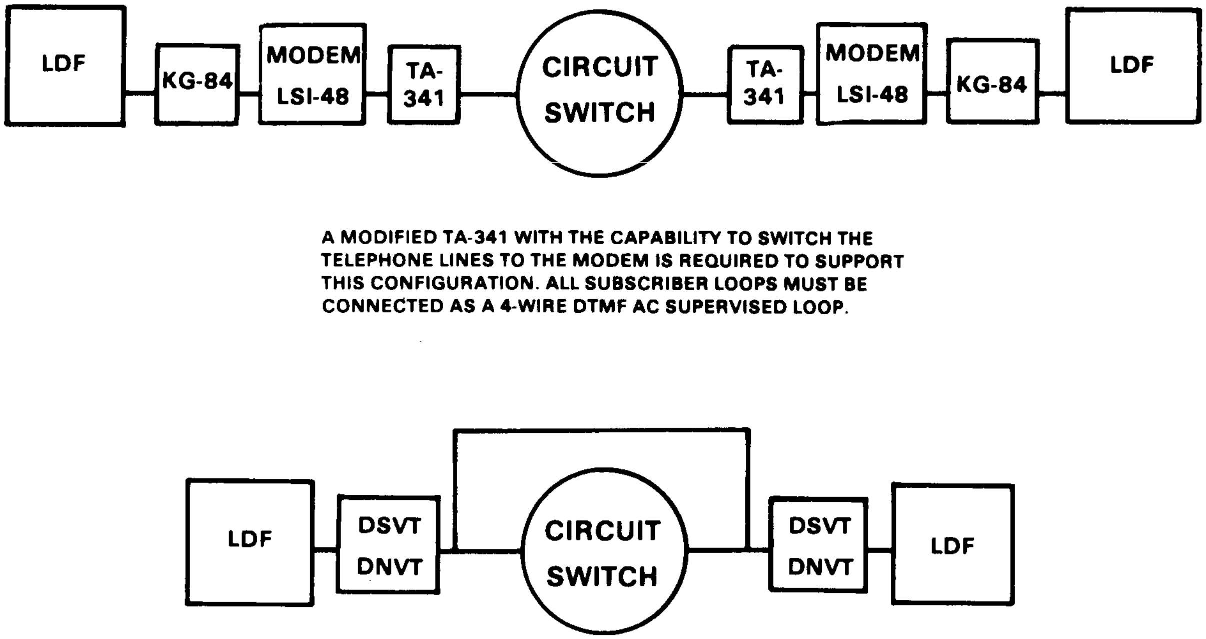


Figure 8-1. Informal TRTS architecture (circuit switched network).



A MODIFIED TA-341 WITH THE CAPABILITY TO SWITCH THE TELEPHONE LINES TO THE MODEM IS REQUIRED TO SUPPORT THIS CONFIGURATION. ALL SUBSCRIBER LOOPS MUST BE CONNECTED AS A 4-WIRE DTMF AC SUPERVISED LOOP.

THE AN/UXC-7 WILL INTERFACE WITH THE TRI-TAC NETWORK USING EITHER SWITCHED OR POINT-TO-POINT FACILITIES.

Figure 8-2. Examples of LDF connections.

LDF is the standard equipment used to pass informal record traffic communications. However, users who have a requirement to pass informal record traffic may use authorized GP user-owned and -operated terminal equipment at their locations. In addition, the following equipment may be used if prior approval is obtained by the unit signal office.

- Desktop or laptop PCs.
- Unit PCs which can be connected to a DSVT or DNVT data port.
- Stand-alone CTs (no standard format used).

8-3. Informal TRTS Message Accountability

Because the LDF does not connect to a message switch or other formal record traffic device, informal message transmissions are not automatically documented. However, some means of transmission/receipt documentation may be required to provide an audit trail for facsimile messages. Therefore, LDF users should maintain an audit record of messages that are transmitted and received at their LDF. This provides record traffic load statistics along with documentation of what is received and to whom the record traffic is delivered. As more automated methods to trace and verify transmissions of informal record traffic are developed, manual recordkeeping will be replaced. Local users will prescribe whatever method suits the unit's need/ operational requirements.

All messages passed over LDF should be voice coordinated before transmission. This coordination should include precedence of the message traffic, number of pages in the transmission, and verification of the receiving operator's name or call sign. In addition, exact delivery instructions can be required for classified or sensitive information. The operator should use authentication procedures when passing classified information. The unit signal operation instructions (SOI) supplemental instructions contain these procedures.

LDF users should precede each transmission with a Facsimile Transmittal Header Sheet to aid in delivery and security.

A Facsimile Transmittal Header Sheet will be locally made and reproduced by the user unit or DA Form 3918-R may be used. Minimum required information on the Facsimile Transmittal Header Sheet will include--

- FROM addressee (name and office symbol).
- TO addressee (name and office symbol).
- Classification of fax transmission.
- Delivery instructions (optional). These instructions may include such entries as DELIVER IMMEDIATELY or HOLD AND DELIVER FIRST DUTY HOUR.
- DATE-TIME/MONTH/YEAR (for control/accountability purposes.) Each fax message should have a unique DTG.
- Number of pages. Always include the Facsimile Transmittal Header Sheet as one of the total number of pages in the transmission. This will enable continuous page accountability.

- Authorized releaser's signature.

The Facsimile Transmittal Header Sheet may serve as a user/operator record copy of the transmission and the addressee. If manual recordkeeping is maintained, the fax operator may return all copies of faxed material.

Fax is an informal system and will not be used to pass record traffic not previously originated or terminated within formal record traffic system channels. Coordination for formal messages may be effected by fax users whenever the need exists.

8-4. Informal Message Transfer

Single Channel Ground and Airborne Radio System (SINCGARS) and the mobile subscriber radiotelephone terminal (MSRT) are the primary means of transmitting fax traffic between users in mobile situations. A single broadcast can provide the information to several addressees simultaneously when required.

LDF users should transmit fax data over wire to the ACUS, when available, to reduce electronic signatures.

FM 11-32 outlines procedures for placing NRI calls from the radio and telephone sides of NRI systems.

CT to SINCGARS transmission may be accomplished following procedures shown in Figure 8-3.

8-5. Informal/Formal TRTS Interface

Record traffic passes from the informal to formal TRTS (or vice versa) whenever a requirement exists to cross system channels. The following procedures outline the transfer between two systems:

Informal to formal TRTS. When the LDF user requires transfer of a message into the formal TRTS, the message text is couriered to a CT for proper message formatting and entry into the formal network. The CT may be at the LDF user's level or at the next higher echelon. Coordination with the LDF organization signal officer is necessary for informal message traffic to be accepted at the CT. This coordination is necessary to ensure only official authorized messages are entered into the formal TRTS. The CT user will be responsible for properly formatting/ processing the LDF user's message into the formal system.

Formal to informal TRTS. A formal message received by a CT will be printed out on hard copy and couriered or faxed over the ACUS to the destination LDF. Message accountability procedures will be observed by the receiving CT. CTs will be collocated with or have direct access to the LDF to effect transfer of record traffic into the informal system.

8-6. Informal TRTS Over Strategic and Tactical Packet Networks

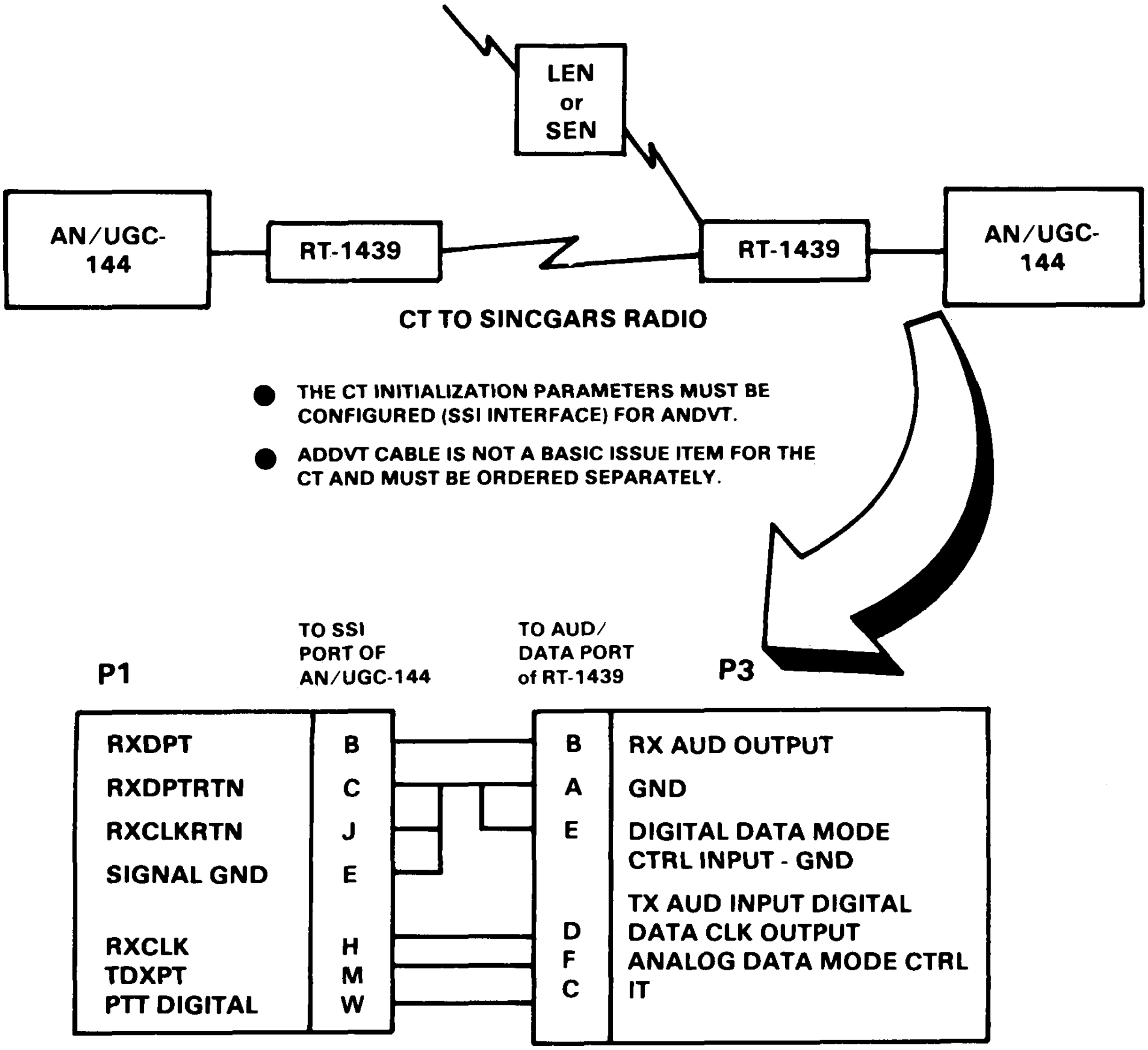
The tactical packet network (TPN) is the battlefield packet network capable of handling traffice classified through SECRET. It overlays on the EAC and ECB voice communications network. DDN consists of two packet networks--the defense secure network (DSNET) and the military network (MILNET) which is unclassified. Objectively, TPN will connect to both DDN networks as shown in Figure 8-4. From a user's viewpoint, the networks will be totally transparent. Users will access their computer, compose messages, and transmit the messages.

TPN fielding to ECB is scheduled to start in September 1991 with full fielding expected by October 1992. Fielding to EAC is scheduled for the FY 93 to FY 94 time frame.

Packet switching is a data handling technique. Users send messages to the packet switch to which they are connected. The packet switch divides the message into packets and treats each packet as an individual transaction. Using network routing that adapts rapidly to the traffic loading and circuit connectivity, packet switching provides --

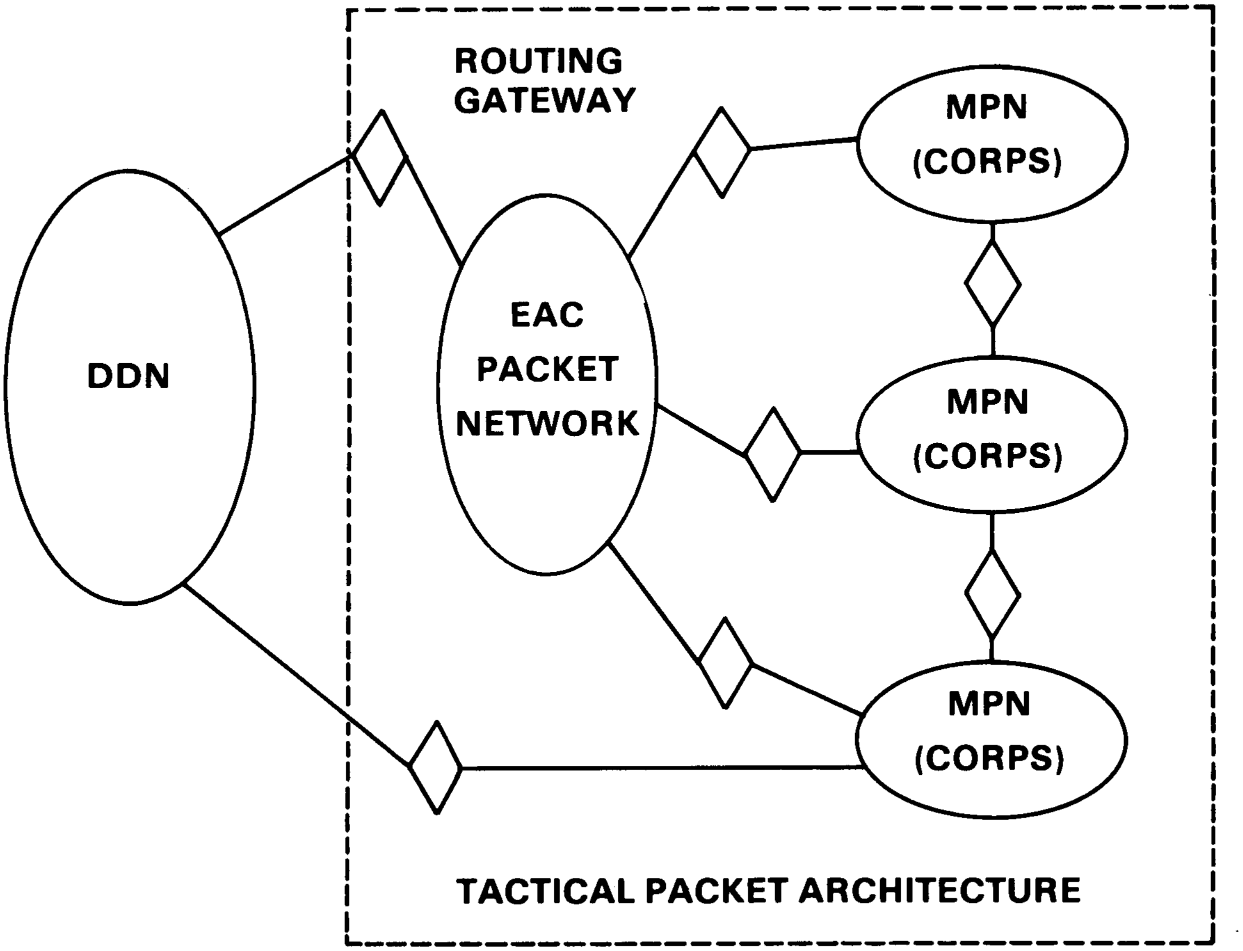
- Efficient use of limited communications capacity.
- Guaranteed data delivery.
- Fast delivery service for small amounts of data such as database updates.

