SUBCOURSE
IT 0763

EDITION
7

US ARMY INTELLIGENCE CENTER AND SCHOOL
LEGAL ASPECTS OF COMSEC MONITORING AND MONITORING EQUIPMENT

THE ARMY INSTITUTE FOR PROFESSIONAL DEVELOPMENT
ARMY CORRESPONDENCE COURSE PROGRAM

AIPD

READINESS/ PROFESSIONALISM
THRU GROWTH

LEGAL ASPECTS OF COMSEC MONITORING AND MONITORING EQUIPMENT

US Army Intelligence Center and School

4 Credit Hours

GENERAL

This subcourse provides you with knowledge required to understand the legal basis for Communications Security (COMSEC) monitoring and the restrictions placed on monitoring and eavesdropping activities. It also describes the equipment used in COMSEC monitoring.

The terminal learning objectives for this subcourse are to:

Identify and discuss the legal aspects of COMSEC monitoring.

Explain the capabilities and identify the major components of COMSEC monitoring equipment.

CONDITIONS: Given this subcourse and a pencil.

STANDARD: You will correctly answer at least 70 percent of the multiple-choice questions on the subcourse examination.

TABLE OF CONTENTS

Title		Page
Title Page		763-i
LESSON 1:	LEGAL ASPECTS OF COMSEC MONITORING	763-1
	Introduction	763-2
	Background	763-2
	Non-COMSEC Telephone Monitoring	763-2
	COMSEC Monitoring	763-10
	Penalties for Illegal Electronic Surveillance	763-12
	Practice Exercise 1	763-13
	Practice Exercise 1 Solutions	763-16
LESSON 2:	COMSEC MONITORING EQUIPMENT	763-17
	Introduction	763-18
	AN/TRR-33 Radio-Telephone Monitoring Set	763-18
	AN/TTR-1A Telephone Monitoring Set	763-27
	Fly Away Kit	763-30
	AN/GRR-8	763-30
	Other Equipment	763-31
	Practice Exercise 2	763-32
	Practice Exercise 2 Solutions	763-34
APPENDIX A:	COMPARISON OF TYPES OF MONITORING	763-35
APPENDIX B:	ACRONYMS	763-37

LESSON 1

LEGAL ASPECTS OF COMSEC MONITORING

OBJECTIVE:

Tasks: At the end of this lesson you will be able to identify and discuss the legal aspects of COMSEC monitoring.

Standard: You will complete the practice exercise to 100 percent accuracy.

REFERENCES:

Executive Order 12333, United States Intelligence Activities, Dec 81
Title 18 US Code, Crimes and Criminal Procedures, 1968
AR 105-23, Administrative Policies and Procedures for Base Telecommunication Services, May 78
AR 190-30, Military Police Investigations, Jun 78
AR 190-53, Interception of Wire and Oral Communications for Law Enforcement Purposes, Nov 78
AR 380-53, Telephone Communications Security Monitoring, Nov 84
AR 380-380, Automated System Security, Mar 85
AR 381-10, US Army Intelligence Activities, Feb 82
AR 525-1, The Department of the Army Command and Control System, Oct 82
AR 530-2, Communications Security, Sep 82

OFFICER'S TASKS:

01-3352.06-0500, Conduct COMSEC M&A Missions
01-3352.06-0531, Open a COMSEC Account
01-3352.06-0532, Administer a COMSEC Account

INTRODUCTION

One of the most important functions an officer in charge of signal security (SIGSEC) assets performs is COMSEC monitoring missions. Before conducting such a mission, it is vital you know exactly what you are allowed to do, and --more importantly --what you are prohibited from doing. Title 18 of the United States Code, executive orders, and Army regulations (AR) contain specific prohibitions concerning monitoring and eavesdropping activities. To protect yourself, your subordinates, and your superiors, you must know not only what you are and are not allowed to do, but also the authority for the conduct of COMSEC monitoring.

BACKGROUND

An excerpt of the Fourth Amendment to the United States (US) Constitution is in figure 1. The provisions of this excerpt form the basis for all restrictions on monitoring and eavesdropping activities. Title III of the Omnibus Crime Control and Safe Streets Acts of 1968 (Title 18 US Code, Sections 2510-2520) places restrictions on electronic intercept of wire and oral communication. However, Title III specifically states that nothing contained therein "shall limit the constitutional power of the President to take such measures as he deems necessary...to protect national security information against foreign intelligence activities." SIGSEC units must operate in the narrow space between their legal responsibilities and the restrictions placed by law.

> "The right of the people to be secure in their persons, houses, papers, and effects against unreasonable searches and seizures, shall not be violated, and no warrants shall be issued."

Figure 1. Fourth Amendment Excerpt.

NON-COMSEC TELEPHONE MONITORING

Department of the Army (DA) has granted authority to a number of Army agencies other than SIGSEC units to monitor telephones. All such monitoring is regulated as strictly as is COMSEC monitoring and restricted to specific situations.

Communication Management Monitoring

Communication management monitoring is governed by AR 105-23. The purpose of this form of monitoring is to determine whether Army telephone systems are functioning properly and efficiently. Recording of conversations is prohibited under this program. Also prohibited is monitoring to determine whether the Army telephone system is being used for other than official purposes.

Operations Center Monitoring

Operations center monitoring is governed by AR 525-1. Operations centers that comprise the DACCS are the Operations Center at the Pentagon and the operations centers of major Army commands (MACOM), Continental US (CONUS) Armies, and Army components of unified and specified commands. These Department of the Army Command and Control Systems (DACCS) are authorized to monitor their own communication to protect classified information. Operations center personnel must be advised telephones are for transmission of official information only and subject to monitoring at all times.

Military Police (MP) Operations Desk Monitoring

MP operations desk monitoring is governed by AR 190-30. Telephone conversations may be recorded at MP operations desks to provide an exact record of emergency communication. Such recordings are usually made by a tape recorder attached to an operations desk telephone. All telephones connected to recording devices must be marked "FOR OFFICIAL USE ONLY -ATTACHED TO RECORDING DEVICE." Access to these telephones is limited to MP operations desk personnel. Emergency telephone numbers printed in a command/installation telephone directory must have a warning statement that emergency conversations will be recorded to ensure accuracy of records. Recordings may be used in place of written entries in an MP log, and may be retained for 60 days. Written transcripts may be made for permanent files. Monitoring or recording of radio or telephone transmissions by MP for any other purpose is governed by AR 190-53.

Law Enforcement Monitoring

As stated above, law enforcement monitoring is governed by AR 190-53 (see appendix A). Intercept of wire communication is authorized only when the information is necessary for criminal investigation and cannot reasonably be obtained in some other manner. The only DA elements authorized to intercept wire communication under AR 190-53 are the Criminal Investigations Command (CID), IP, US Army Intelligence and Security Command (USAINSCOM), and 650th MI Group. The latter two organizations may investigate espionage, sabotage, and treason cases. Intercepts in investigations may be conducted as criminal cases or as counterintelligence (CI) cases, in which case AR 381-10 applies. Intercepts for CI purposes will be discussed later in this lesson. There are two types of communication intercept for law enforcement purposes--consensual and nonconsensual.

- A consensual intercept is one in which at least one party to a conversation is aware of the intercept.

- A nonconsensual intercept is one in which no party to a conversation is aware of the intercept.

In general, any intercept is prohibited unless there is probable cause to believe an offense punishable by death or imprisonment for more than a year has been, is being, or is about to be committed. Additionally, consensual intercepts are permitted in cases of obscene or threatening phone calls to include harassment, extortion, bribery, bomb threats, or threats of bodily harm made to authorized users of Department of Defense (DOD) telephones.

Consensual Interceptions. The authorization for each consensual interception shall define clearly the manner in which the interception is to be accomplished. A consensual interception shall not involve the installation of equipment in violation of the constitutionally protected rights of any non-consenting person whose conversation will be intercepted. Requests for consensual interceptions will be made as prescribed for nonconsensual interceptions, except only the following information need be included:

- A description of the facts and circumstances requiring the intended interception, the means by which it would be conducted, the place in which it would be conducted, and its expected duration.

- The names of all the persons whose conversations are expected to be intercepted and their roles in the crime being investigated. When the name of the nonconsenting party (ies) is not known when the request is made, the official making the request shall supply such information within 39 days after termination of the interception. If the information is not known at the end of this period, it shall be supplied whenever it is discovered.

- A statement that, in the judgment of the person making the request, the interception is warranted in the interest of effective law enforcement.

An application for a court order is not needed in this situation. Written approval of the request shall be made by the Secretary of the Army, the Army general counsel, or in their absence, the DOD General Counsel. This approval authority can not be delegated.

Nonconsensual Intercepts Within the US. When a nonconsensual intercept is deemed necessary for a criminal investigation, the MACOM will send a "Request for Authorization" through HQDA to the Army general counsel. If the offense being investigated is espionage, sabotage, or treason, the request will be sent through HQDA (DAMI-CI). All other requests will be sent through HQDA (DAPE-HRE). The request for authorization will contain:

The offense being investigated.

- The type of communication to be intercepted.
- The place of the interception (one of the parties must be using a DOD telephone).
- Whose communication will be intercepted.
- The type of interception to be used.
- The length of time the interception will be maintained.
- The circumstances warranting the interception in place of other means of investigation.

If the Army general counsel decides in favor of the interception, the official making the request will coordinate with a US attorney for the issue of a court order to authorize the interception. The following condition must exist in order to conduct COMSEC monitoring; at least one monitored party is using a DOD telephone.

Nonconsensual Intercepts Outside the US. The request for authorization will be processed the same as prescribed for intercepts within the US. If the target is subject to the Uniform Code of Military Justice (UCMJ), upon receipt of the approval, the requester will send the application to a military judge who has been assigned by the Judge Advocate General to receive such applications. The judge can approve or disapprove the request based on guidance published in AR 190-53. If the target of the interception is not subject to the UCMJ, the Army general counsel will, upon approving the request, determine what further approval is required by law.

Time Limits for Interception. Interception within the US may be approved for up to 30 days and may be extended for periods of up to 30 days per extension. Interceptions outside the US and extensions thereof may be for up to 60 days. Extension requests must be submitted the same as original applications.

Termination of Interceptions. Interceptions will be ended when (whichever occurs first):

- The authorization for the interception expires.
- The desired information is obtained.
- It is evident the interception is and will be nonproductive.

Electronic Surveillance

Electronic surveillance is governed by chap 3, AR 381-10 (see appendix A). This regulation provides guidance for Army intelligence organizations to:

- Conduct electronic surveillance for the support of foreign intelligence and CI activities.

- Obtain approval to conduct electronic surveillance.

- Process electronic surveillance information including that received from other agencies and governments and index and safeguard such information.

General Policy. Activities listed are governed by AR 381-10. Military or civilian members of the Army may not without specific approval--

- Engage in electronic surveillance.

- Directly or indirectly request any person or agency to engage in electronic surveillance.

- Assist any person or agency in conducting such surveillance.

Army intelligence elements may receive, retain, use, or disseminate electronic surveillance information on a US or non-US person from non-Army sources without prior approval if they--

- Do not directly or indirectly request surveillance be conducted or assist in the conduct of the surveillance.

- Report in accordance with paras 3-5c and 3-6e, AR 381-10.

All electronic surveillance information must be screened, safeguarded, and indexed in accordance with paras 3-6 through 3-8, AR 381-10, regardless of the source of the information.

Approval Authority. Electronic surveillance targeted against anyone within the US or against US persons anywhere must be approved in advance by the Secretary or Under Secretary of the Army. Before requesting secretarial approval, HQDA will obtain Attorney General approval and warrants when required.

Electronic surveillance targeted against non-US persons outside the US must be approved in advance by the Commander, USAINSCOM; Commander-in-Chief US Army Europe (CINCUSAREUR); or Commander, Eighth Army (EUSA). This authority may be delegated to the respective deputy commander, chief of staff, or subordinate responsible MI group commander. No further delegation is permitted.

Approval Standards. The following definitions apply only for the portion of this lesson concerning approval standards for electronic surveillance and those portions of AR 381-10 so identified.

Foreign Intelligence Information (para 3-4b(2), AR 381-10):

Information that relates to the ability of the US to protect against--

- Actual or potential attack or other grave hostile acts of a foreign power or agent of a foreign power.
- Sabotage or international terrorism by a foreign power or agent of a foreign power.
- Clandestine intelligence activities by an intelligence service or network of a foreign power or agent of a foreign power.

Information on a foreign power or foreign territory that relates to--

- The national defense or the security of the US.
- The conduct of the foreign affairs of the US.

Foreign Power (para 3-4b(2), AR 381-10):

- A foreign government or any of its components, whether or not recognized by the US.
- A faction of a foreign nation or nations not substantially composed of US persons.
- An entity openly acknowledged by a foreign government to be directed and controlled by such government.
- A group engaged in or planning international terrorism.
- A foreign based organization not substantially composed of US persons.

Agent of a Foreign Power (para 3-4b (5), AR 381-10). A person who--

- On behalf of a foreign power, is engaged in clandestine intelligence activities (including covert activities intended to affect the political or governmental process), sabotage, or international terrorist activities. It includes anyone who conspires with, or knowingly aids and abets a person engaging in such activities.
- Is unlawfully acting for or following the direction of a foreign power. The fact a person's activities may benefit or further the aims of a foreign power does not bring that person under the purview of this definition. Evidence must show the person is taking direction from or acting in knowing concert with the foreign power.

Approval standards for electronic surveillance depend on a combination of whether the surveillance is to be within or outside the US, whether or not the surveillance is to be directed against a US person, and whether the requested surveillance is consensual or nonconsensual.

All (consensual and nonconsensual) electronic surveillance conducted against non-US persons outside the US and all consensual electronic surveillance of non-US persons within the US require the approval authority has reasonable grounds to believe the surveillance will gather significant foreign intelligence or CI that cannot be reasonably obtained by less intrusive means.

All nonconsensual electronic surveillance conducted within the US will be limited to the collection of foreign intelligence information as defined above where the approval authority has reasonable grounds to believe--

- The target is a foreign power or an agent of a foreign power.
- The place where the electronic surveillance is directed is being used, or will be used by a foreign power or an agent of a foreign power.
- The information needed cannot be otherwise obtained.

Nonconsensual electronic surveillance of a US person outside the US will be approved only if--

- A probable cause exists to believe the target is an agent of a foreign power.
- Reasonable grounds exist to believe the electronic surveillance will gather significant foreign intelligence or CI that cannot otherwise be obtained.

Approval for consensual electronic surveillance of US persons will be limited to the collection of foreign intelligence and CI information in accordance with procedure 1, chap 2, AR 381-10. This procedure concerns the collection of information about US persons and applies to all methods of collection.

Approval Procedures. Requests for approval of electronic surveillance will--

- Detail the facts showing the approval standard is satisfied.
- Describe the nature and content of conversations expected to be intercepted.
- Identify the unit that will conduct the surveillance.
- Identify all people under investigation or those whose conversations could be intercepted and identify those who have agreed to the surveillance.
- Describe the equipment to be used, transmission method, the recording device, and the installation method.

State the location of the proposed surveillance. If applicable, include the address, telephone number, room number, whether inside or outside a building, on public or private property, means of access, and whether physical trespass will be necessary to install technical listening equipment at the locations of the proposed surveillance.

- Give the expected duration of the surveillance. It should be as short as possible consistent with the limitations described below under "Time Limits."

- Describe any other less intrusive investigative procedures that have been tried and failed, why they may fail again, or why they are too dangerous to try.

- If the request is for an extension of a previous authorization, describe the results thus far obtained from the interception, or give a reasonable explanation of the failure to obtain results.