Packet switching techniques are not designed for large database dumps or continuous data streams from sensors. The time delay imposed by the packet switches becomes so great that dedicated circuits are more efficient.



- THE CT INITIALIZATION PARAMETERS MUST BE CONFIGURED (SSI INTERFACE) FOR ANDVT.
- ADDVT CABLE IS NOT A BASIC ISSUE ITEM FOR THE CT AND MUST BE ORDERED SEPARATELY.

Figure 8-3. CT to SINCGARS radio.



◇ = Gateway device

MPN = MSE packet network

Figure 8-4. Objective architecture.

8-7. Informal TRTS Using PCs

There is a difference in the connectivity of PCs to DDN and TPN as illustrated in Figure 8-5.

In garrison, PCs connected to DDN are used as simple terminals. PC software has to be loaded into the PC's hard disk drive memory to allow the user to interoperate correctly with the DDN. The ISSO/BSO must be contacted to ensure the PC is properly configured for the appropriate terminal settings. They will also provide guidance in connection of the PC to a terminal access controller (TAC) or other associated host terminal.

The PC user must understand how to use a PC communications package so the PC can interoperate/interface with the DDN.

In addition to understanding that the PC is not a host or access terminal, the PC user must be aware that the host or TAC connection alone does not give access capabilities to DDN. To access a host or a TAC from a PC, the user must have an authorized account (address and password) and this information must be registered by the ISSO/BSO with the host/TAC terminal.

When deployed to the field, PCs must be capable of operating as hosts. All PCs connected to TPN must have installed the TPN registration and TPN host-specific software. PCs are connected directly or via a command post (CP) LAN. Each PC has its own name and address compatible with the DDN format.

Unlike the strategic network, TPN users are mobile and there is no habitual relationship between a packet switch and the users.

TPN has developed a registration process that maps user names to physical address. Users affiliate to the network and their physical location is recorded. The records are queried by users who wish to send messages but do not know the physical location of the recipient. Registration and querying of records is an automated function transparent to the user. It is performed automatically by the communications package of the host computer.

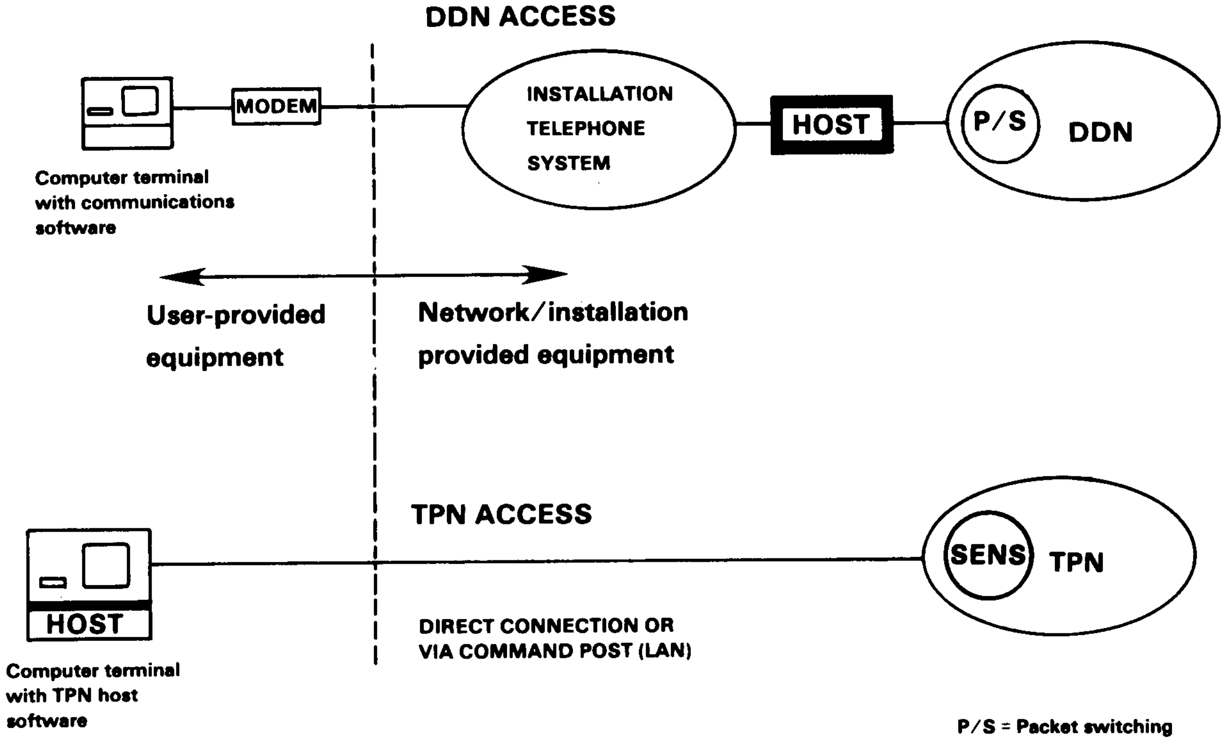


Figure 8-5. Comparison of DDN vs TPN access.

The objective of total interoperability between TPN users and users of MILNET and DSNET requires the development of a multilevel secure (MLS) device. The MLS device will enable TPN users requiring access to both networks from passing classified information to the MILNET.

8-8. User and DDN/TPN Connectivity

Figure 8-6 is a realistic depiction of the interconnection of automation devices on the battlefield. Note that many of the devices are designed to communicate only with other like devices and cannot send data to any other device on the battlefield.

CTs can only exchange information with other CTs.

The only means of transferring data from a PC to a maneuver control system (MCS) device is by carrying a floppy disk from one to the other. MCS could be used to distribute informal record traffic received from a CT. On CTs so equipped, the CT operator would have to download the message to a floppy disk and carry the disk over to the MCS terminal. The MCS operator could then upload the message and distribute it over the circuit switch or packet network. (Note: At publication time of this manual, not all CTs were equipped with floppy diskette drives. Eventually, all CTs will be retrofitted with 3.5 inch diskette drives.)

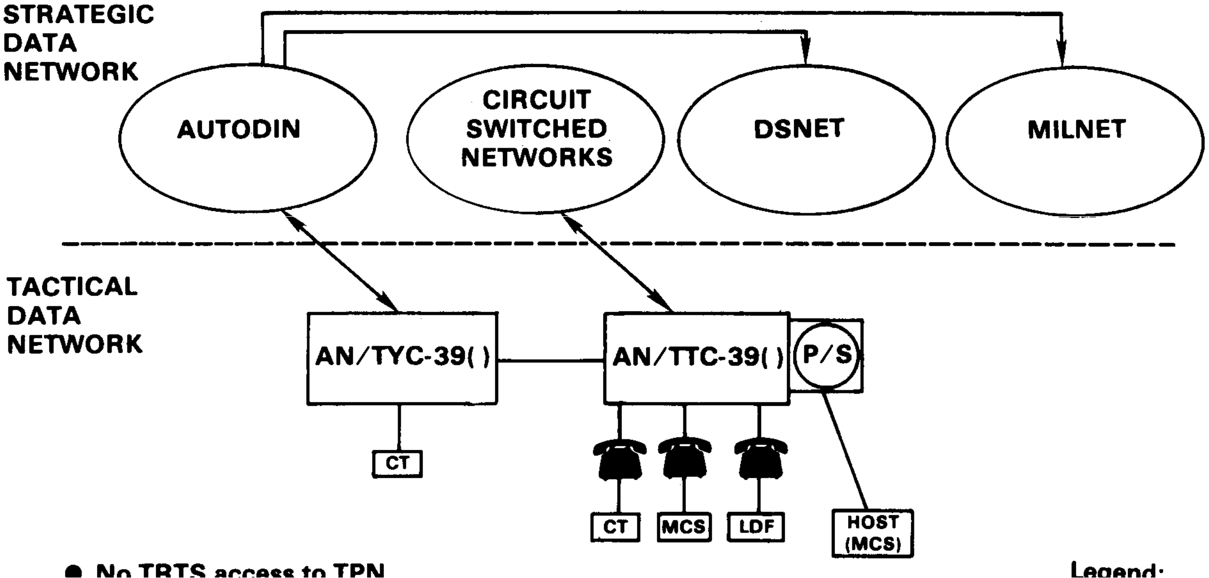
Distribution has the following drawbacks:

- The MCS operator can send the message only to users on his network (either circuit or packet) unless the MCS device is connected to both networks.

- The MCS operator cannot send the message to fax users.

- The MCS operator cannot send the message to PC or CT users.

When all the battlefield functional area C^2 systems are using the packet network, informal traffic should be sent via the packet network. The packet network delivers to multiple addresses and stores messages temporarily for mobile users. The problem is that none of the TRTS components can interoperate with the packet network. File transfer via floppy disk will be the only TRTS to TPN interface.



- No TRTS access to TPN
- PCs & BAS on circuit network cannot interface with TRTS or TPN
- TPN hosts cannot send/receive DDN E-mail or AUTODIN traffic

Legend:

☎ =DNVT/DSVT

Figure 8-6. Network interconnectivity.

8-9. TRTS Integration Across the Battlefield

A major step towards interoperable automated systems is the fielding of the ATCCS. This system is made up of common hardware and software components that allow users to rapidly exchange relevant C^{2}information across the battlefield between standardized CPs. ATCCS is composed of five battlefield functional area control systems designed for specific functional areas:

- MCS.

- Advanced Field Artillery Tactical Data System (AFATDS).

- All Source Analysis System (ASAS).

- Combat Service Support Control System (CSSCS).

- Forward Area Air Defense Command, Control, Communications, and Intelligence (FAADC^{3}I).

Figure 8-7 shows where each system will be deployed and interoperate/interconnect across the battlefield. ATCCS will be integrated into each users' CP where the system will network and interface with CNR, MSE, tactical switchboards, and commercial telephone lines. Total integration with ATCCS will allow multiple access to a single corporate battlefield information database where commanders will be able to select and retrieve the information needed for immediate or sound decision making.

Major functions of ATCCS software.

In the text edit/integrated business package and joint automated message processing modes, the user will be able to create, print, save, distribute, route, and edit messages, spreadsheets, and databases.

In the graphics mode, users will be able to have a map of the area of operations stored within computer memory. This map can be called up, edited or updated, and transmitted to other ATCCS stations. Also, the user may compose graphics displays to either transmit to other stations or provide briefing materials.

ATCCS facilitates information management as users can manipulate their databases to produce situation, battle resource, and summary reports for commanders and staff across the battlefield.

Procedures on how to set up, initialize, and maintain each system is being fielded as each system is fielded. (Currently only the MCS portion of ATCCS has been tested, fielded, and used in both training and real world wartime missions.) MCS is to be used at other battlefield functional areas until individual functional area BASS are fielded. Once each functional area has their portions of ATCCS fully fielded, a total integration across the battlefield will be achieved, as a total interaction of functional area C^2 will be realized.

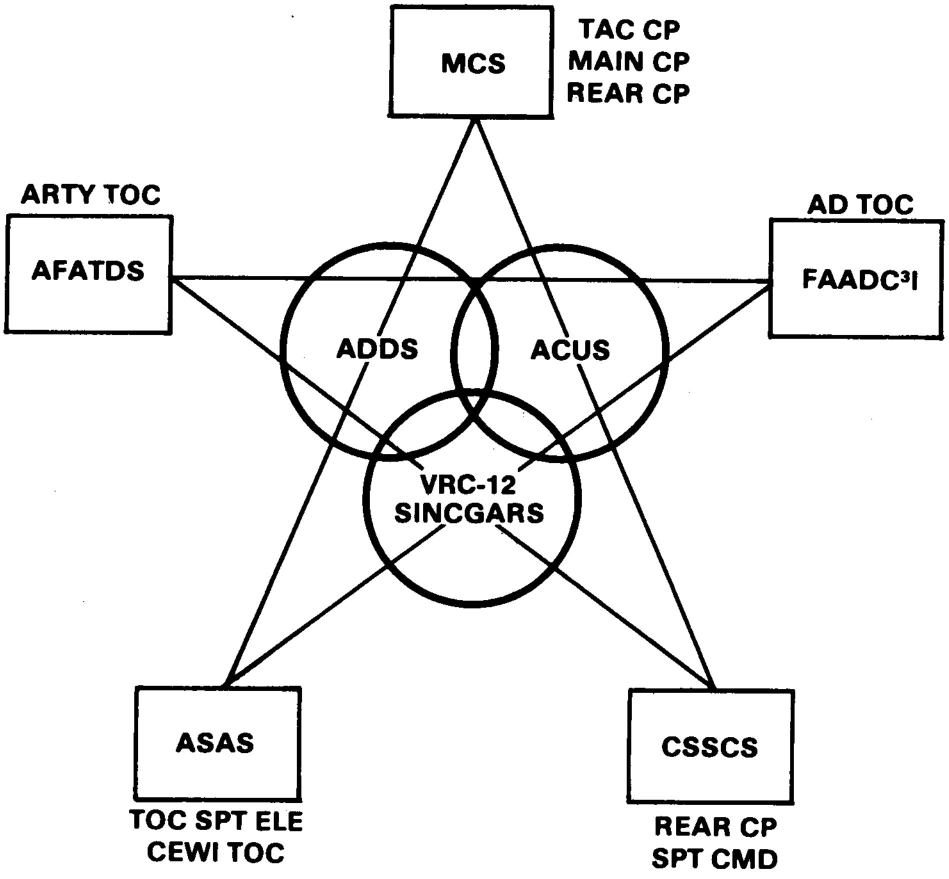


Figure 8-7. Battlefield functional area control systems.

Chapter 9

EAC Tactical TCC Fundamentals

9-1. Introduction

This chapter covers tactical TCC organization and operation and communications means relating to the EAC environment.

The Signal Corps-operated over-the-counter TCCs are scheduled to be phased out as MSE, EAC-Communications Improvement Plan (CIP), BAS, and TRTS communications systems are fielded. Phase out will be ongoing into the mid-to-late 1990s or until the slower, less efficient tactical TCCs are replaced with user-owned, -operated, and -maintained terminal equipment. Tactical TCCs will remain in operation until units have received their authorized user-owned and -operated PCs and digital facsimile equipment. Until AirLand Operations become more automated and the TRTS network is fully fielded, the tactical TCCs will continue to provide over-the-counter record traffic support.