- Show the request has been coordinated with the appropriate command judge advocate.

- If known, show whether previous requests have been made for electronic surveillance on any of the same persons, facilities, or places to be surveilled. State whether such requests were approved or disapproved by a military or federal judge.

- If electronic surveillance of a US person outside the US is requested, include a statement that the proposed electronic surveillance is consistent with US obligations under applicable Status of Forces Agreements.

Requests for approval by the Secretary or Under Secretary of the Army will be submitted through command channels to HQDA (DAHI-CICI), Washington, DC 20310, who will coordinate with The Judge Advocate General and submit the request through the Army general counsel. The Assistant Chief of Staff, Intelligence (ACSI) will be responsible for obtaining approval from the Secretary or Under Secretary of the Army. Requests submitted by electrical message may key the information to the format specified for written requests. Telephone requests must be confirmed in writing within 48 hours.

Time Limits for and Termination of Surveillances. Approvals will not be granted for more than 30 days for electronic surveillances within the US and 90 days outside the US. Renewals will be for a maximum of 30 and 90 days respectively. As an exception, renewals of electronic surveillance involving strategic foreign intelligence cases targeted against foreign government agencies and their non-US person employees may be for up to six months. All renewal requests will be submitted through the same channels as the original request. All electronic surveillances will be terminated as soon as all the desired information described on the request is obtained regardless of how much time remains until the authorization expires. If the authorization is not renewed by the expiration date, the surveillance will be terminated.

COMSEC MONITORING

The results of COMSEC monitoring made by SIGSEC personnel, with certain exceptions, cannot be used for law enforcement or intelligence purposes. Therefore, SIGSEC personnel and equipment cannot be used for any purpose other than COMSEC monitoring. The publications governing COMSEC monitoring are:

- AR 380-53.
- AR 530-2.

COMSEC Monitoring Operations

COMSEC monitoring will be conducted in a manner that minimizes, as much as possible, the monitoring and recording of conversations not relevant to the COMSEC monitoring mission. Conversations conducted over DOD telecommunication systems will be assumed to be official communication subject to monitoring. COMSEC monitoring will be limited to official telecommunication systems owned or leased by DOD including radio networks, telephones, telephone systems, and transmission systems.

Use of COMSEC Monitoring Products

The products of COMSEC monitoring will be used to meet COMSEC objectives. Exceptions are as follows:

- Information obtained from COMSEC monitoring may be used in connection with disciplinary or administrative action against DA personnel for knowing, willful, or negligent actions that result in the unauthorized disclosure of classified information. Recorded tapes of conversations involved may be released upon written request of the supported commander or designate representative if required for evidence.
- Information may be obtained incidentally during the course of COMSEC monitoring authorized by AR 380-53 that relates directly to a significant crime. This information will be reported by the COMSEC monitoring elements to the commander directing the COMSEC monitoring mission.

COMSEC Monitoring Working Materials

Routine access to COMSEC monitoring working materials such as operator logs, operator or analyst notes, and recording tapes will be limited to SIGSEC specialists. Access to COMSEC monitoring working materials may be granted to commanders and their designated staff officers exercising direct management authority over the COMSEC monitoring element if such access is for the purpose of supervising, directing, and checking the efficiency, regulatory compliance, and mission effectiveness of COMSEC monitoring personnel.

Unprocessed working material will be dated and marked "WORKING PAPERS". This material will be classified according to content and marked with the highest classification of any information contained therein. If monitoring personnel are unable to determine the classification, a minimum tentative classification of CONFIDENTIAL will be assigned.

Processed recording tapes will be classified according to content. These tapes will retain a minimum classification of CONFIDENTIAL until erased or degaussed using an approved device from the listing in AR 380-380.

COMSEC monitoring working material will be destroyed, erased, or degaussed after the supported commander reviews and approves the final report, or 45 days after production, whichever is sooner.

COMSEC monitoring may be divided roughly into two categories: Conventional Telephone (CT) Monitoring and Radio-telephone (RT) Monitoring. Although the requirements and restrictions are similar for each category, there are differences. These two categories will be discussed in turn.

Use of Conventional COMSEC Telephone Monitoring Tapes for Training Purposes. The use of actual COMSEC CT monitoring tapes for training purposes within the monitoring unit is prohibited. The COMSEC unit may make its own training tapes based on actual COMSEC problems noted during monitoring if names or other data sufficient to identify individuals who participated in monitored telephone conversations are excluded.

COMSEC Radio-telephone Monitoring

The basic restrictions and policies concerning use, dissemination, classification, and destruction of working materials and controls for monitoring equipment specified for CT monitoring also apply to RT monitoring with the exceptions and differences discussed below. In general, where policies differ between CT and RT, those for RT are more lenient. RT monitoring is limited to frequencies or channels totally dedicated to DOD. These provisions preclude monitoring amateur and CB radio transmissions. As with CT monitoring, only persons trained in COMSEC monitoring duties and awarded a SIGSEC military occupational specialty are authorized to install and operate COMSEC RT monitoring equipment. This policy does not prevent non-SIGSEC personnel from monitoring a transmission by using a tactical voice radio when authorized by their commander as part of his unit's self-monitoring program.

Self-Monitoring Program. Commanders are urged by AR 530-2 to establish self-monitoring programs for tactical voice radio nets under their control. Self-monitoring allows the commander to enforce radio net discipline and use of proper radio procedures. So long as non-SIGSEC personnel and equipment are not used, the commander may monitor any transmission in his organization.

Use of COMSEC Monitoring Tapes for Training Purposes. COMSEC RT monitoring tapes may be used within the monitored unit for training. However, the tapes will not be released outside the COMSEC monitoring unit. Although not prohibited, the use of monitoring tapes is discouraged because of the possibility of violating the privacy act and mishandling or compromising information obtained through COMSEC monitoring. If possible, the COMSEC unit should make its own training tapes based on actual COMSEC problems noted during monitoring.

PENALTIES FOR ILLEGAL ELECTRONIC SURVEILLANCE

The current federal statute governing electronic surveillance is Title III of the Omnibus Crime Control and Safe Streets Act of 1968 (18 US Code sections 2510-2520).

Criminal Penalties

Section 2511 specifies that any person who willfully intercepts, endeavors to intercept, or procures any other to intercept or endeavor to intercept, any wire communication illegally, or who willfully discloses or uses, endeavors to disclose or use, or endeavors to use the contents of any wire communication illegally obtained shall be fined no more than $10,000 or imprisoned for not more than five years, or both.

Civil Penalties

Section 2520 authorizes any person whose wire communication is illegally intercepted, disclosed, or used, to take civil action against the person who illegally intercepted, disclosed, or used, or procured another person to illegally intercept, disclose, or use such communication; and to recover damages at the rate of $100 per day for each day of violation, or $1,000, whichever is higher, plus punitive damages, plus attorney's fees, and other litigation costs reasonably incurred.

PRACTICE EXERCISE 1

This exercise is to be worked after you study the lesson. After you complete the exercise, check your answers with the solution sheet.

1. You are in charge of a SIGSEC monitoring team. SP4 Jones of your team has asked you why there were so many restrictions placed on eavesdropping and monitoring activities. All these restrictions just make it harder to do the job. What is your answer?

_____

_____

2. Which of the following is the definition of a consensual intercept?

   a. None of the parties to a conversation is aware of the intercept.

   b. All of the parties to a conversation are aware of the intercept.

   c. At least one party to a conversation is aware of the intercept.

   d. Only one party to a conversation is aware of the intercept.

3. Who is the final approval authority of a nonconsensual interception of communication for law enforcement purposes conducted overseas?

   a. The commander of the MACOM exercising authority over the law enforcement unit.

   b. The Army General Counsel.

   c. The Secretary of the Army.

   d. The military judge who issues the court order.

4. Chapter 3, AR 381-10, governs electronic surveillance activities. What does it also cover?

   I COMSEC activities

   II SIGINT activities

   a. I only.

   b. II only.

   c. Both I and II.

   d. Neither I nor II.

5. Electronic surveillance of which of the following listed personnel does NOT require prior approval of the Secretary or Under Secretary of the Army? (THERE MAY BE MORE THAN ONE CORRECT ANSWER; CHOOSE ALL CORRECT ANSWERS.)

   a. SP5 James Quincey, stationed in Munich, Germany.

   b. Helmut Goering, a German citizen who works in the PX in Munich, Germany.

   c. Hans Braun, a German soldier assigned to liaison duties with the US Army in Munich, Germany.

   d. Barbara Stein, a German tourist in the US.

   e. George Nelson, a retired LTC, US Army, who lives in Germany.

6. What are the three questions that must be asked in order to determine which set of standards is to be applied for approval of electronic surveillance?

   _____

   _____

   _____

7. In addition to COMSEC monitoring, for what may COMSEC telephone monitoring equipment be used?

   a. Operations center monitoring.

   b. Intercepts for law enforcement purposes.

   c. Electronic surveillance for intelligence purposes.

   d. No other monitoring functions.

8. Who may install and operate COMSEC monitoring equipment?

   _____

9. For what reasons may someone, not SIGSEC-trained, who has direct management authority over a SIGSEC monitoring team, have access to monitoring working materials?

   _____

10. The commander of the supported unit requests the tapes of your COMSEC telephone monitoring of his unit so he may determine whether anyone in the unit used official telephones to make unauthorized AUTOVON calls. Are you allowed to provide him these tapes?

    a. No, because the request was not COMSEC-related.

    b. No, because he is not allowed access to the tapes under any circumstances.

    c. Yes, so any persons so using the telephones can be identified and punished.

11. While monitoring a telephone conversation, SP4 Robinson, the SIGSEC specialist who works for you, hears, during an otherwise official conversation, one party tell the other how to gain access to a house of prostitution. He asked you whether the Military Police should be notified. What is your answer and reason?

    _____

    _____

12. The commander of one of the units you support has asked to borrow your radio-telephone monitoring equipment so he may conduct a tactical radio self-monitoring program while his unit is in the field. What do you do?

    a. Loan him the equipment, but do not supply any personnel.

    b. Loan him the equipment, but have a SIGSEC specialist accompany the equipment to the field to install it.

    c. Do not loan him the equipment because even if a SIGSEC specialist would install it, the supported unit does not know how to operate it.

    d. Do not loan him the equipment because only SIGSEC specialists are permitted to use it.

PRACTICE EXERCISE 1 SOLUTIONS

1. You should explain to SP4 Jones the restrictions are designed to preserve the rights of people to be secure against unreasonable searches and seizures under the Fourth Amendment to the US Constitution (page 763-2).

2. c (page 763-4).

3. d (page 763-5).

4. d (page 763-5).

5. b and c (page 763-6).

6. Is the surveillance within or outside the United States? Is it directed against a US person? Is it consensual or nonconsensual? (page 763-8).

7. d (page 763-6).

8. Only personnel trained in COMSEC monitoring duties and who have been awarded a SIGSEC MOS (pages 763-11).

9. Supervising, directing, and checking on the regulatory compliance and mission effectiveness of SIGSEC monitoring personnel (page 763-10).

10. a (page 763-11).

11. The MPs should not be notified because the only times COMSEC monitoring may be used for law enforcement purposes are in the event of security violations and information obtained incidentally during an authorized COMSEC monitoring that relates directly to a significant crime (pages 763-10 and 11).

12. d (page 763-10).

LESSON 2

COMSEC MONITORING EQUIPMENT

OBJECTIVE:

Task: At the end of this lesson you will be able to identify the major components of COMSEC monitoring equipment.

Standard: You will complete the practice exercise to 100 percent accuracy.

REFERENCES:

TM 32-5805-201-14P, Telephone Monitoring Set AN/TTR-1A, Dec 80
TM 32-5895-263-14P, Monitoring Set, AN/TRR-33, May 80

OFFICER'S TASKS:

01-3352.06-0500, Conduct COMSEC M&A Mission
01-3352.06-0531, Open a COMSEC Account
01-3352.06-0532, Administer a COMSEC Account

INTRODUCTION

One of the most important functions a SIGSEC support element performs is COMSEC monitoring. To conduct such a mission, the SIGSEC element must be able to use the various types of monitoring equipment which it is issued. Therefore, as an officer who may be in charge of a SIGSEC element during your career, you must know the equipment, its capabilities and limitations.

AN/TRR-33 RADIO-TELEPHONE MONITORING SET

The AN/TRR-33 radio-telephone monitoring set is a tactical communication monitoring system designed to receive and record transmitted AM and FM radio frequency signals from 0.5 to 157.5 megahertz (MHz). It can monitor voice communication and telegraphy.

Under Army of Excellence the AN/TRR-33 is not organic at echelon corps and below.

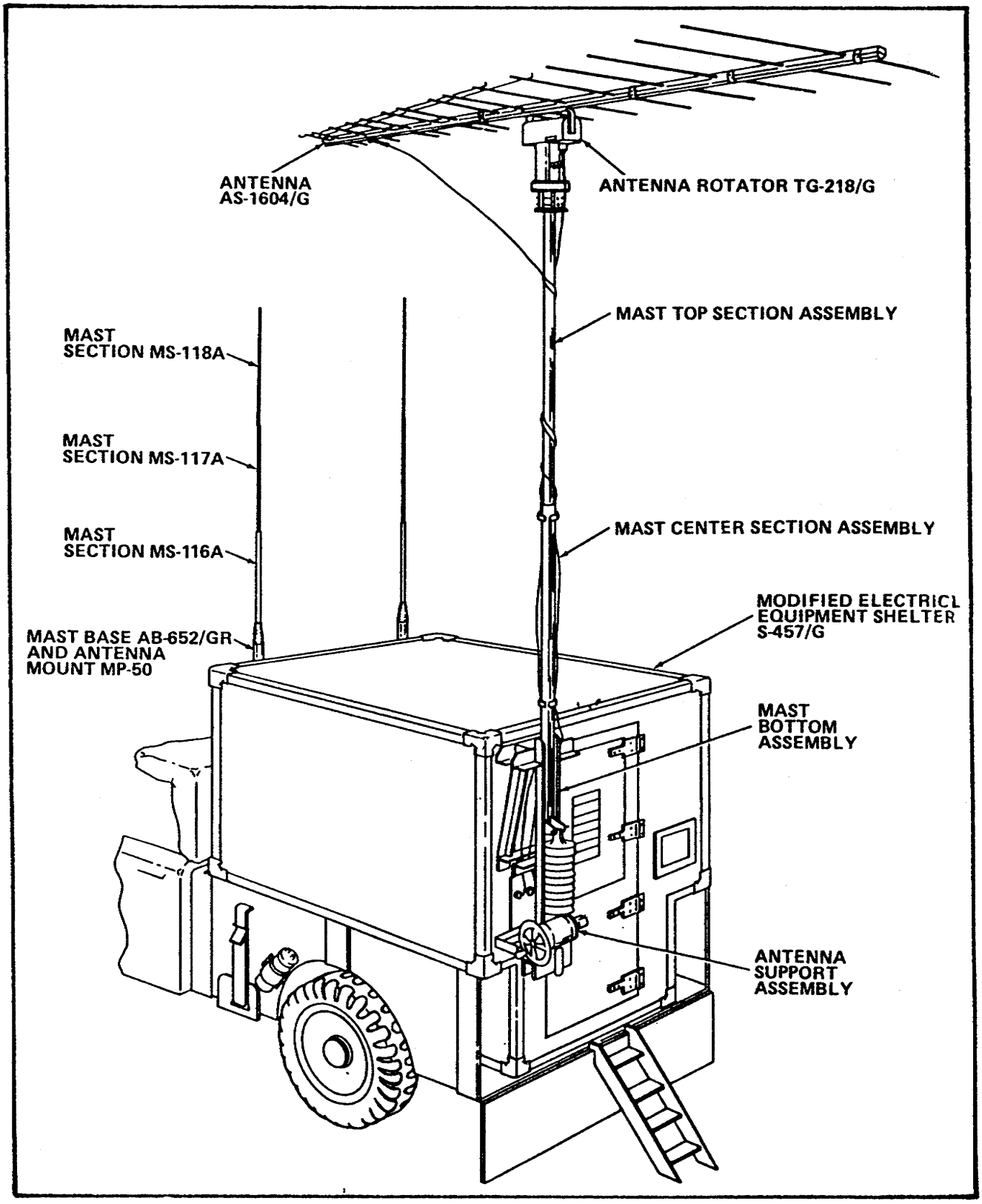

Figure 2. AN/TRR-33 Exterior View.