Until tactical TCCs are replaced at EAC and theater Army locations, procedures in this chapter will be in effect for those remaining TCCs. Procedures in this chapter augment the procedures for message processing found in--

- FM 11-490-2.
- JANAP 128( ).
- DOI 103.

9-2. Organization

The table(s) of organization and equipment (TOE) of the signal battalion or signal brigade determine the mission of the unit, the number of people, and the types of equipment. Each TCC will have a flexible mission as determined by the organization's AirLand Operations mission. Regardless of what mission the unit may have, a typical TCC will have a message section, a transmit-receive (means) section, and a messenger section. In larger TCCs, sections may be physically separated; in a smaller TCC, the sections may be collocated in one area. Paragraph 9-5 provides additional information on each of the three TCC sections.

9-3. Operational Objectives

The principal objectives in TCC operation are accuracy, speed, security, and reliability in the accomplishment of the mission. An effective training plan, to include cross- training of all platoon personnel, will greatly enhance the TCCs in meeting required objectives. Continuous and realistic training of TCC personnel will improve the overall level of proficiency within the communications platoon. TCC training must reinforce and emphasize- -

- Accuracy in message processing of transmitted and received messages.

- Speed of service in processing messages.

- Security practices to include proper use of COMSEC (physical, cryptographic, and transmission emission security).

- Reliability of service through operator preventive maintenance and scheduled maintenance programs.

9-4. Communications Means

A tactical TCC may have one or more of the following means to communicate narrative, data, voice, or facsimile messages:

- Teletypewriter (TTY) facilities use wire, radio, or a combination as a transmission means. TTY equipment is secured by on-line cryptographic equipment as determined by the TOE. The AN/UGC-74 is a TTY used to compose, edit, store, transmit, receive, and print messages. It is designed to interface/operate with the older TTY sets that use standard keyboards or transmitters- distributors for preparing and transmitting prepunched paper tape messages.

- Radio teletypewriter (RATT) is a means of transmitting information by keyboard or perforated tape over high frequency (HF) radio circuits. International Morse Code may also be transmitted by HF RATT equipment. RATT is primarily in operation at EAC for backup communications for C^2 and to interface with allied forces. RATT is used in some applications for access to operations/intelligence and administrative/logistics networks. RATT has a very high electronic signature and is used more and more as a backup system. Some division GP RATT nets are being used until MSE is fielded.

- Telephones (secure and nonsecure instruments) vary from the sound-powered TA-1/TP to the full-duplex voice/DSVT KY-68. Tactical telephones are designed primarily as a common user system.

- Messenger service is grouped in categories according to the way the messenger travels--foot, motor, and air messengers. Messengers provide a secure means of delivering large bulky items, but messengers are relatively slow and are limited by the transportation means available.

- Modern tactical facsimile now operates over existing standard voice radios and wire circuits. Newer equipment is lightweight, rugged, portable, and low power. The systems are capable of operating from standard and vehicular power. Facsimile enables electronic transmission/reception of typed or handwritten record traffic, maps, overlays, drawings, photographs, and other types of documents containing black and white, color, or gray shades.

No matter what means the TCC uses to transmit or receive communications, overall objectives remain the same--accuracy, speed, security, message privacy, and reliability.

9-5. Organization and Operation

Telecommunications functions and operating procedures are contained in Chapter 10 of FM 11-490-2. Each tactical TCC publishes local procedures to meet local message processing requirements. All functions prescribed in FM 11-490-2 must be performed by the tactical TCC to support the TCC mission. However, all positions described in Chapter 10 may not be required by a tactical TCC.

Each TCC has the following three sections assigned:

Message center section.

The message center section processes all message traffic handled by the TCC; selects how the message is to be transmitted (TTY, facsimile, voice, or messenger); maintains TCC files, maps (for messenger routes), communications status logs, and official headquarters time.

Outgoing messages originated in the headquarters or incoming messages addressed to the headquarters served are passed directly between the headquarters and the message center section.

The message center section is the administrative element of the TCC. Records are maintained to facilitate traffic delivery and to record the handling of each message. Staff reference files are not maintained in the message center section. The following functions are performed by one or more personnel assigned to the message center:

- Acceptance and delivery clerk.
- Reproduction clerk.
- Outgoing routing clerk.
- Collator and sorting clerk.
- Internal router.
- Traffic checker.

Means section.

The means section consists of the operating personnel and the terminal facilities for transmitting and receiving messages. The terminal facilities that may be employed are RATT, continuous wave (CW), TTY, and facsimile. The receivers and transmitters are usually remotely located and connected to the terminal equipment by wire or cable.

Message processing steps and procedures contained in Chapter 11, Sections II and III of FM 11-490-2 should be incorporated into the TCC SOP.

Service message procedures are contained in Chapter 15 of FM 11-490-2. Automatically generated service message procedures for TCCs connected to an AN/TYC-39( ) message switch are contained in Chapter 6 of this manual. Additional information concerning automatically generated service messages can be found in JANAP 128.

Facsimile procedures for processing and transmitting messages in common user and dedicated operations are found in Chapter 14 of FM 11-490-2.

RATT and radiotelegraph message procedures are found in applicable ACP 117 manuals. The following functions are performend by one or more personnel assigned to the means section:

- Keyboard operator.
- Proofreader.
- Transmit operator.
- File clerk.
- Receive operator.
- Service message clerk.

Messenger section.

The messenger section of the TCC consists of the messengers and equipment essential to an efficient and effective delivery service. Although this section is a part of the TCC, messenger service and supporting equipment are an unresourced mission for the Signal Corps. (See Chapter 10 for messenger service procedures.)

9-6. TCC and TRTS Message Transfer

Properly formatted and addressed message traffic is transmitted to a connected AN/TYC-39( ) for relay to the CT or vice versa. All messages to a TCC will be formal record traffic.

9-7. Outgoing and Incoming Message Flow

Figure 9-1 shows manual narrative originate (outgoing) message flow. Figure 9-2 shows manual narrative terminate (incoming) message flow. These charts represent how record traffic should move from one processing step to the final disposition. These charts are applicable for record traffic processed within a CT or TCC.

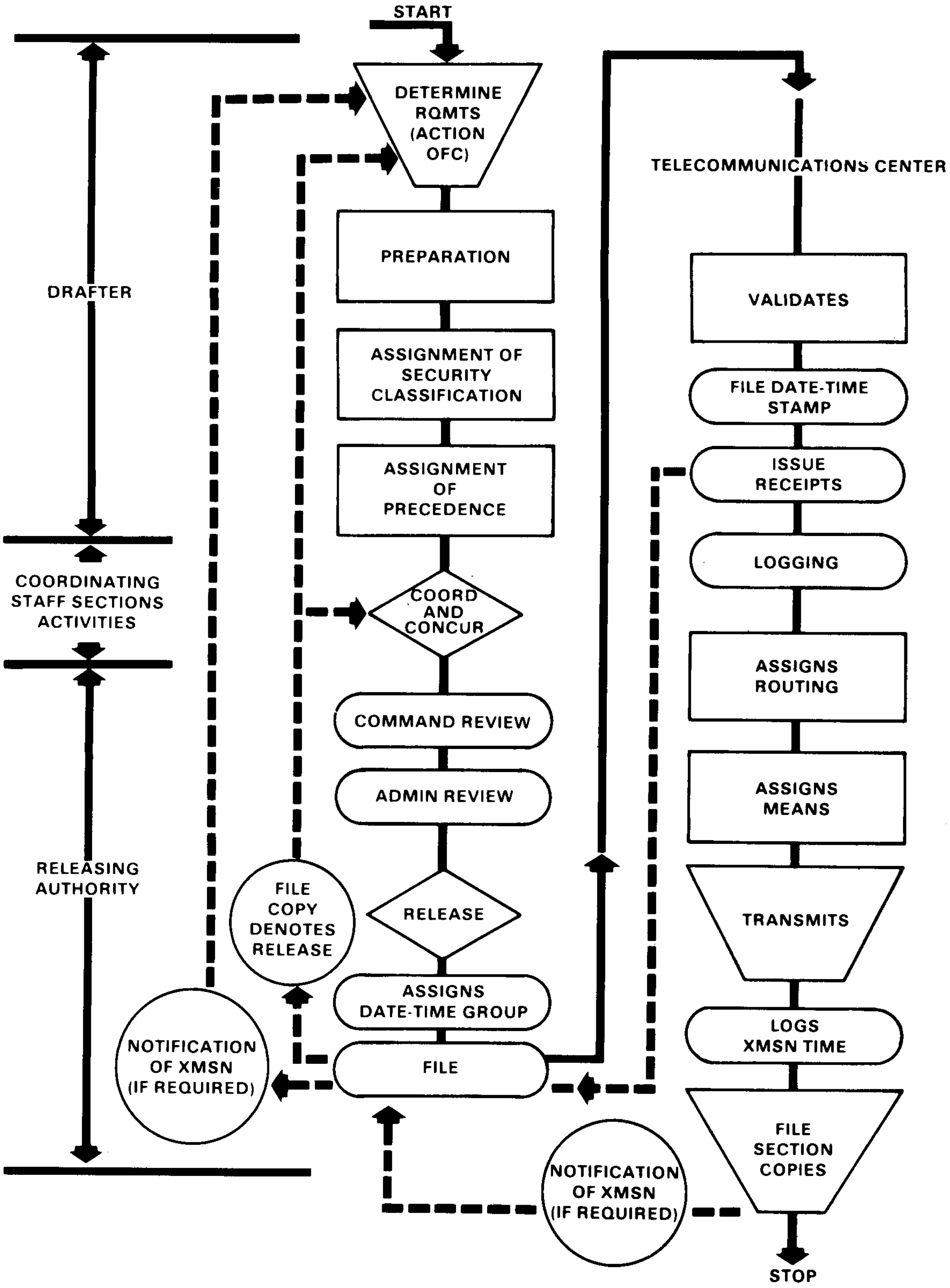


Figure 9-1. Outgoing message flow.

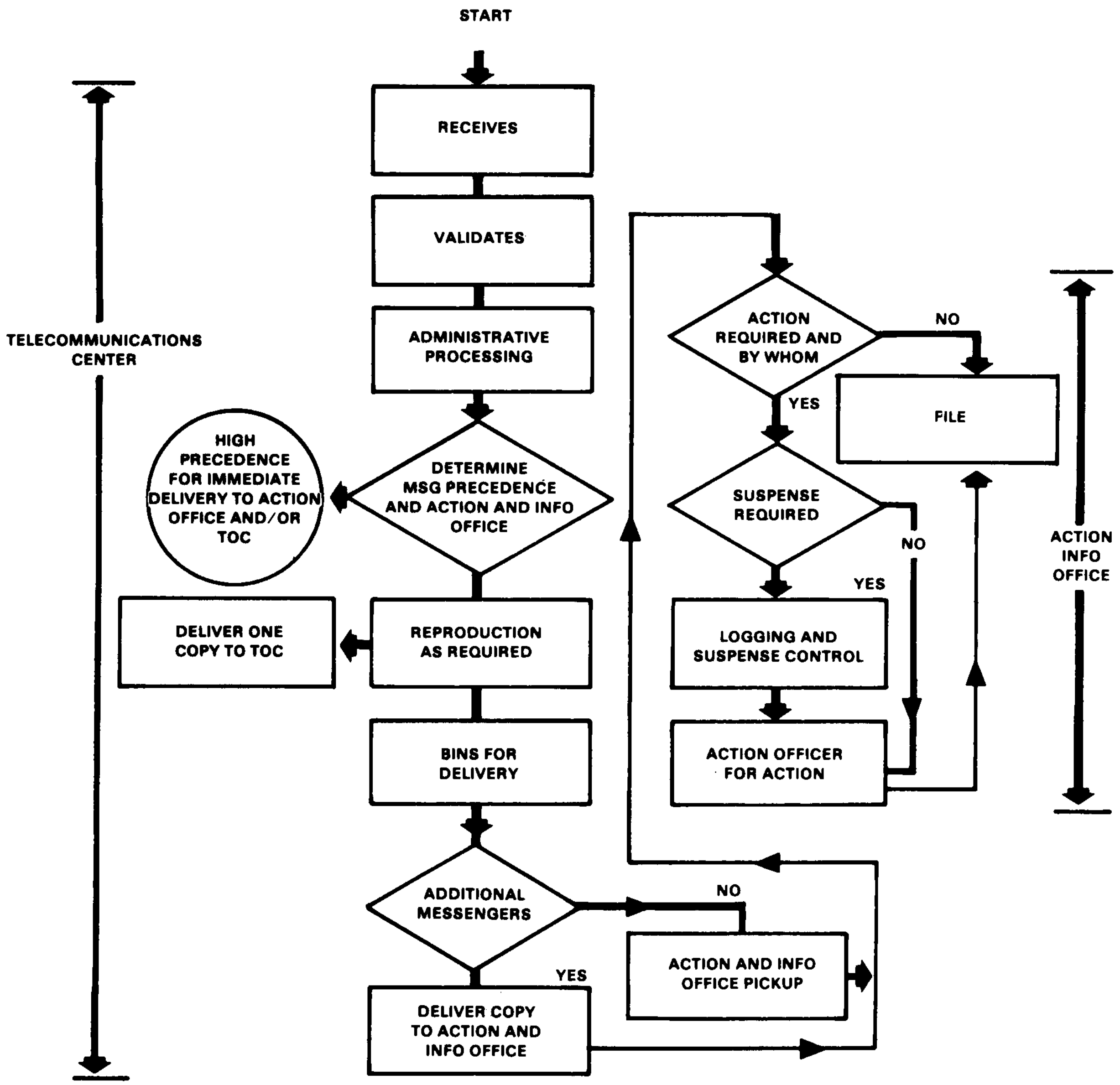

START
RECEIVES
VALIDATES
ADMINISTRATIVE PROCESSING
TELECOMMUNICATIONS CENTER
HIGH PRECEDENCE FOR IMMEDIATE DELIVERY TO ACTION OFFICE AND/OR TOC
DETERMINE MSG PRECEDENCE AND ACTION AND INFO OFFICE
DELIVER ONE COPY TO TOC
REPRODUCTION AS REQUIRED
BINS FOR DELIVERY
ADDITIONAL MESSENGERS
NO
YES
ACTION AND INFO OFFICE PICKUP
DELIVER COPY TO ACTION AND INFO OFFICE
ACTION REQUIRED AND BY WHOM
NO
FILE
YES
SUSPENSE REQUIRED
NO
YES
LOGGING AND SUSPENSE CONTROL
ACTION OFFICER FOR ACTION
ACTION INFO OFFICE

Figure 9-2. Incoming message flow.

Chapter 10

Messenger Service Fundamentals and Procedures

10-1. Introduction

This chapter provides information on messenger service. Features are listed, types are defined, ways of employment are given, transportation modes are identified, routing is recommended, and miscellaneous information is presented.