Components

- Exterior (see figure 2). The AN/TRR-33, with the exception of the auxiliary Antenna Equipment RC-292, is contained in Electrical Equipment Shelter S-457/G which has been modified externally and internally to accommodate the components. It is normally mounted in a 1-1/4 ton truck, M880 series. However, in some units it is mounted in a gamma goat. The equipment is powered by 120-volt, single-phase, 60-Hz commercial power or a trailer-mounted Generator Set PU-620/M. The auxiliary RC-292 antenna is erected near the shelter, with the distance separating the shelter and antenna limited by the Radio Frequency Cable Assembly CG--107A/U which connects the antenna base at the top of the mast to the signal entrance box on the shelter.

The antenna structure assembly of the AN/TRR-33 is attached to the rear of the shelter, together with the mast top and center section assemblies which support Antenna Rotator TG-218/G. The antenna rotator serves as a mounting base for a undirectional AS-1604/G antenna.

Two antenna mounts, MP-50, are on the front of the shelter support omni-directional whip antennas, each of which consists of mast base AB-652/GR and mast section MS-116A, MS-117A, and MS-118A.

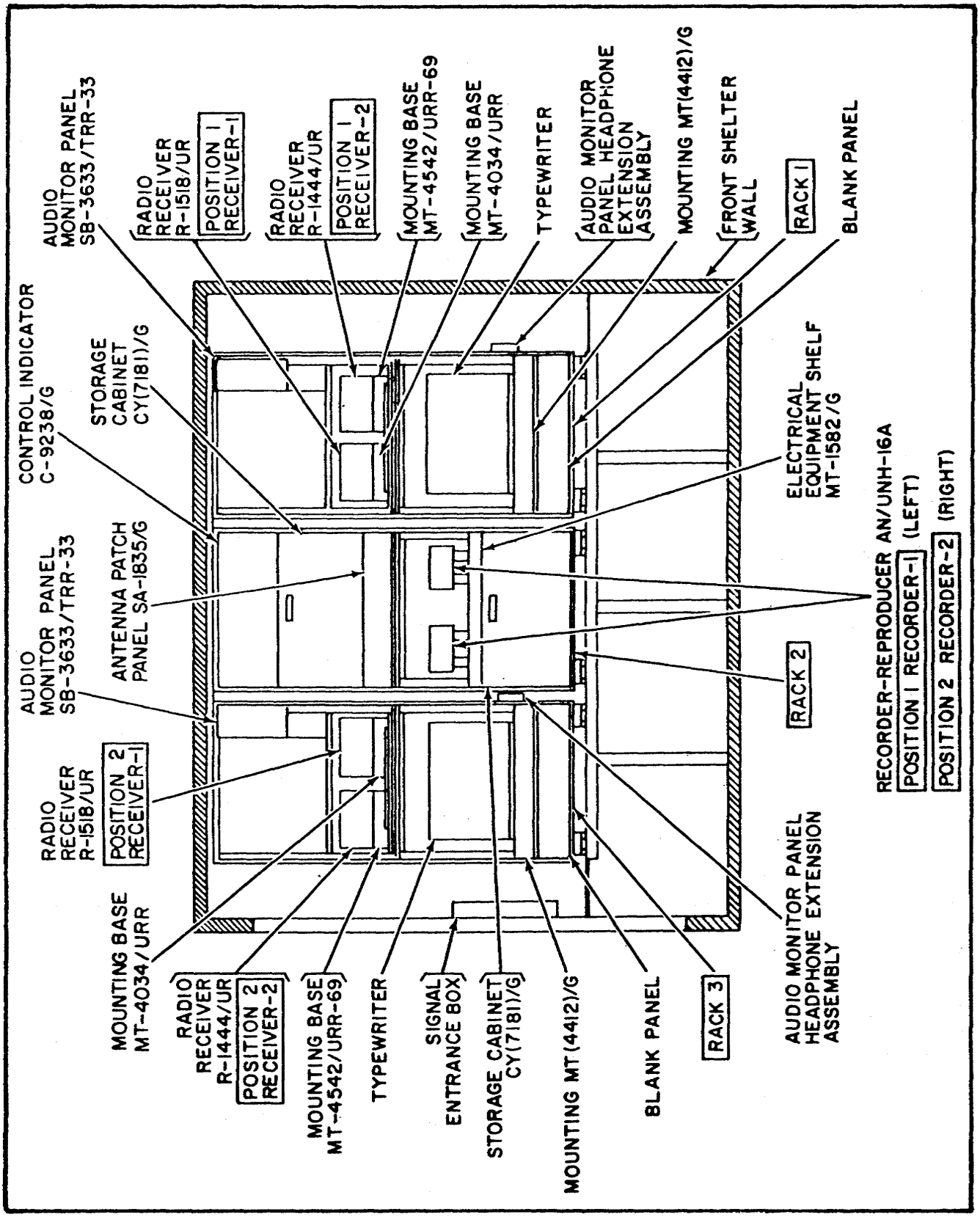

Figure 3. AN/TRR-33 Interior Roadside View.

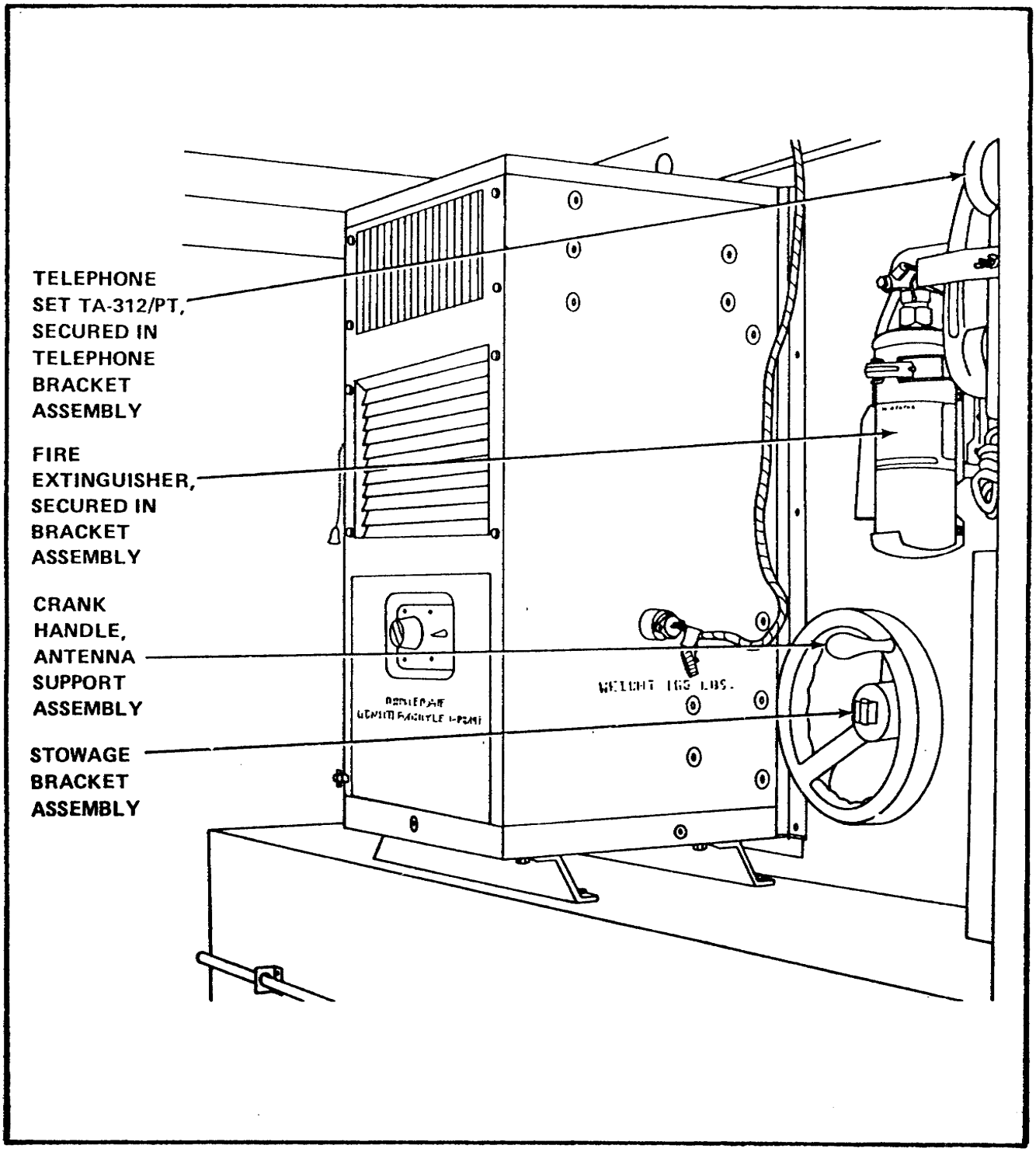

Figure 4. AN/TRR-33 Interior Rear Curbside View.

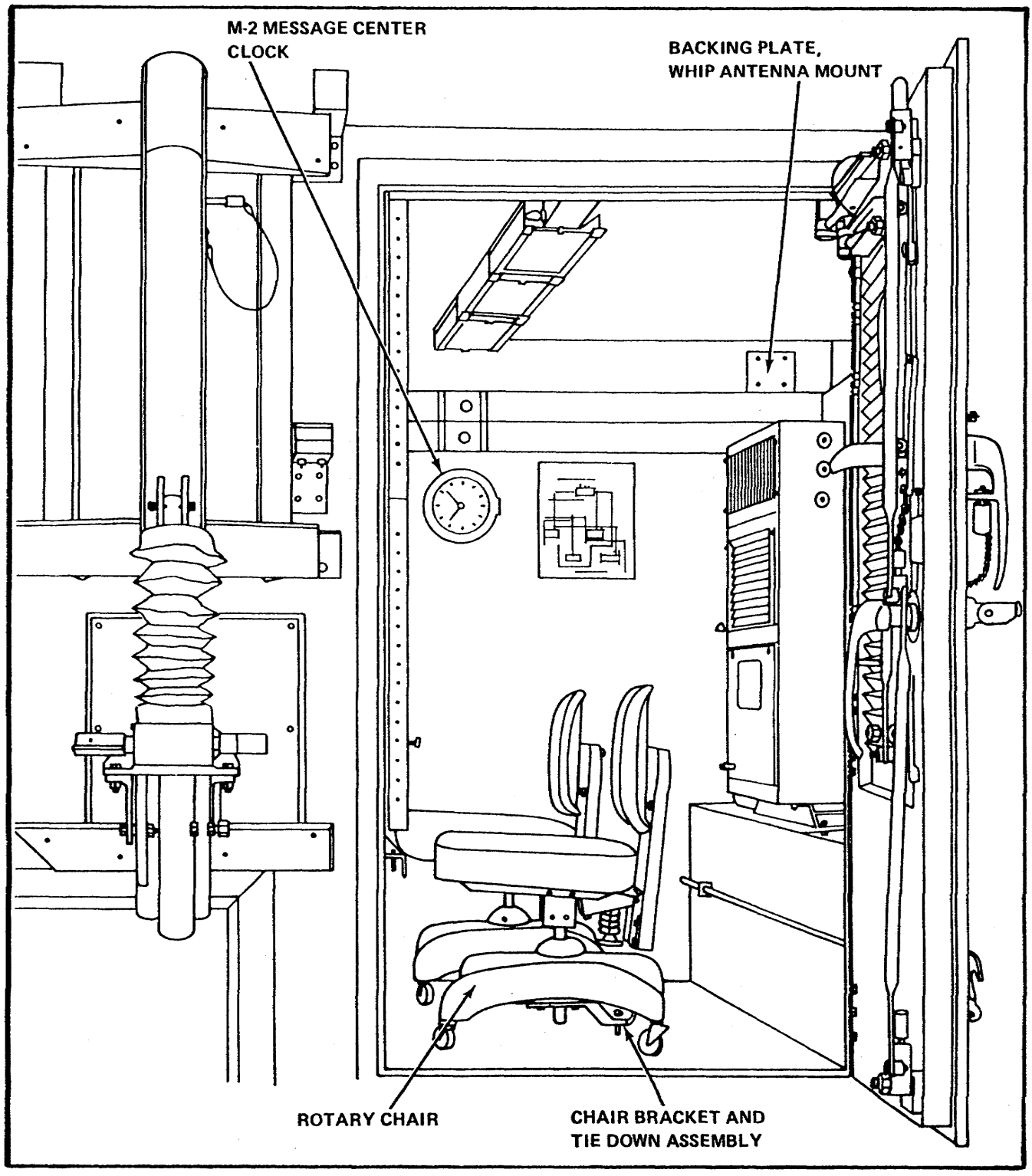

Figure 5. AN/TRR-33 Interior Front View.

- Interior (see figures 3, 4, and 5). The AN/TRR-33 contains two identical monitoring positions, each of which can be operated independently. Both positions share components such as antennae and power supplies. Those components which are not shared are in pairs, one for each monitoring position. Interior shelter components include two rotary chairs with attached brackets and tiedown assemblies and an eight-day, M-2 message center clock mounted on the front wall alongside an equipment cabling diagram.

At the top of the front wall, above the electrical wiring raceways, are backing plates for the whip antenna mounts. Radio frequency cabling is routed counterclockwise around the shelter from these backing plates to the rack-mounted antenna patch panel. An air-conditioning and heating unit is provided with the shelter; the control box is on the curbside toward the rear of the shelter. A fire extinguisher is located forward of the control box. The shelter is equipped with a TA-312/PT Telephone Set for land line communication.

Six rack assemblies, include DC and AC power connector sets, are provided with the shelter. These assemblies are arranged in three racks and secured to the shelter and a supporting bracket. Racks 1 and 3, which are identical, are the two monitoring positions. Equipment common to both positions and the recorder-reproducers for the two positions are in rack 2.

Antennae. The AN/TRR-33 uses three types of antenna systems, totaling four antennae.

- The unidirectional AS-1604/G antenna, mounted on the rear of the shelter, receives signals in the 50-1100 MHz frequency range.

- Two omnidirectional whip antennae, mounted on the front of the shelter, receive signals from 3 to 300 MHz, thereby covering the HF and VHF bands.

- An RC-292 antenna is an elevated, modified ground plane antenna designed to increase the range of selected radios. It is an omnidirectional antenna with a frequency range of 20-76 MHz.

Receivers. Each monitoring position has two radio receivers:

- An R-1444 receiver, which is a solid state HF receiver capable of monitoring continuous wave (CW), frequency shift keying, upper and lower sideband, AM, and FM transmissions at frequencies from 0.5 to 30 MHz. The set can be used from fixed sites, vehicular installations, or as a manpack radio. It can be powered by 230 volt AC, 115 volt AC, or 24 volt DC external power sources or from internal batteries. SIGSEC personnel use the R-1444 primarily to monitor single side band (SSB) and AM voice signals. The CW capability is not used because SIGSEC personnel are not trained to copy code. The FM function is not used because military FM radios operate at frequencies higher than the R-1444's range.