The supporting signal officer/ISSO is responsible for ensuring that messenger service is provided with necessary augmentation by the supported organization. Requirements for messenger service is coordinated by the ISSO/BSO with the G3/S3 who tasks unit assets to provide messenger service personnel/equipment. Due to the expected high number of CTs and LDFs to be in service across the tactical battlefield and associated heavy increase in record traffic, anyone can and may become a courier on the battlefield. Procedures are required to ensure messenger service/courier techniques are known and integrated, when and where necessary, into the TRTS.

For success in battle, uninterrupted availability of information paths for the effective performance of C^2 functions is mandatory. When other electrical means of passing record traffic are not available to the commander, messenger service becomes vital to the record traffic system. It is a secure means to--

- Deliver record traffic when electrical transmission means are inoperable because of jamming, interference, or equipment failures.

- Deliver bulky items such as large oversized maps.

10-2. Messenger Service

A main feature of messenger service is that all units have assets to provide on-demand messenger service when the unit needs the service. Other features of messenger service are--

- Reliability.
- Flexibility.
- Security. (It is the most secure means available to units.)

The main advantages of messenger service are that it can handle large volumes of information and can transport long messages and oversized items to other locations.

10-3. Types of Messenger Service

Scheduled messengers follow prearranged and published time schedules, travel designated routes, and stop at predesignated points and headquarters. They normally pick up and deliver pouches of record traffic as directed by the signal officer or G1/S1. If messenger service is required on a recurring basis, the supporting signal officer determines if a unit's location and requirements can be added as a scheduled messenger service requirement.

Special messengers do not operate on fixed schedules. They are used when scheduled service has not been established or to augment scheduled service. Special messengers are employed when the urgency of record traffic cannot wait for transmission by other means.

10-4. Messenger Employment

The effectiveness of messenger service depends on the proper employment of messengers to meet the requirements of each message or groups of messages. Classification of material being transported and any special considerations or precautions that must be taken must be explained to messengers. Note that the messenger must have the same security clearance as the highest classification of the material being transported. Figure 10-1 is a messenger service checklist to assist supervisors in messenger employment.

Classification of material to be couriered:

- Does messenger have the same level security clearance as material being couriered?
- Is classified material properly wrapped or secured from viewing?

Tactical situation:

- Will messenger encounter hostile forces and, if so, what actions need be taken to protect material being transported?

Availability of transportation:

- What mode of transportation is required and has it been coordinated and available?
- Is an assistant messenger/driver required?
- Are maps of the route available, marked, and familiar to the messenger?
- If relay posts are being used, .does the messenger know of their location?

Urgency of messenger service:

- How rapid must the material be delivered? Is the messenger aware of delivery time constraints?
- Does the mode of transportation meet delivery time requirement needs?

Weapons required to arm messenger:

- Is the messenger/assistant messenger armed with weapons and sufficient ammunition?
- Is the messenger familiar with the provisions of deadly force?

Emergency actions required or to be taken:

- In the event of hostile actions, should material be hidden or destroyed?
- If material is to be destroyed, are destruction methods known/available to the messenger?

Name and telephone number of primary and alternate point of contact at delivery destination.

Instructions for actions to take in the event the messenger is unable to deliver the material.

Figure 10-1. Messenger service checklist.

The type of messenger employed is determined by the urgency of the message, size of the message, terrain to be covered, weather conditions (current and future), and availability of transportation. Messengers are classified as foot, motor, or air messengers.

Foot messengers are ordinarily used for short distances when the terrain is impassable for vehicles. When foot messengers are used to carry messages over long distances, a message relay system is employed. Small tactical units depend on foot messengers for command post distribution and interplatoon communications.

Motor messengers are used between headquarters or echelons when the distance and the bulk of traffic warrants them. If the tactical situation or traffic load requires it, the supporting signal officer may establish daily scheduled motor messenger service.

Scheduled and special air messenger services are used for the delivery of record traffic over relatively long distances or where terrain features prohibit the use of motor or foot messengers. Air messenger service is used frequently during tactical operations. Fixed and rotary wing aircraft may be used and the pilot, observer, or passenger may be employed as the air messenger. Personnel traveling between CPs are excellent resources for transporting distribution. Unit SOPs should identify procedures personnel will follow to pick up distribution prior to travel.

Messengers will be armed, normally with their assigned weapons, and usually accompanied by an armed assistant. Messenger and assistant should be issued compasses and maps.

Messengers will be briefed on the tactical situation and any special considerations prior to departure.

Messengers will not leave the couriered material unattended at any time. They will maintain personal custody of the material until it is properly delivered to an authorized individual at the messenger destination.

Prior to departure, the messenger will be advised of actions to take in the event of an emergency situation such as hostile action or adverse weather conditions. See paragraph 10-8 for double messenger procedures.

10-5. Messenger Transportation and Equipment

Vehicles and personnel used for motor messengers will be tasked by subordinate commands and supervised by unit signal officers. (Tactical situations may dictate that the CT/LDF user provide the vehicle and messenger/driver.) Official messenger signs will be displayed on vehicles while they are engaged in official messenger activities.

Aircraft use is coordinated by the supporting signal officer and the organization's aviation section. Aircraft will normally be furnished as the need arises and as the tactical situation permits. The signal officer must be aware of and plan around supported unit aviation assets and mission.

10-6. Messenger Routes

The selection and reconnaissance of messenger routes should be accomplished by experienced officers or noncommissioned officers. Maps, sketches, and verbal instructions are used to indicate what routes the messengers should follow in delivering record traffic. Messengers should be experienced in land navigation and trained to use other expedients in following their route. Messengers should be skilled in--

- Using night vision goggles at night in difficult terrain.

- Using assistance and following directions from the military police.

- Following field wire lines in rear areas.

- Knowing how to read/identify wire tagging methods to identify wire lines leading to their destination.

The following factors should influence the supervisor/planner when selecting messenger routes:

- Type of messenger to be used.

- Cover and concealment of the area that would provide protection from hostile action and observation.

- Availability of the route under existing weather and traffic conditions.

- Length and condition of the route.
- Tactical situation of the area.
- Items to be transported.

10-7. Messenger Posts

Messenger relay posts are established to minimize interruptions caused by vehicle failure, messenger fatigue, and messenger casualties. The number of relay posts required along the route and the provision of personnel for these installations are determined by the signal officer or ISSO.

10-8. Double Messengers

Double messengers are used when the record traffic items to be delivered are of vital importance to C^2 or when the route to be traveled exposes a messenger to hostile fire. Although traveling within contact distance of each other, messengers should maintain a sufficient interval to protect them from simultaneous exposure to enemy fire or ambush.

Each messenger carries a copy of the message to be delivered. When practical, one of the messengers may be sent by an alternate route. Each messenger should be briefed on what methods to take to avoid hostile contact and to prevent record traffic from being lost, delayed, or compromised.

Chapter 11

Basic Emergency Procedures

11-1. Introduction

This chapter sets forth the procedures for preparing, practicing, and executing emergency plans. CT, LDF, and TCC supervisors will ensure that these procedures are considered when drafting and implementing their local emergency plans or when updating current emergency plans upon receipt of TRTS equipment.

Basic emergency plans (BEPs) are a command responsibility. The organization SOP must include emergency plans that provide for--

- Emergency destruction of classified material and equipment.
- Emergency evacuation of classified material and equipment.
- Precautionary destruction of classified material and equipment.

11-2. Purpose

The overall purpose of having a BEP is to prevent loss or capture of classified material or sensitive equipment during hostile action. The following factors influence the decision to conduct either destruction, evacuation, or precautionary destruction of material.

- Level and sensitivity of classified material held by the organization.
- Proximity of hostile forces and their intent towards aggressive actions.

11-3. BEP Provisions

The following provisions will be incorporated into the organization emergency plans.

- Assignment of specific responsibilities by duty rather than by name with alternates designated. This is important in multilevel access CTs and TCCs where several people may be on duty when the emergency or hostile action occurs.
- Authorization for the senior member present to implement the emergency plan.
- Removal of classified record traffic files.
- Location of security container combinations.
- Instructions for purging CTs and actions to take in formatting extra ASCs and floppy disks as well as disposition of controlled cryptographic items (CCI).
- Instructions for thermate and thermite incendiaries for destruction of terminals, equipment, and classified holdings.

The initial step in BEP is the reduction of the amount of classified material held. The CT and TCC should not have command reading files or be a storage area for excessive holdings of classified record traffic.

The following information should be incorporated into the BEP.

Evacuation instructions. Evacuation consists of removal of material to a safe/secure location. Removal is conducted in a systematic manner based on the following factors:

- Time available.
- Future requirements for the equipment and material.
- Degree of hazard involved in the evacuation.
- Security at new location.
- Means of transportation available.

- Evacuation routes (primary and alternate) available.

Priority of destruction instructions. The priority for emergency destruction is TOP SECRET first, SECRET second, followed by CONFIDENTIAL, and then unclassified record traffic. (If time permits, all unclassified record traffic will be destroyed.) Whenever hostile action is imminent, it is highly desirable to take prompt action to reduce classified holdings to the minimum amount necessary to continue operations. Reduction of holding should be IAW--

- AR 380-5 for destruction of classified defense information.

- TB 380-41-3 and AR 380-40 for destruction of cryptographic keying material.

- TB 380-40-22 for the destruction of CCI.

- TM 750-244-2 for the destruction of TOE equipment.

11-4. BEP Coordination

Emergency plans involving TRTS and TCC classified record traffic, as well as sensitive equipment, must be coordinated with or incorporated into command emergency plans to ensure the plans may be effectively and securely accomplished if hostile action occurs. As a minimum, the G2/S2 and supporting signal officer should be coordinating addressees on BEPs.

11-5. Action Subsequent to BEP Implementation

Higher headquarters should be notified by immediate message of all actions taken under the organization’s emergency plan. Information in the formal record traffic report will include--

- Material lost or destroyed.

- Method and degree to which material was destroyed.

- Circumstances which caused BEP to be implemented.

Reports of incidents that result in an insecurity or compromise of classified material will be submitted IAW AR 380-5.

11-6. BEP Proficiency

Supervisors will ensure all assigned personnel are aware of actions to take if hostile action or emergency situations occur which endangers classified/sensitive material or equipment. Personnel must be aware that the CT is classified (normally TOP SECRET) unless purged and that loss of a CT or associated record traffic could cause serious damage to the national security of the United States.

Training should be accomplished by conducting dry runs of procedures and required actions to take in case of an emergency. Realistic training and supervision of actions taken during training will result in classified material and equipment being better safeguarded during hostile actions.

CT and TCC personnel should know not only what actions to take if hostile action occurs but also what actions are required to protect equipment and material in the event of fires in or around their equipment.

Appendix A

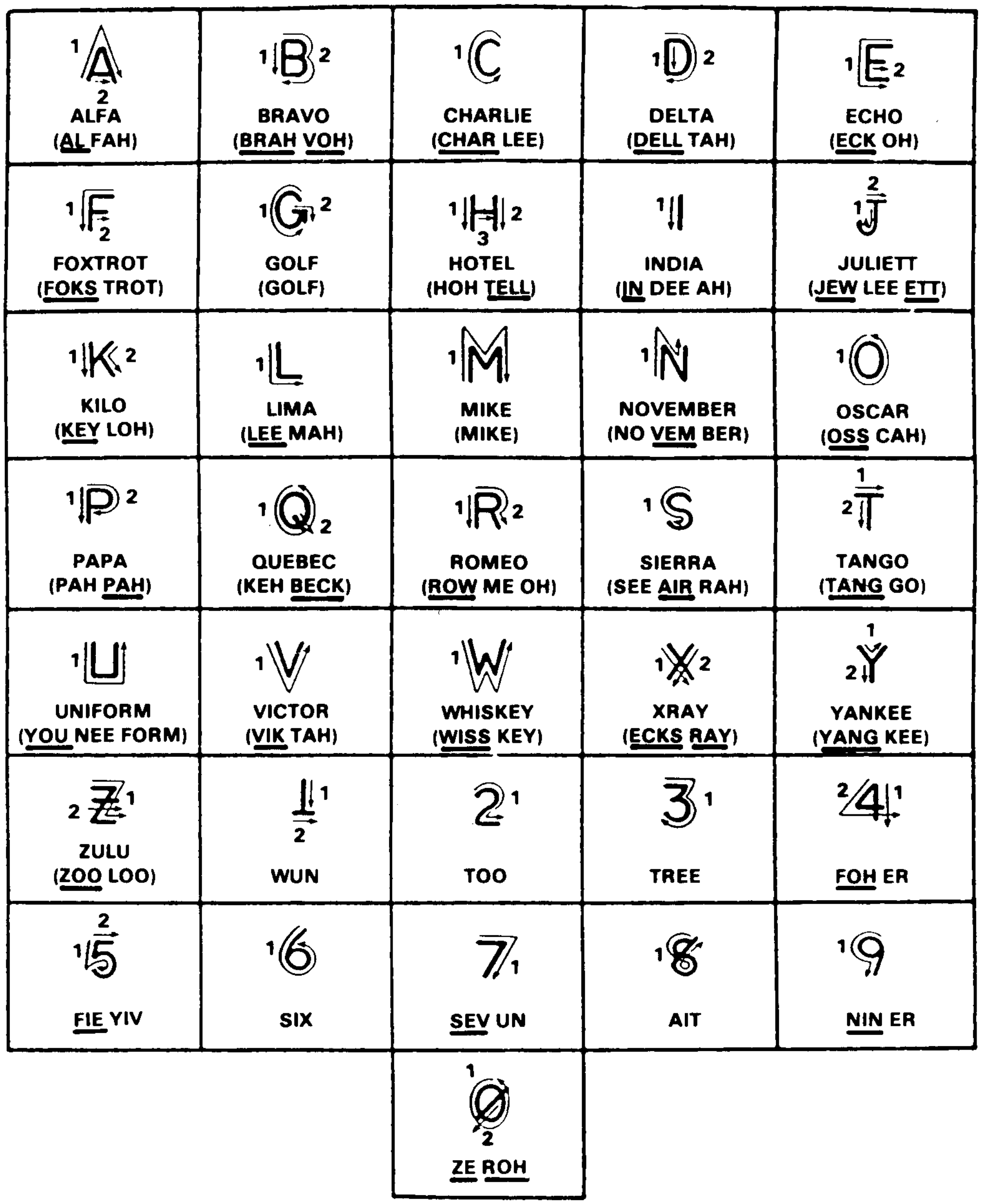
Military Lettering and Phonetic Alphabet

A-1. Military Lettering

Legibility is important in making handprinted entries in logs, registers, and number sheets. Entries should be typed or legibly handprinted. Most letters are formed with a straight line as the foundation stroke. Other letters require a round or circular line as the foundation stroke. The letter Z has a line through the center to distinguish it from the number 2. Numerals must be distinct. They are made with either a straight or circular stroke. The numeral 1 always has a line under it to distinguish it from the letter I. A zero has a line diagonally through it to distinguish it from the letter O.

A-2. Phonetic Alphabet

Certain letters of the alphabet have similar sounds and often are confused in telephone conversations. Figure A-1 shows the word to be used in voice communications to represent letters of the alphabet and numbers.