- The R-1518 receiver is capable of receiving AM, FM, and CW transmissions from 19 to 157.5 MHz. This radio can operate from fixed sites, vehicular installations, or as a manpack radio. It uses the same power

sources as the R-1444. It is used primarily for monitoring FM transmissions.

Recording Devices. The AN/TRR-33 can be equipped with either AN/UNH-16A or AN/PNH-4 recorders. Only one type will be in a given AN/TRR-33. The AN/UNH-16A is the newer model and gradually replacing the AN/PNH-4.

- The AN/UNH-16A Recorder-reproducer is a miniature, two-channel, four-track unit that uses a cassette operating at a speed of 15/16 inches per second. Total operating time is more than two hours per tape. It operates on 12 volts DC, but has a plug-in power supply which allows it to be used with 110-220, volts AC or 24-volt DC power sources. It has a microphone to allow operator comments on the tape.

- The AN/PNH-4 is a self-contained, portable, battery operated, tape recorder-reproducer which uses 1/4 inch tape reels and operates on external 24-volt power or from internal batteries.

Other. The AN/TRR-33 also contains two telegrapher's mills, one for each position. These mills are used by the operators to copy transmissions as they are monitored.

Equipment Use

When setting up a monitoring site, either or both of the positions in the AN/TRR-33 may be used. Any of the antennae may be used in any combination with any of the radios provided the radio and antenna operate on the same portion of the radio frequency spectrum. If desired, two or more radios can share the same antenna. The antenna/radio connections are made with an antenna patch panel. The cables from the individual antenna are connected to the back of the antenna patch panel on the left side. The receivers are connected on the right side. Using the connecting cables, any antenna can be connected to any receiver. Or, an antenna can be shared by two or more receivers simply by connecting the antenna to the appropriate antenna splitter input and connecting the outputs to the desired receivers. If either of the antenna splitters is used, the power switch in the center of the antenna patch panel must be placed in the "on" position.

Once the equipment is set up and checked out, the monitoring mission can begin. The operator is given a frequency or set of frequencies to monitor and tune the equipment accordingly. When he receives a transmission, he uses either a foot switch or a toggle switch on the equipment rack to activate the recorder and record the conversation. At the same time, he copies the traffic on the telegrapher's mill using an abbreviated copy format which allows a good operator to keep up with the fastest net. As soon as there is a break in the traffic he will highlight any COMSEC discrepancies noted in the traffic. This highlighting is called message analysis. Generally, all analysis is done from the hand copy taken by the operator. The tape serves as a back-up in case the operator misses a segment of the conversation.

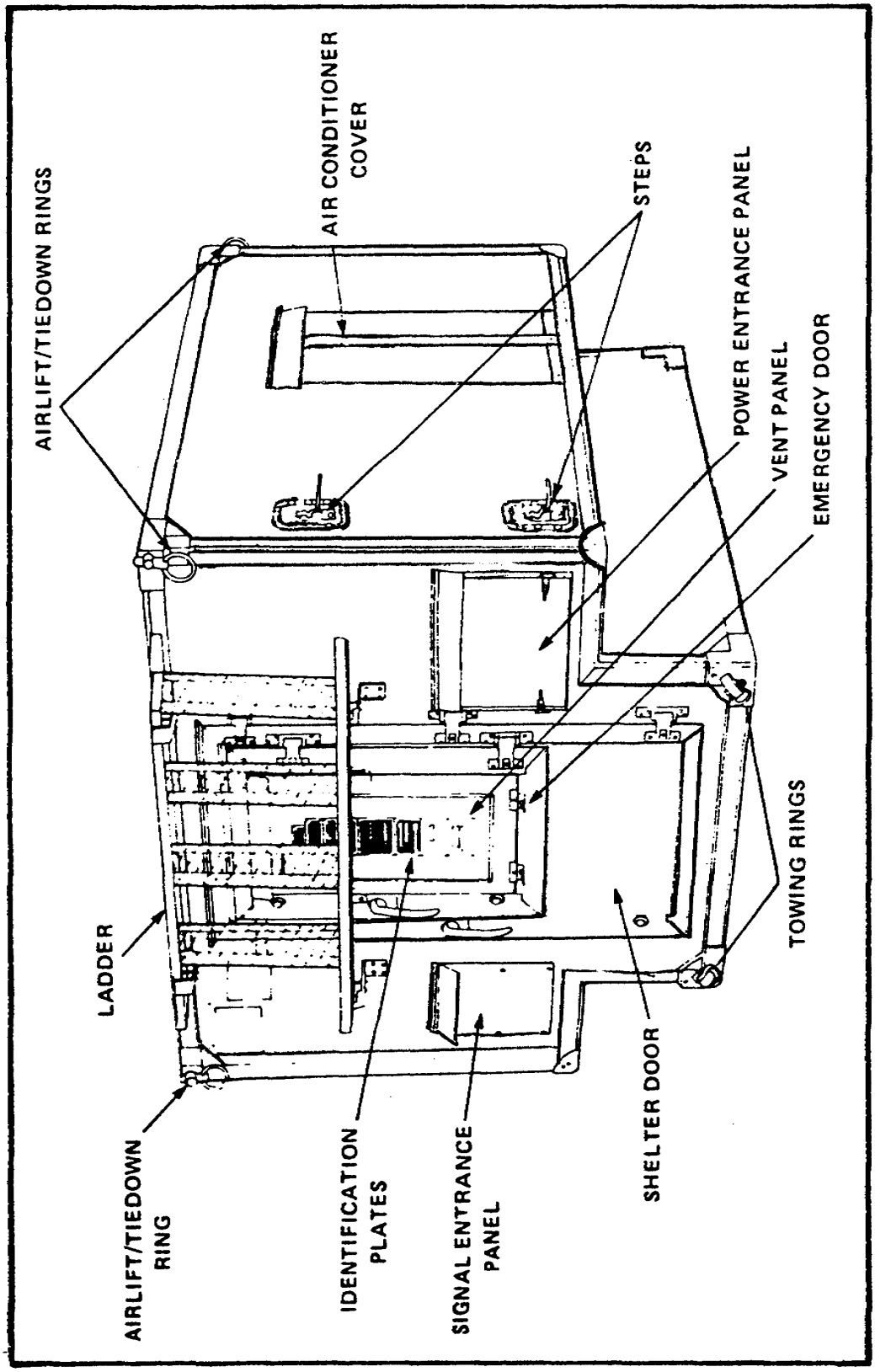

Figure 6. AN/TTR-1A Exterior View.

AN/TTR-1A TELEPHONE MONITORING SET

The AN/TTR-1A is a land line, voice-frequency system capable of monitoring a maximum of 26 lines or trunks. The set is housed in an S-457 shelter mounted on a 1-1/4 ton truck, M880 series. It requires 120 volt AC, 60-hertz power from either a commercial source or a PU-620/M generator. An exterior view of the shelter is shown in figure 6. The AN/TTR-1A equipment requires at least the minimum degree of protection of SECRET.

Components

The Telephone Monitoring Set consists of two Digit Display Indicators (ID-1682), two Audio Frequency Monitors (TA-836), two Monitor Switching Panels (SB 3216), four AN/PNH-4 Recorder-Reproducers, two 15-foot, 26-pair cables with telephone hocks, or connectors, on one end and pigtails on the other, two 250-foot 26-pair cables with hocks on each end, and two distribution boxes (J-1077).

There are auxiliary items such as chairs, a typewriter, and an air conditioner, as in the AN/TRR-33. As can be deduced from the above listing of the equipment, the AN/TTR-1A is two monitoring stations in one shelter. Within the constraints of equipment location and cable length, two switches may be monitored at the same time. These items of equipment are illustrated in figure 7.

Under Army of Excellence the AN/TTR-1A is not organic at echelon corps and below.