ALFA (AL FAH)	BRAVO (BRAH VOH)	CHARLIE (CHAR LEE)	DELTA (DELL TAH)	ECHO (ECK OH)
FOXTROT (FOKS TROT)	GOLF (GOLF)	HOTEL (HOH TELL)	INDIA (IN DEE AH)	JULIETT (JEW LEE ETT)
KILO (KEY LOH)	LIMA (LEE MAH)	MIKE (MIKE)	NOVEMBER (NO VEM BER)	OSCAR (OSS CAH)
PAPA (PAH PAH)	QUEBEC (KEH BECK)	ROMEO (ROW ME OH)	SIERRA (SEE AIR RAH)	TANGO (TANG GO)
UNIFORM (YOU NEE FORM)	VICTOR (VIK TAH)	WHISKEY (WISS KEY)	XRAY (ECKS RAY)	YANKEE (YANG KEE)
ZULU (ZOO LOO)	WUN	TOO	TREE	FOH ER
FIE YIV	SIX	SEV UN	AIT	NIN ER
		ZE ROH		

NOTE: The underlined portion of the alphabet denotes accent syllables.

Figure A-1. Phonetic alphabet.

Appendix B

World Time Zones and Time Conversion Table

B-1. Date and Time

In messages, these are expressed as six digits followed by the ZULU (Z) zone suffix. The first pair of digits denotes the date, the second pair the hour (24-hour clock), the third pair the minutes past the hour. Example of a DTG is 201132Z.

B-2. Greenwich Mean Time (GMT)

This time is accepted as the basis for measuring time throughout the world. Time groups expressing GMT are designated by the letter suffix Z immediately following the last digit of the group. Any other suffix used after a 4-digit DTG (corresponding to the Z of GMT) indicates the zone in which the local civil time is expressed. It does not designate location on the earth's surface. The proper suffix can be determined from the time zone map and the time conversion table. (See Figures B-1 and B-2.)

B-3. Difference in Time

Numerals in the zone indicate the number of hours that local time differs from GMT. Time zones extend east and west from Greenwich to the 180th meridian. If a given zone lies east of the prime meridian, the appropriate number is added to convert it to local time. In converting local time to GMT, the appropriate number is subtracted. For zones west of the prime meridian, the process is reversed. Deviation in time shown on the time zone map will occur because of local policies or conditions.

B-4. Conversion of Time

The time conversion table converts time in one zone to time in any other zone. Vertical columns indicate time zones. Zone Z is GMT. Time in each successive zone to the right of zone Z is 1 hour later, to the left of zone Z is 1 hour earlier. Time in each successive shaded area to the right is 1 day (24 hours) later, to the left is 1 day (24 hours) earlier. To determine the time in zone Z when it is 0500 hours in zone 1, proceed as follows: Find 0500 in column I and locate figure 2000 in the corresponding line in column Z. Since 2000 is not in a shaded area, the time is 2000 hours yesterday. (See Figure B-2.)

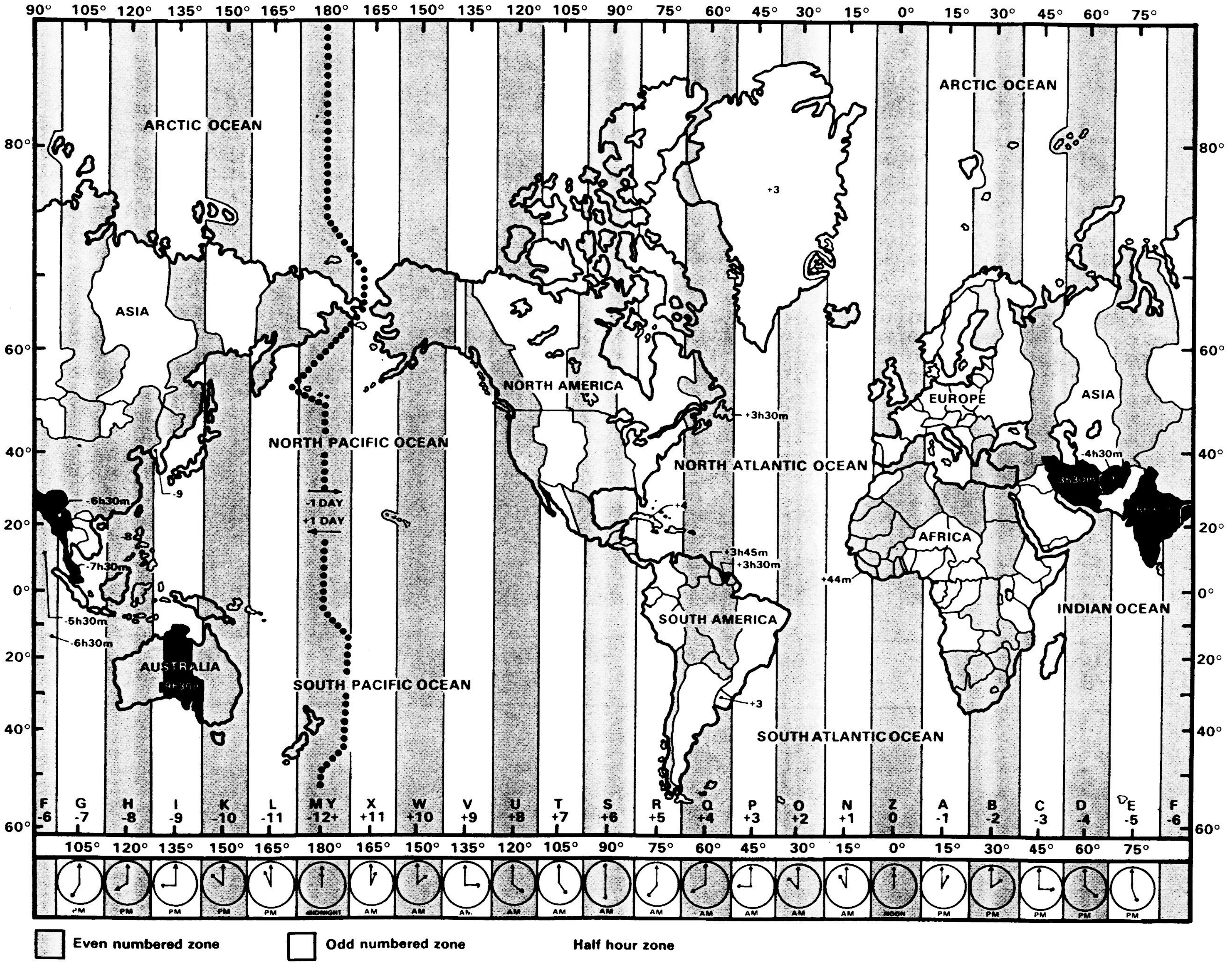


Figure B-1. Standard time zones of the world.

	Y	X	W	V	U	T	S	R	Q	P	O	N	Z	A	B	C	D	E	F	G	H	I	K	L	M	
	+12	+11	+10	+9	+8	+7	+6	**+5**	+4	+3	+2	+1	**0**	-1	-2	-3	-4	**-5**	-6	-7	**-8**	**-9**	-10	-11	-12	
PREVIOUS DAY	1800	1900	2000	2100	2200	2300	2400	0100	0200	0300	0400	0500	0600	0700	0800	0900	1000	1100	1200	1300	1400	1500	1600	1700	1800	SAME DAY
	1900	2000	2100	2200	2300	2400	0100	0200	0300	0400	0500	0600	0700	0800	0900	1000	1100	1200	1300	1400	1500	1600	1700	1800	1900	
	2000	2100	2200	2300	2400	0100	0200	0300	0400	0500	0600	0700	0800	0900	1000	1100	1200	1300	1400	1500	1600	1700	1800	1900	2000	
	2100	2200	2300	2400	0100	0200	0300	0400	0500	0600	0700	0800	0900	1000	1100	1200	1300	1400	1500	1600	1700	1800	1900	2000	2100	
	2200	2300	2400	0100	0200	0300	0400	0500	0600	0700	0800	0900	1000	1100	1200	1300	1400	1500	1600	1700	1800	1900	2000	2100	2200	
	2300	2400	0100	0200	0300	0400	0500	0600	0700	0800	0900	1000	1100	1200	1300	1400	1500	1600	1700	1800	1900	2000	2100	2200	2300	
	2400	0100	0200	0300	0400	0500	0600	0700	0800	0900	1000	1100	1200	1300	1400	1500	1600	1700	1800	1900	2000	2100	2200	2300	2400	
SAME DAY	0100	0200	0300	0400	0500	0600	0700	0800	0900	1000	1100	1200	1300	1400	1500	1600	1700	1800	1900	2000	2100	2200	2300	2400	0100	NEXT DAY
	0200	0300	0400	0500	0600	0700	0800	0900	1000	1100	1200	1300	1400	1500	1600	1700	1800	1900	2000	2100	2200	2300	2400	0100	0200	
	0300	0400	0500	0600	0700	0800	0900	1000	1100	1200	1300	1400	1500	1600	1700	1800	1900	2000	2100	2200	2300	2400	0100	0200	0300	
	0400	0500	0600	0700	0800	0900	1000	1100	1200	1300	1400	1500	1600	1700	1800	1900	2000	2100	2200	2300	2400	0100	0200	0300	0400	
	0500	0600	0700	0800	0900	1000	1100	1200	1300	1400	1500	1600	1700	1800	1900	2000	2100	2200	2300	2400	0100	0200	0300	0400	0500	
	0600	0700	0800	0900	1000	1100	1200	1300	1400	1500	1600	1700	1800	1900	2000	2100	2200	2300	2400	0100	0200	0300	0400	0500	0600	
	0700	0800	0900	1000	1100	1200	1300	1400	1500	1600	1700	1800	1900	2000	2100	2200	2300	2400	0100	0200	0300	0400	0500	0600	0700	
	0800	0900	1000	1100	1200	1300	1400	1500	1600	1700	1800	1900	2000	2100	2200	2300	2400	0100	0200	0300	0400	0500	0600	0700	0800	
	0900	1000	1100	1200	1300	1400	1500	1600	1700	1800	1900	2000	2100	2200	2300	2400	0100	0200	0300	0400	0500	0600	0700	0800	0900	
	1000	1100	1200	1300	1400	1500	1600	1700	1800	1900	2000	2100	2200	2300	2400	0100	0200	0300	0400	0500	0600	0700	0800	0900	1000	
	1100	1200	1300	1400	1500	1600	1700	1800	1900	2000	2100	2200	2300	2400	0100	0200	0300	0400	0500	0600	0700	0800	0900	1000	1100	
	1200	1300	1400	1500	1600	1700	1800	1900	2000	2100	2200	2300	2400	0100	0200	0300	0400	0500	0600	0700	0800	0900	1000	1100	1200	
	1300	1400	1500	1600	1700	1800	1900	2000	2100	2200	2300	2400	0100	0200	0300	0400	0500	0600	0700	0800	0900	1000	1100	1200	1300	
	1400	1500	1600	1700	1800	1900	2000	2100	2200	2300	2400	0100	0200	0300	0400	0500	0600	0700	0800	0900	1000	1100	1200	1300	1400	
	1500	1600	1700	1800	1900	2000	2100	2200	2300	2400	0100	0200	0300	0400	0500	0600	0700	0800	0900	1000	1100	1200	1300	1400	1500	
	1600	1700	1800	1900	2000	2100	2200	2300	2400	0100	0200	0300	0400	0500	0600	0700	0800	0900	1000	1100	1200	1300	1400	1500	1600	
	1700	1800	1900	2000	2100	2200	2300	2400	0100	0200	0300	0400	0500	0600	0700	0800	0900	1000	1100	1200	1300	1400	1500	1600	1700	

Figure B-2. Time conversion table.

Appendix C

Precedence Assignment Guide

C-1. Precedence Categories

There are six precedence categories within the two record traffic communities (GENSER and DSSCS). The precedences and examples are shown in Table C-1.

C-2. Precedence Abuse

Messages of like precedence are handled on a first in, first out basis. All immediate messages received at the AN/TYC-39() message switch will be received, stored, and relayed in the order received. It has been common practice in the past for message originators to OVER PRECEDENCE their messages thinking the message will get to an addressee faster. What happens is too many messages of the same precedence will actually delay message delivery because the switch is saturated with an over abundance of high precedence record traffic. Message originators are encouraged to assign a precedence which accurately reflects the speed of delivery and speed of action required or requested of the message addressee.

Table C-1. GENSER and DSSCS precedences.

Precedence Designation and Prosign	Example of Use	Order of Handling
CRITIC (W)	Critical intelligence community messages. DSSCS use only.	Ahead of all other messages.
EMERGENCY COMMAND PRECEDENCE (Y)	Certain designated emergency action C^2 messages. Originated by the NCA. Used in GENSER only.	Ahead of all (P) priority and routine messages. Requires immediate action and delivery

Table C-1. GENSER and DSSCS precedences (continued).

Precedence Designation and Prosign	Example of Use	Order of Handling
FLASH (Z)	Initial hostile contact or operational messages of extreme importance. GENSER and DSSCS.	Ahead of all other messages except CRITIC and ECP.
IMMEDIATE (O)	Operational orders affecting current operations. May be assigned to admin messages having a direct impact on the tactical situation. GENSER and DSSCS.	Ahead of all (P) priority and routine messages. Requires immediate action and delivery
PRIORITY (P)	For all messages requiring expeditious action by the addressees. Used to give essential information for the conduct of operations in progress. GENSER and DSSCS.	Ahead of routine messages.
ROUTINE (R)	Messages not of sufficient urgency to justify a higher precedence, but which must be delivered without delay. Used in GENSER and DSSCS.	After all messages of higher precedence.

C-3. Precedence Assignment

CT and TCC personnel should be aware that overall responsibility of assigning a precedence to record traffic is the message originator. No record traffic message will be delayed due to questions regarding the validity of a message precedence. All messages are processed IAW the precedence assigned to the message, based on the first in, first out, by precedence guidelines.

Appendix D

Use of Passwords with CT

D-1. CT Passwords

The CT uses passwords to limit access to different setups, functions, and levels of classified material processed and stored by the CT. Password control allows the CT owner to permit certain individuals access to different levels of classified material and to make changes to the operating parameters without giving all operators access to TOP SECRET material.

There are nine passwords used in the CT. These passwords control access to such functions as changing the GUARDED menu, enabling different classification levels for the terminal, changing the PLA/RI table, setting different passwords for the classification level of the operators, transmitting messages, and entering the Disk Operating System (DOS).

Passwords are critical to the CT security. Persons having passwords must be instructed on password sensitivity, protection, and personal responsibility for their security. For security reasons, passwords will be treated as more valuable than safe combinations.

Functions which require one or more passwords to access them are listed below.

DOS. The password to access DOS should be limited to a minimum number of personnel as it is not required for routine message processing.

GUARDED. The password to access this function must be strictly controlled and issued to a minimum number of personnel. The GUARDED menu is where initialization items are entered or changed and where the PLA/RI table is updated (additional password is required for this function).

ENABLE. The password to access the ENABLE function will be strictly controlled and issued only to those personnel requiring specific access. All personnel who are authorized to compose messages for a given level of classification will have the same password for this function. A different password is used for each level of access with a user having automatic access to all classifications at or lower than what they are authorized. Access to SECRET means the user can access SECRET and CONFIDENTIAL but not TOP SECRET.

PLA/RI. The password to access this function will be controlled by the security manager. The PLA/RI password is used to add, delete, and make changes to the PLA/RI table.

SET PASS. The password to access this function is limited to CT personnel with a TOP SECRET clearance and a need to know. This password allows the CT manager to change any of the current passwords prior to changing to new passwords.

D-2. CT Password Control

The security manager or ISS0 is responsible for the generation, issuance, and control of all system passwords, CT passwords require the following procedures to be in effect:

- Randomly generated (never common words or phrases).
- Classify at the highest level as the granted access.
- Require strict receipt procedures.
- Change at least semiannually or upon departure of an individual having knowledge of a password.

Password generation and control is outlined in paragraph 2-15 of AR 380-19.

The CT manager, using stringent password control, will be able to limit access to the different CT functions. Restricted access will reduce the possibility of unauthorized parameter alterations, and compromise of information, while still allowing multiple users to process outgoing and incoming record traffic efficiently.

Appendix E

Commonly Used Operating Z Signals

Operating Z signals are three-letter signals starting with the letter Z and used to expedite communications. They are also used to convey frequently used requests and information relating to communications. When preceded by the prosign INT, Z signals form a request or ask a question. EXAMPLE: INT ZDK -- Request retransmission. When Z signals are used alone, they convey an order or make a positive statement. Table E-1 lists commonly used operating Z signals. (See ACP 131 for a more thorough listing and definitions of Z signals.)

Table E-1. Commonly used Z signals.

Z SIGNAL	MEANING
ZDK	Following repetition of ___ is made IAW your request.
ZUE	Affirmative (yes).
ZUG	Negative (no).
ZUJ	Standby.
ZAR	This is my ___ request (first, second, and third).
ZDF	Message was received at (time expressed in ZULU).
ZEL	This is a correction to message ___.
ZEQ	Message missent to this station/ terminal-- -3 and relayed to ___ at ___ Z. -4 Unable to determine correct RI. -6 Delayed by misrouting at this station/terminal.
ZES	Message received. -1 Incomplete (portion missing). -2 Garbled (portion unreadable).

Table E-1. Commonly used Z signals (continued).

Z SIGNAL	MEANING
ZFD	Suspected duplicate of a previously transmitted message.
ZFG	Exact duplicate of a previously transmitted message.
ZFR	Cancel message ______.
ZOB	I will take no further action on this message.
ZOV	The correct RI for the message you sent is ______.
ZFH	This message is being passed to you by-- -1 for Action. -2 for Information. -3 for Comment.
ZKJ-2	I am closing down (until....).
ZUI	Your attention is invited to ____.
ZFF	Inform me when this message has been received by-- -1 Action addressee. -2 Information addressee. -3 All addressees. -4 Action addressee's TCC or CT/LDF.

Appendix F

Example of Operations Order for CT

This appendix provides examples of work sheets used with operation orders (OPORDs) for the CT.

Table F-1 contains columns for the 45 initialization table items the user must enter to initialize the CT. This work sheet should be used when preparing an OPORD deploying the CT.

Table F-1. CT initialization table entry work sheet.

INITIALIZATION ITEM	ENTRY BY USER/CT OPERATOR
1. CURRENT DAY	____________________
2. CURRENT MONTH	____________________
3. CURRENT YEAR	____________________
4. LOCAL TIME	____________________
5. ZULU TIME	____________________
6. ACCESS LEVEL OF USER	____________________
7. TERMINAL COMMUNITY	____________________
8. CONTENT/COMM INDICATOR	____________________
9. ORIGINATOR/DESTINATION LANGUAGE MEDIA FORMAT (LMF)	____________________
10. TERMINAL RI	____________________
11. TERMINAL PLA	____________________
12. TERMINAL CLASSIFICATION	____________________
13. TERMINAL PHONE NUMBER	____________________
14. CHANNEL ID	____________________
15. EOL SEQUENCE	____________________
16. XMIT START ENVELOPE	____________________

Table F-1. CT initilization table entry work sheet (continued).

INITIALIZATION ITEM	ENTRY BY USER/CT OPERATOR
17. XMIT STOP ENVELOPE (1-8)	
18. XMIT STOP ENVELOPE (9-16)	
19. RCV START ENVELOPE	
20. RCV STOP ENVELOPE (1-8)	
21. RCV STOP ENVELOPE (9-16)	
22. MASTER/SLAVE	
23. DACB PROTOCOL	
24. CHANNEL CONTROL	
25. MESSAGE CODE/PARITY	
26. LOOP RATE	
27. DATA RATE	
28. ERROR CONTROL	
29. SSI INTERFACE	
30. AUTO RESYNC	
31. CLOCK SOURCE	
32. EXT CLOCK SOURCE	
33. TRANSMIT SIGNAL SENSE	
34. RECEIVE SIGNAL SENSE	
35. SERIAL DATA CODE	
36. NUMBER OF STOP BITS	
37. DATA MODE CONTROLS	
38. MODE VI STORAGE BLOCKS	
39. MODE I ANSWER TIMER	
40. BAUD RATE	
41. STOP BITS	
42. PARITY	
43. AUTO-OPT	
44. PLA/RI PARAMETERS	

Table F-2 is the PLA/RI entry work sheet. This work sheet contains space for 20 entries. If more entries are needed, a second blank work sheet can be used. This work sheet is used during initialization and whenever a PLA/RI is updated.

Close coordination with the supporting signal officer is required to obtain correct initialization and PLA/RI table entries.

Table F-2. CT PLA/RI table entry work sheet.

ITEM	RI	PLA	CLASS	PHONE
1.	______	____________	______	______
2.	______	____________	______	______
3.	______	____________	______	______
4.	______	____________	______	______
5.	______	____________	______	______
6.	______	____________	______	______
7.	______	____________	______	______
8.	______	____________	______	______
9.	______	____________	______	______
10.	______	____________	______	______
11.	______	____________	______	______
12.	______	____________	______	______
13.	______	____________	______	______
14.	______	____________	______	______
15.	______	____________	______	______
16.	______	____________	______	______
17.	______	____________	______	______
18.	______	____________	______	______
19.	______	____________	______	______
20.	______	____________	______	______

NOTE: A password is required before making changes to the PLA/RI table.

PREPARED BY: ________
DATE: ________

Appendix G

Alarms and Indicators

When a significant action or an error occurs, the CT user is informed by an indicator appearing within the windows on the top three lines of the terminal or by an audible alarm. Table G-1 shows a listing of the AN/UGC-144 alarms and indicators, their causes, and additional information on causes or responses as appropriate. The common response for all alerts, and often the only response, is to press the ALARM RESET button.

Table G-1. AN/UGC-144 alarms and indicators.

INDICATOR	CAUSE	COMMENTS
FAULT	System malfunction is detected.	Run self test.
ALERT	Alert message requires attention.	Press ALT and NEXT ALERT to view; ALT and CLR ALERT twice to clear.
INFORMATION	Displays menu type and additional information of current operation.	No action required.
SSI-TX	Highlights when transmitting a message.	No action required.
SSI-RX	Highlights when receiving a message.	No action required.
OFF-HOOK/ON-HOOK WINDOW		
OFF-HOOK	Highlights when terminal is connected to communication line.	No action required.
ON-HOOK	Highlights when terminal is disconnected from a communication line.	No action required.

Table G-1. AN/UGC-144 alarms and indicators (continued).

INDICATOR	CAUSE	COMMENTS
GO-VOICE	Highlights when a "GO to Voice" signal is received.	Go to voice.
PHASE	Highlights when two terminals are in phase.	No action required.
PARITY	Highlights when a parity error occurs.	Check SSI setup.
SYN	Highlights when two terminals are synchronized.	No action required.
MSG RCV	Highlights when a message is received.	MSG RCV indicator flashes and audio alarm sounds when flash or above is received.
PRINTER WINDOW		
PRINTER	Highlights when printer is printing.	No action required.
CHK PTR	Highlights when printer off-line for more than 15 seconds.	Place printer on-line.
MSG MEM PERCENT USED	Displays internal memory used. Highlights at 90 percent. At 95 percent indicator flashes and messages moved to ASC.	Ensure formatted floppy disk is available.
DSK MEM PERCENT USED	Displays percent of memory used on hard disk.	No action required.
ZULU TIME	Greenwich Mean Time.	Time is indicated with a Z.
LOCAL TIME	Local time at your site.	No action required.

Table G-1. AN/UGC-144 alarms and indicators (continued).

INDICATOR	CAUSE	COMMENTS
DATE	ZULU date	Automatically updated at 0000Z each day.
AUDIBLE ALARM		
(An AUDIO ALARM sounds when immediate user attention is required or when detecting a fault or malfunction.)		
	Parity error occurs.	Check SSI settings.
	Flash or higher message is received.	Take immediate action to process message.
	Ring data signal received from DSVT.	Check SSI settings.
	A DACB INV is received.	Check SSI settings.
	A FIG S or J code is received.	Check SSI settings.
	Connection to distant end cannot be established.	Contact supporting signal officer.
	DACB protocol is used and SSI setup parameters are rejected by distant end.	Contact supporting signal officer.
	GO-ON-HOOK is received.	GO-ON-HOOK.
	Directed to GO TO VOICE.	GO TO VOICE.
	Message memory has less than 5 percent of storage remaining.	Move message to formatted floppy disk.
	Disk has less than 1 percent of storage remaining.	Replace disk.

Appendix H

Initialization Table Entries

H-1. Background

In the operating environment, the CT can be connected to one of the following equipments: DSVT, DNVT, or DLED. Tables H-1 through H-9 show the suggested settings for the initialization settings for the CT dependent upon the mission of the unit that owns the CT. Initialization table changes are required when operating in certain formats and modes.

H-2. Table Contents

Tables H-1 through H-7 show initialization entries for the CT using the DSVT connected through an AN/TTC-39().

Table H-1. SET UP MENU: Date/Time Update (DTU).

CT PROMPT	USER ENTRY
CURRENT DAY	APPROPRIATE DAY) (TWO DIGITS)
CURRENT MONTH	(APPROPRIATE MONTH) (USE ARROW KEYS)
CURRENT YEAR	APPROPRIATE YEAR) (FOUR DIGITS)
LOCAL TIME	(TIME AT LOCATION) (FOUR DIGITS)
ZULU TIME	(GMT) (FOUR DIGITS)

Table H-2. SET UP MENU: ACCESS.

NOTE: ACCESS sets the operator's level of classification. A password is re quired. Set classification to highest level which the operator/user can trans mit or receive. If operation is in a Y community, DOI-103 is displayed as an option.

CT PROMPT	USER ACTION (DEFAULTS SHOWN)
UNCLASSIFIED	ENABLED
RESTRICTED	DISABLED
CONFIDENTIAL	DISABLED
SECRET	DISABLED
TOP SECRET	DISABLED
--OR--	
DOI-103	ENABLED
TRANSMIT	DISABLED

Table H-3. SET UP MENU: Guarded (System Parameters).

NOTE: A password is required to make changes.

CT PROMPT	USER ACTION (DEFAULTS SHOWN)
TERMINAL COMMUNITY	R for JANAP 128 Y for DOI-103
CONTENT/COMM INDICATOR.	ZYUW
ORIGINATOR/DESTINATION LMF	AA
TERMINAL ROUTING INDICATOR	AS LISTED IN ACP/DOI
TERMINAL PLAIN LANG ADDR	YOUR LOCATION
TERMINAL CLASSIFICATION	AS PRESCRIBED

Table H-3. SET UP MENU: Guarded (System Parameters) (continued).

CT PROMPT	USER ACTION (DEFAULTS SHOWN)
TERMINAL PHONE NUMBER	CONTACT AN/TTC-39() SWITCH
CHANNEL ID	NO ENTRY
EOL SEQUENCE	<CR><CR><LF>
XMIT START ENVELOPE	NO ENTRY
XMIT STOP ENVELOPE (1-8)	NO ENTRY
XMIT STOP ENVELOPE (9-16)	NO ENTRY
RCV START ENVELOPE	NO ENTRY
RCV STOP ENVELOPE (1-8)	NO ENTRY
RCV STOP ENVELOPE (9-16)	NO ENTRY

Table H-4. SET UP MENU: Guarded (SSI Parameters).

NOTE: A password is required to make changes.

CT PROMPT	USER ACTION
MASTER/SLAVE	MASTER
DACB PROTOCOL	ON
CHANNEL CONTROL	MODE I BLOCK BY BLOCK
MESSAGE CODE/PARITY	ASCII ODD PARITY
LOOP RATE	32000
DATA RATE	16000
ERROR CONTROL	MULTISAMPLING
SSI INTERFACE	DSVT
AUTO RESYNC	OFF

Table H-4. SET UP MENU: Guarded (SSI Parameters) (continued).

CT PROMPT	USER ACTION
CLOCK SOURCE	INTERNAL
EXT CLOCK POLARITY	POSITIVE
TRANSMIT SIGNAL SENSE	MARK POSITIVE
RECEIVE SIGNAL SENSE	MARK POSITIVE
SERIAL DATA CODE	NRZ
NUMBER OF STOP BITS	1
DATA MODE CONTROLS	ON
MODE VI STORAGE BLOCKS	NONE
MODE I ANSWER TIMER	DEFAULT

Table H-5. SET UP MENU: Guarded (Printer Set Up Parameters).

NOTE: A password is required to make changes.

CT PROMPT	USER ACTION
BAUD RATE	9600
STOP BITS	1
PARITY	ODD
AUTO-OPT	TRANSMIT/RECEIVE

Table H-6. SET UP MENU: Guarded (RI/PLA Set Up Parameters)

NOTE: An additional password is required to make changes. (Entries may be preset by the supporting signal officer.)

#	RI	PLA	CLASS	PHONE

NOTE: Use function keys to EDIT LINE, ADD LINE, DEL LINE, or ERASE as required.

Table H-7. SET UP MENU: Guarded (Set Pass Set Up Parameters).

NOTE: This allows the security manager/AMPSSO/signal officer to set or change passwords for functions as shown.

FUNCTION	DEFINITION/PASSWORD
RSTRD	RESTRICTED Classification Access Password
CONF.	CONFIDENTIAL Classification Access Password
SEC	SECRET Classification Access Password
TOPSEC	TOP SECRET Classification Access Password
DOI103	DOI103 TERMINAL Community Access Password
XMT REL	TRANSMIT/RELEASE Enable Password
GUARDED.	GUARDED SETUP MENU Access Password
RIPLA.	RI/PLA TABLE SETUP Access Password
DOS	DOS Access Password

Table H-8 shows changes to the initialization table for a CT using a DLED going through an AN/TYC-39(). Only items shown need to be changed from those shown in Tables H-3 and H-4.

Table H-8. Initialization changes pertaining to DLED use.

CT PROMPT	CHANGES MADE
SYSTEM PARAMETERS	
XMIT STOP ENVELOPE (1-8)	<LF><LF><LF><LF><LF><LF><LF>N
XMIT STOP ENVELOPE (9-16)	NNN
RCV STOP ENVELOPE (1-8)	<LF><LF><LF><LF>)<LF><LF><LF>N
RCV STOP ENVELOPE (9-16)	NNN
SSI PARAMETERS	
MASTER/SLAVE	SLAVE
DACB PROTOCOL	OFF
LOOP RATE	16000
SSI INTERFACE	DLED
CLOCK SOURCE	EXTERNAL
DATA MODE CONTROLS	OFF

The following change is made to the initialization table entries (Table H-4) when the CT uses a DSVT in MSE.

LOOP RATE	16000

The following change is made to the initialization table entries (Table H-4) when the CT uses a DNVT in MSE.

SSI INTERFACE	DNVT

Table H-9 shows the changes to be made to the initialization table entries (Table H-3) when the CT is set for ACP 127 or MODE II JANAP 128/DOI 103 format when a message must pass through an AN/TYC-39() or through AUTODIN.

Table H-9. Changes for ACP 127/MODE II format for input through AN/TYC-39() or AUTODIN.

CT PROMPT	CHANGES MADE
XMIT START ENVELOPE	CZC
XMIT STOP ENVELOPE (1-8)	<LF><LF><LF><LF><LF><LF><LF>N
XMIT STOP ENVELOPE (9-16)	NNNN
RCV START ENVELOPE	CZC
RCV STOP ENVELOPE (1-8)	<LF><LF><LF><LF><LF><LF><LF>N
RCV STOP ENVELOPE (9-16)	NNN

Appendix I

CT Factory Default Setting

When a CT arrives at the authorized location, some initialization items will already be preset in the CT's memory. When a CT is turned into maintenance or zeroized for storage, the CT must be reset to the factory default settings. Table I-1 is provided for the CT operator to use as required. Failure to reset the CT to factory options prior to storage or return the terminal to maintenance will constitute a reportable security violation. See AR 380-5 for reporting procedures.

Table I-1. Factory default settings.

TERMINAL CLASSIFICATION	UNCLASSIFIED
TERMINAL COMMUNITY	R
CONTENT/COMM INDICATOR	ZYUW
ORIGINATOR/DESTINATION LMF	AA
TERMINAL PHONE NUMBER	NONE
TERMINAL RI	RUTAMPA
TERMINAL PLA	NONE
EOL SEQUENCE	NONE

Table I-1. Factory default settings (continued).

TRANSMIT START ENVELOPE	NONE
TRANSMIT STOP ENVELOPE	NONE
RECEIVE START ENVELOPE	NONE
RECEIVE STOP ENVELOPE	NONE
MASTER/SLAVE	SLAVE
DACB FUNCTION	ON
CHANNEL CONTROL	MODE I BLOCK BY BLOCK
MESSAGE CODE/PARITY	ASCII ODD PARITY
SSI LOOP RATE	16000 BAUD
SSI DATA RATE	1200 BAUD
SSI ERROR CONTROL	MULTISAMPLING
SSI INTERFACE	DSVT
AUTO RESYNC	OFF
CLOCK SOURCE	INTERNAL
EXTERNAL CLOCK POLARITY	POSITIVE
TRANSMIT SIGNAL SENSE	MARK POSITIVE
SERIAL DATA CODE	NRZ
NUMBER OF SSI STOP BITS	1
DATE MODE CONTROL	ON
MODE VI STORAGE BLOCKS	NONE
MODE I ANSWER TIMER	DEFAULT
PRINTER MESSAGE CODE	ASCII ODD PARITY
PRINTER BAUD RATE	1200 BAUD
PRINTER STOP BITS	1
AUTO-PRINT OPTION	OFF
AUTO-SAVE OPTION	OFF
CAPS LOCK OPTION	OFF
SPACE OPTION	SPACES
LINE LENGTH	69
TABS	No Tabs Set

Appendix J

Security and Protection Measures for Diskettes

J-1. In addition to procedures listed in Chapter 2 of this manual, the following procedures amplify requirements and must be followed at all times the CT is being used.

Security procedures. Diskettes containing classified or sensitive material must be afforded the same level of security that paper copy material is provided.

Diskettes containing sensitive Privacy Act data will be marked "FOR OFFICIAL USE ONLY- Privacy Act Data." Both the label on the diskette and its protective jacket will be appropriately marked.

Diskettes containing classified data will be handled and marked IAW AR 380-5. Both the label on the diskette and its protective jacket will be appropriately marked.

Diskettes will be stored to prevent unauthorized access, damage, modification, or destruction.

If diskettes become defective and are to be destroyed, the media should also be reformatted, re-initialized, or degaussed before being shredded or placed in a container for destruction.

"Deleting" or "killing" a file does not remove the data contained in that file from the diskette. It is simply "marked" as deleted, so that normal DOS operations cannot access the file. Utilities exist that can recover the file. Therefore, diskettes containing sensitive information must be reformatted, reinitialized, or degaussed prior to reuse.

Backup copies of sensitive data should always be maintained and stored away from work areas. Backup copies of sensitive data must be protected in the same manner as the original data.

Diskettes will not be removed from the organization without written approval from the ISSO/B SO.

On multiuser systems, each user should maintain his own diskettes. Those data files maintained on the hard disk should be write-protected to avoid damage or destruction by other users.

As an item of government property, diskettes are subject to inspection/examination for the presence of unauthorized data or software.

Diskettes and the files contained therein should be marked and labeled IAW MARKS.

Protection procedures. Diskettes must be protected when removed from their protective jackets. The following actions must be taken in order to properly protect diskettes.

Do not place diskettes on terminals, in books, or under equipment. Do not toss a diskette loosely in a drawer.

Do not place diskettes near any magnetic source such as telephones, radios, tape recorders, or loudspeakers of any kind.

Do not touch exposed areas of diskettes or try to wipe them clean, as they are easily scratched.

Do not place diskettes in direct sunlight and keep them away from extreme heat or cold.

Do not write directly on a diskette with ball point pen, lead pencil, or other hard writing instruments. Instead, use a felt tip pen and a label.

Do not leave diskettes containing sensitive information unattended in PCs or word processors.

Do not expose diskettes to cigarette smoke, ashes, or liquids of any kind. Accumulated particles on the diskette surface can damage the disk drive heads or the diskette or both.

J-2. The ISSO/BSO will provide training to ensure CT users are aware of and comply with required security and protection procedures associated with data diskettes.

J-3 . If a diskette marked as FORMATTED contains classified information and has not been protected at the highest level of classification of the material contained on the disk, a report will be initiated to supervisory/security personnel in accordance with AR 380-5.

Glossary

Acronyms, Abbreviations, and Definitions

addressee - The activity or individual to whom a message is directed by the record traffic originator. Addressees are indicated as either ACTION or INFORMATION.

ADDS Army Data Distribution System

admin administrative

ADP automatic data processing

AFATDS Advanced Field Artillery Tactical Data System

AFFOR Air Force forces

AFSOB Air Force Special Operational Base

Allied Communications Publication (ACP) - A series of publications designed for standardized communications procedures between the United States and its allies. ACPs govern the operations of signal systems in support of combined operations. ACP 201 is an index of ACPs, CT and TCC operators are obligated to use and follow the instructions contained in ACPs.

AMPSSO automated message processing special security officer

ANDVT advanced narrowband digital voice terminal

Area Common-User System (ACUS) - ACUS is a secure, multiuser, high volume C^2, administrative, logistics, operations, and intelligence voice and data traffic system. It is an integrated switching system from the battalion through theater Army. ACUS provides interface points with access to the strategic and sustaining base environments.

ARFOR	Army forces

Army Tactical Command and Control System (ATCCS) - The C^2 system for AirLand Operations (corps/tactical area of information management area).

ASAS	All Source Analysis System

ASCII - American standard code for information interchange. A standard code using a coded character set consisting of 7-bit coded characters used for information interchange among data processing systems, data communications systems, and associated equipment. The ASCII set consists of control characters and graphic characters.

AUD	audio

audit trail - A chronological record of activities that will enable the reconstruction, review, and examination of the sequence of events concerning each step in the process, transmission, receipt, and delivery of record traffic.

authentication - A security measure designed to protect a communications system against fraudulent transmissions or simulation by establishing the validity of a transmission, message, or originator.

auto dial - A function that allows for the automatic dialing of telephone numbers. An expanded version of programmed dialing found in commercial telephone instruments.

automatic digital network (AUTODIN) - A worldwide automatic communications network for DOD end-to-end message switched digital data communications. There are 15 AUTODIN switching centers in various locations worldwide.

automatic voice network (AUTOVON) - A worldwide automatic switched nonsecure voice communications system for end-to-end, voice connections for the DOD. It is part of the DCS. It is now designated the Defense Switched Network (DSN)(q.v.).

auxiliary storage cassette (ASC) - A component of a communications terminal on which to record/store record traffic.

basic emergency plan (BEP) - A series of plans of action that should be simple, capable of rapid execution and include priorities, methods, and levels of destruction, or evacuation to prevent unauthorized access to classified material or sensitive equipment.

battlefield automated systems (BAS) - These systems are used on the battlefield at corps, division, and brigade levels to collect, process, and distribute information required by commanders and staffs. Examples of BAS systems are the ASAS, TACCs, TACFIRE, and the AFATDS.

BSO	brigade/battalion signal officer
CEWI	Combat Electronic Warfare and Intelligence
CHS	common hardware and software
CIP	Communications Improvement Plan

circuit switching - A method of handling record traffic through a switching center, either from local users or from other switching centers, whereby a connection is established between the using terminals. The circuit will stay in use until the connection is released by one of the users. Primarily oriented to single connection to single destinations.

clk	clock

combat net radio (CNR) - This term covers a wide range of single- channel radio systems which provide immediate real-time C^2 voice capability.

communications security (COMSEC) - The protection resulting from all measures designed to deny unauthorized persons information of value that might be derived from the possession and study of telecommunications, or to mislead unauthorized persons in their interpretation of the results of such possession and study. COMSEC includes cryptosecurity, transmission security, emission security, and physical security of COMSEC material and information.

communications terminal (CT) - AN/UGC-144 computer terminal used to process formal tactical record traffic. Contains preformatted message headings to facilitate entry into the TRTS.

compromise - The known or suspected unauthorized disclosure or loss of sensitive defense information.

controlled area - A restricted area, adjacent to, or encompassing limited or exclusion areas where security controls have been applied to provide protection to an information processing system's equipment.

controlled cryptographic item (CCI) - A controlled COMSEC item that is unclassified when unkeyed. Although unclassified, the CCI is controlled to prevent loss or theft. When CCI is keyed, it becomes classified at the same level as the keying material within the CCI.

Corps/Theater ADP Service Center Phase II (CTASC II)- Administrative and logistical network that interfaces through the MSE and other message/circuit switching.

CRITIC - A precedence used for critical intelligence record traffic. This information includes but is not limited to strong indications of the imminent outbreak of hostilities of any type, aggression of any nature against a friendly country, or indication or use of NBC weapons.

CRITICOM critical intelligence communications cryptosecurity - The component of COMSEC that results from the provision of technically sound cryptosystems and their proper use.

CSN channel sequence number

CSS central security service (as used in this manual)

CSSCS Combat Service Support Control System

ctrl control

CW continuous wave

date-time group (DTG) - The date and time, expressed in digits and a time zone suffix, a message was prepared for transmission. The DTG is expressed as six digits followed by the zone suffix; the first pair of digits denotes the date, the second pair the hours, the third pair the minutes. When grouped with a standardized abbreviation for the month and the last two digits of the year (for example, 081948Z JAN 90), the DTG is a reference number for citing a record traffic message.

dedicated loop encryption device (DLED) - A CCI used to secure record traffic circuits between designated CTs and AN/TYC-39()s and between AN/TTC-39( )s and AUTODIN switching facilities.

Defense Communications Agency (DCA) - Provides access to the worldwide DCS. The DCA DCS is obtained at specific in-theater communications nodes at EAC. The DCA is being reorganized and renamed the Defense Information Systems Agency (DISA).

Defense Communications System (DCS) - A worldwide complex of defense establishment communications networks and control centers organized into a single compatible long haul general purpose system which provides theater-to-CONUS connectivity. These circuits are managed by the DCA. Access to the worldwide DCS is obtained at specific in-theater communications nodes at EAC.

Defense Data Network (DDN) - A packet-switched network with two elements - -backbone network (trunk circuits and packet switches) and access network (circuits and equipment). Access circuits and equipment allows the subscriber to connect to a vast network of several hundred packet switches worldwide.

Defense Operating Instructions (DOI) - A series of publications that establish operating procedures and instructions for record traffic within the DSSCS. DOI 103 is DSSCS operating instructions.

Defense Special Security Communications System (DSSCS) - This is a critical intelligence communications system and special intelligence communications network which provides for the transmission of CRITIC, SIGINT, and SCI record traffic.

Defense Switched Network (DSN) - The DSN is the C^2 telecommunications network for the US armed forces and other DOD authorized users. The DSN will evolve from its present analog character towards a digital communications network. DSN will include interface with foreign national tactical networks as well as public telephone and administrative private line networks. This has replaced AUTOVON (q.v.).

DGM	digital group multiplexer
DIA	Defense Intelligence Agency
DIAM	Defense Intelligence Agency Manual

digital nonsecure voice terminal (DNVT) TA-1035/TT - The DNVT is a 4-wire terminal contained in a ruggedized case which transmits and receives digitized voice and loop signaling information. The DNVT provides digital communications interface with MSE and EAC-CIP circuit switches. This equipment is also interoperable with the DSVT.

digital subscriber voice terminal (DSVT) KY-68 - A terminal device used in the intelligence community communications system, encrypted and decrypted voice traffic, and provides secure digitized data traffic. The DSVT provides secure and nonsecure access to the switched networks and secure access to nonswitched networks.

DISA Defense Information Systems Agency (See Defense Communications Agency.)

DMS Defense Message System

DOS Disk Operating System

DSNET Defense Secure Network

DTMF dual- tone multifrequency

DTU date/time update

ECB echelons corps and below

electronic mail (E-mail) - Unclassified.

elm element

emission security - Component of COMSEC that results from all measures taken to deny unauthorized persons information of value that might be derived from intercept and analysis of compromising emanations from cryptographic equipment and telecommunications systems.

end of line (EOL) - A series of computer functions that indicate to the computer terminal that the end of a line of text has been reached.

EPLRS Enhanced Position Location Reporting System extension switches - MSE extension node switch, either an SEN switch or an LEN switch. Extension switches allow wire line terminal subscribers (telephone, facsimile, and data) as well as NRI and RAU to enter the ACUS.

FAAD	Forward Area Air Defense
FAADC^{3}I	Forward Area Air Defense Command, Control, Communications, and Intelligence

facsimile (fax) - Fax is a system of telecommunications for the transmission of fixed images (maps, graphs, and narrative text) with reception in a permanent form. Used at brigade and battalion level in TRTS for informal record traffic.

first in, first out - An order of precedence for processing record traffic messages based upon the order in which the messages were received. All priority messages would be processed before processing began on a routine message.

FLCS	Force Level Control System

full-duplex - A mode of operation that allows for transmission and receipt of voice or data messages over a circuit. Two messages going in opposite directions at the same time over the same circuit. In wire operation, the term 4-wire indicates a circuit is using two lines or channels for communications.

gateway (circuit switch) - A switching center, located at corps rear boundary/EAC, that uses store and forward capability to interface/access to theater user terminals, allied systems, and AUTODIN switching centers record traffic.

gateway (packet switch) - Provides a path for data flow between different networks. Gateways used to connect LANs with other LANs or with WANs. In tactical application, connects tactical networks to DSNET 1.

GENSER	general service
GMT	Greenwich Mean Time

half-duplex - A mode of operation that allows data to be passed in either direction, but in only one direction at a time. In a 2-wire circuit, the term half-duplex indicates a circuit using one line or channel for communications in both directions.

inadvertent disclosure - Accidental exposure of sensitive defense information to a person not authorized access. This may result in a compromise or a need-to-know violation.

INFO information

information addressee - Organization listed on a record traffic message who has been forwarded the message for information purposes only. No action on the information addressee's part is required.

information service support officer (ISSO) - An individual appointed by the commander of a post, installation, or equivalent command level to act as the focal point and principal advisor for all information systems security matters.

initialize - A process of entering selected and required information into terminal memory. The term refers to all the actions taken to set up, turn on, and operate a terminal when it first enters service in a network.

insecurity - Any occurrence that may jeopardize the security of classified record traffic or cryptographic material/items. Physical insecurities involve the loss, theft, capture, tampering, or unauthorized viewing, access, or photography of classified material. A personnel insecurity occurs when a person having access to classified information is suspected of espionage, defection, subversion, or sabotage.

JANAP Joint Army-Navy-Air Force Publication

JOC Joint Operations Center

JSOTF Joint Service Office task force

JTF	joint task force
LAN	local area network

language media format (LMF) - LMF is computer characters that inform the receiving terminal or switching center in what format the message was prepared and what the required output will be at the addressee terminal.

LENS	large extension node switch

lightweight digital facsimile (LDF) - A lightweight, one-man portable digital and analog facsimile terminal. It electronically transmits black-and-white graphic or text information between remote or centralized military communications facilities. The facsimile is designed for use with present and future digital communications systems. LDFs may be mounted and used in tactical vehicles which are user-owned and -operated.

MARFOR	Marine forces
MARKS	Modern Army Recordkeeping System
MCS	maneuver control system
MCSF	Marine Corps Special Forces

message privacy - Procedure applied to record traffic that ensures only authorized individuals obtain access. All record traffic, both formal and informal, is processed with utmost privacy.

message switching - The technique of receiving a message, storing it until the proper outgoing line is available, and then retransmitting the message. No direct connection between the incoming and outgoing lines is set up as is circuit switching. Message switching is done on a store and forward basis.

MILNET	military net
MLS	multilevel secure

mobile subscriber equipment (MSE) - The MSE system covers the corps rear boundary forward to the division maneuver battalions rear area of 37,500 square kilometers (15,000 square miles). Node centers make up the system's backbone and provide connectivity to extension switches and RAUs. The MSE system lets subscribers communicate with each other on a discrete address basis, using fixed directory numbers regardless of a subscriber's battlefield location.

mobile subscriber radiotelephone terminal (MSRT) - The MSRT provides users a means of discretely addressing switched common-user system users by radio linkage. There are approximately 1,900 MSRTs within a corps area which allows subscribers to communicate with other MSRT users within its radio range or to communicate with wire subscribers and distant MSRTs through an RAU. The MSRT, combined with an RAU, allows subscribers to place full-duplex secure voice and data calls to fixed or mobile users.

mode - In record traffic communications, different types of protocols are used for channel coordination to transfer data from a switch to a switch, or from a switch to a terminal. In AUTODIN, modes I, II, III, IV, and V are used in various equipments to switch configurations. In MSE, mode VI is a duplex operation with automatic error and channel controls allowing independent and simultaneous two-way transmission.

MPN	MSE packet network
msg	message

multilevel security operation - A mode of operation in which various categories and types of classified record traffic may be concurrently stored and processed within a system which permits concurrent access by users not cleared for the highest category of information in the system and users having the proper clearances and need-to-know. The separation of personnel and information on the basis of security clearance and need-to-know is accomplished by the operating system and associated system software.

NCA national command authority

NCS node control switch

need-to-know - The necessity for access to, knowledge of, or possession of classified or other sensitive defense information in order to carry out official military duties. Responsibility for determining access rests with the individual who has current possession, knowledge, or control of the information and not upon the prospective recipient.

need-to-know violation - The disclosure of classified or other sensitive defense information to a person who is cleared but has no requirement for such information to carry out assigned duties.

net radio interface (NRI) - Method for bridging between the commander's two primary means of C^2, tactical radio, and telephone networks. NRI extends communications distance as it connects the tactical radio into the division/corps wire system.

network gateway - A special purpose dedicated computer that attaches two or more networks and routes packets from one to the other. In particular, gateways are used to connect different large, medium, and small networks.

node - Signal center operated by US Army Signal Corps personnel.

NSWTG Naval Special Warfare Training Group

packet switching/DDN - Provided by a data packet-switch processor specifically designed for high-speed communications. Provides for interconnection of multiple hosts in a local or geographically distributed environment.

packet switching/MSE - A system in which messages are broken down into smaller units called packets (a group of data and control characters in a specified format that are then individually addressed and routed throughout the network). The packet format allows data traffic to be forwarded over MSE without competing with voice switching resources. In packet switching, data record traffic is automatically routed around congested, damaged, or destroyed network components. All routing is transparent to the user.

password - A word, character, or combination of words and characters that permits access to otherwise inaccessible data, information, or computer files.

PC personal computer

personnel security - The procedures established to ensure that all personnel who have access to sensitive defense information have the required authority as well as the appropriate security clearances.

physical security - The component of COMSEC that results from all physical measures necessary to safeguard classified equipment, material, and documents from access or observation by unauthorized personnel.

plain language address (PLA) - An abbreviated or nonabbreviated activity/organization title with associated geographical location, used in message addressing. Standardized PLAs have been developed to eliminate variances in the manner in which a specific organization may be addressed.

PSN packet-switch network

PWDS Protected Wire Distribution Systems

R Worldwide Routing Indicator Community (GENSER - worldwide) radio access unit (RAU) - A high mobility multipurpose wheeled vehicle (HMMWV) and shelter with necessary electrical components to provide mobile radiotelephone subscriber access to the mobile subscriber equipment system. There are 92 RAUs in a five-division corps.

RAM random access memory

record traffic - Messages in permanent or quasipermanent form that is recorded by the originator, the addressee, or both.

routing indicator (RI) - A series of letters assigned to indicate the geographical location of a terminal; a fixed headquarters of a command, activity, or unit at a geographic location; and the general location of a switch or terminal to facilitate the routing of record traffic over communications systems.

S variable - Classified encrypt/decrypt key variable used in DSSCS record traffic. See the supporting signal officer or COMSEC officer for additional information.

sanitize - To rearrange/delete/overwrite recorded data information to prevent unauthorized disclosure. To properly sanitize a CT, all initialized data is returned to factory default options.

SCIF sensitive compartmented information facilities

sensitive compartmented information (SCI) - Information and material that requires special controls for restricted handling within compartmented intelligence systems and for which compartmentalizing is established.

secure voice system (SVS) - The secure voice system replaces the automatic secure voice communications (AUTOSEVOCOM) system. The SVS currently consists of the secure telephone units (STU-III) to provide secure voice telephone service for common users and the RED switch program which provides high quality secure voice to C^2 users on a network separate from the common-user network.

SENS small extension node switch

sensitive defense information - Any information which requires a degree of protection and which should not be made generally available. This type of information includes, but is not limited to, that information which must be safeguarded to prevent damage to national defense and protect information which the commander considers essential for the mission.

service message - A brief, concise message between CTs or TCCs pertaining to any phase of record traffic handling.

SFOB Special Forces Operational Base

SIGINT signals intelligence

SINCGARS Single Channel Ground and Airborne Radio System

single subscriber interface (SSI) - Component of CT that allows connection of CT to various secure devices for encryption/decryption of record traffic. SSI setup is accomplished by the supporting signal officer.

SPECAT special category

special security officer (SSO) - Individual or office who manages DSSCS record traffic, security clearances, and routine administrative matters pertaining to special intelligence, critical intelligence, and SCI record traffic.

speed-of-service - The expected speed for each precedence of record traffic to be processed and delivered to the intended addressees.

Message originators expect/require record traffic to be delivered in the time frame as indicated by the precedence they have assigned to their message.

SSI single subscriber interface

SSN station serial number

SSO special security officer

store and forward - A record traffic message handling technique whereby messages are received and held at a message switch pending availability of outgoing circuits and then transmitted onward IAW the designated precedence.

TAC terminal access controller

TACCS Tactical Army Combat Service (CSS) Computer System

TACFIRE tactical fire direction system

Tactical Record Traffic System (TRTS) - A group of networks and systems that provide for the acceptance, transmission, receipt, processing, and distribution of originated and terminated formal or informal record traffic communications. Means include tactical TCCs with associated teletypewriters, messenger service, and RATT; user-owned and -operated computer processors, facsimile sets and augmented messenger service; Signal Corps-owned and -operated message and circuit switches; and the DCA/DISA subsystems (AUTODIN/DMS/AUTOVON, DSN/DDN).

telecommunications center (TCC) - An organization/section responsible for the acceptance, transmission, receipt, process, and distribution of incoming and outgoing record traffic. TCCs will normally have three internal sections to accomplish their mission--means section (transmit-receive), messenger section, and message center section.

TPN tactical packet network

transmission security - The component of communications security that results from all measures designed to protect transmissions of record traffic from interception and exploitation by means other than cryptoanalysis.

TRC transmission release code

TRI-TAC joint tactical communications

TS Top Secret

TTY teletypewriter

voluntary correction (VOL CCN) - Communications term that means a message originator or a CT user has changed/corrected the textual content of a previously transmitted message. A VOL CCN must be sent prior to the distant end servicing the message for being garbled or incomplete. The complete message or a portion of the message may be corrected by using VOL CCN.

WAN wide area network

WX weather

xmit transmit

xmsn transmission

Y Worldwide Routing Indicator Community (DSSCS - SSO)

References

SOURCES USED

These are the sources quoted or paraphrased in this publication.

Allied Communications Publication (ACP)

ACP 127. US Supplement l(H). Communications Instructions Tape Relay Procedures. May 84.

ACP 131. Communication Instructions Operating Signals. May 86.

Army Regulation (AR)

AR 25-11. Record Communications and the Privacy Communications System. 4 Sep 90.

AR 25-400-2. The Modern Army Recordkeeping System (MARKS). 15 Oct 86.

AR 190-13. The Army Physical Security Program. 20 Jun 85.

AR 380-5. Department of the Army Information Security Program. 25 Feb 88.

AR 180-19. Information Systems Security. 1 Aug 90.

AR 380-40. Policy for Safeguarding and Controlling COMSEC Information. 1 Jun 82.

Defense Intelligence Agency Manual (DIAM)

DIAM 50-3. (0) Physical Security Standards for Sensitive Compartmented Information Facilities. 2 May 80.

Defense Operating Instructions (DOI)

(S) DOI 101. DSSCS Address Groups (U). Jul 90.

(C) DOI 103. Operating Instructions: System/Data Procedures (U). May 90.

Department of the Army Forms (DA Form)

DA Form 1594. Daily Staff Journal or Duty Officer's Log. Nov 62.

DA Form 1999-R. Restricted Area Visitor Register. Jan 88.

DA Form 2028. Recommended Changes to Publications and Blank Forms. Feb 74.

DA Form 3918-R. Facsimile Transmittal Header Sheet. Jul 90.

DA Form 4011. Telecommunications Center Delivery List. Apr 73.

DA Form 4016. Telecommunications Center Originating Message Register. Apr 73.

DA Form 5651. Message Control Log. Aug 87.

DA Form 5651-1. Terminating Message Register. Aug 87.

Field Manual (FM)

FM 3-5. NBC Decontamination. 24 Jun 85.

FM 3-100. NBC Operations. 17 Sep 85.

FM 5-20. Camouflage. 20 May 68.

FM 5-25. Explosives and Demolitions. 10 Mar 86.

FM 11-23. Theater Communications Command (Army). 28 Nov 72.

FM 11-30. MSE Communications in the Corps/Division. 27 Feb 91.

FM 11-32. Combat Net Radio Operations. 15 Oct 90.

FM 21-26. Map Reading and Land Navigation. 30 Sep 87.

FM 24-1. Signal Support in the AirLand Battle. 15 Oct 90.

FM 24-16. Communications -Electronics: Operations, Orders, Records and Reports. 7 Apr 78.

FM 25-101. Battle Focus Training. 30 Sep 90.

Joint Army-Navy-Air Force Publication (JANAP)

JANAP 128(1). Automatic Digital Network (AUTODIN) Operating Procedures. Mar 83.

JANAP 201(L). (C) Status of Noncryptographic JANAPs and ACPs (U). 1 Oct 83.

Technical Bulletin (TB)

TB 380-40-1. (0) Security Provisions for Use of TSEC/KY-65A and TSEC/KY-75A. 4 Feb 89.

TB 380-40-22. (0) Security Standards for Controlled Cryptographic Items. 29 Aug 86.

TB 380-41. (0) Procedures for Safeguarding, Accounting, and Supply Control of COMSEC Material. 1 Jul 81.

TB 380-41-3. (0) Procedures for Safeguarding Accounting and Supply Control of COMSEC Material, Volume 3--Accounting and Reporting Procedures. 30 Oct 85.

TB 380-41-5. (0) Procedures for Safeguarding, Accounting, and Supply Control of COMSEC Material, Volume 5, Safeguarding COMSEC Material. 1 Apr 87.

DOCUMENTS NEEDED

These documents must be available to the intended users of this publication.

FM 11-490-2. Army Communications Facilities; Telecommunications Center Operating Procedures. 31 Oct 84.

By Order of the Secretary of the Army:

GORDON R. SULLIVAN
General, United States Army
Chief of Staff

Official:

PATRICIA P. HICKERSON
Brigadier General, United States Army
The Adjutant General

DISTRIBUTION:

Active Army, USAR and ARNG: To be distributed in accordance with DA Form 12-llE, requirements for FM 24-17, Tactical Record Traffic System (TRTS) (Qty rqr block no. 0214).

PIN: 023721-000