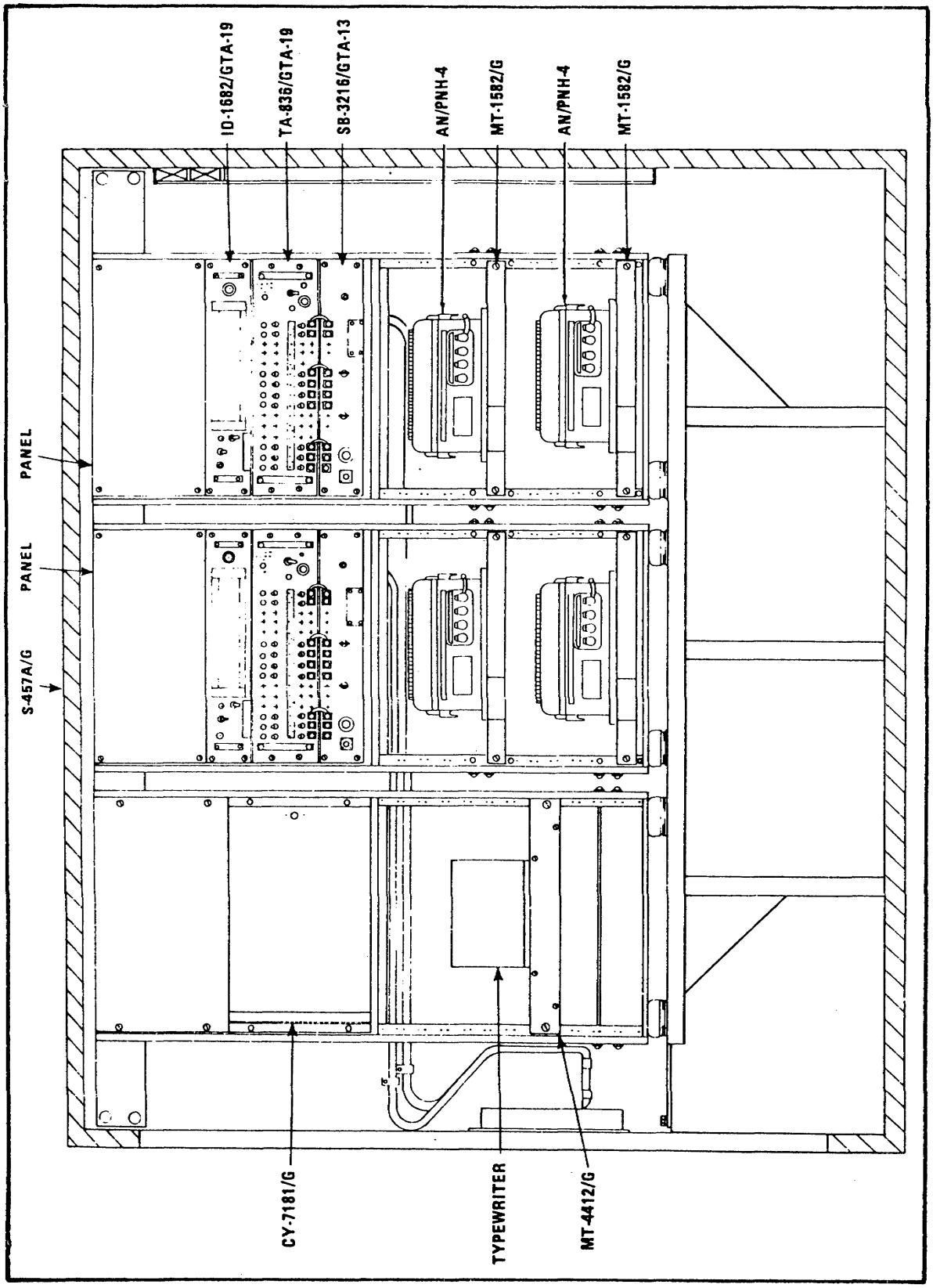

Figure 7. AN/TTR-1A Left Side Rack Mounted Components.

Digital Display Indicator. The digital display indicator (DDI), can receive two- and four-wire inputs from up to 15 monitored lines. It displays numbers dialed from a dial telephone or keyed from a touch-tone telephone. On the back of the DDI, there are 15 toggle switches used to set each circuit for either two-wire or four-wire operation. Although the DDI is capable of monitoring 15 lines, the cable, being a 26-pair conductor, is limited to 13 lines. Therefore, an AN/TTR-1A is limited to monitoring a maximum of 26 lines.

Audio Frequency Monitor. The audio frequency monitor has 15 channels, each connected through the monitor switching panel to the recorders, allowing the operator to listen to any one line without disturbing the recording of the conversation. The back of the audio frequency monitor contains 15 input mode selector switches, which adjust the circuitry to match the line voltage of the circuit to be monitored. These switches, which are adjusted by a small, flat screwdriver, have four positions:

- Military ringdown line.
- 24-volt.
- 48-volt.
- 60-volt.

The military ringdown line setting is used for all four wire lines. Generally, a dial telephone has two wires and a tone telephone has four wires.

Monitor Switching Panel. The monitor switching panel is used to select the circuit to be recorded.

Installation and Operation

Installation. Basically, the AN/TTR-IA is connected to the local telephone distribution frame using the 26-pair cables. However, connecting this equipment to one particular telephone system demands critical care. This system is the tactical automatic switch (TAS). The TAS is a multimillion dollar computerized system located at corps and higher echelons. There are three main precautions to remember regarding a TAS hookup:

- Always use a common power source.
- Always use a common ground.
- Always have the TAS wireman hook up your lines to the TAS system.

If you don't use the same power and ground as the TAS, you will probably be asked to disconnect your set. The TAS system is so sensitive it will function properly only when all equipment connected to it is powered by the same source and connected to the same ground.

Operation. After the equipment is connected and operational, the operator is ready to monitor telephone calls. Assume the division G2 plans officer's telephone is connected to line 7 of the monitoring equipment. When he lifts the telephone receiver, the telephone generates an "off hook" signal. The signal is picked up by the audio frequency monitor and activates an audible alarm to alert the operator there is an off-hook condition on one of the monitored lines. It simultaneously causes the dialed number indicator lamp at line 7 to glow, telling the COMSEC operator which line is active. When the number is dialed or keyed, the outgoing pulses are picked up, decoded, and the numbers listed on the DDI. By that time, the operator will have turned the line selector switch to position 7.

Once the connection is made, the operator will listen for a few seconds to determine whether he can legally monitor and record the telephone call. To make this determination, he uses the criteria presented in lesson 1 of this subcourse. If the call may be monitored, the operator will turn the appropriate recorder selector switch to position 7 and record the call. He will include identifying data and a summary of the conversation on the monitor log sheet. If a call cannot be monitored, the operator immediately stops listening, turns the line selector switch to the neutral position, and awaits the next call.

FLY AWAY KIT

The "Fly Away Kit" is one-half of an AN/TTR-1A mounted in a case that can be carried by two people. It can fit in the cargo compartment of a commercial aircraft, hence the nickname. It consists of one bank of an AN/TTR-1A minus the monitor switching panel. It can monitor up to 15 lines and has the same capabilities as the full AN/TTR-1A, and functions in the same manner subject to the limitations of being only one bank, not having the monitor switching panel, and not being in a shelter. Due to its nature, it is not suited to a tactical mission, and therefore found nearly exclusively in USAINSCOM units. Also, because it is dismounted from the AN/TTR-1A, there are many varieties of tape recorders used with it.

AN/GRR-8

The AN/GRR-8 (Watkins Johnson) is a portable, manpack tactical radiotelephone receiver capable of monitoring voice radio AM and FM signals from 0.5 to 500 MHz. It is composed of a WJ-8640 receiver and a WJ-9180-1 signal monitor. It is capable of operating from 115 volts, alternating current (VAC) or 24 volts, direct current (VDC) power, and has a battery pack containing a recharger unit that operates off a 115/230 VAC power source.

Also, it has a detachable battery pack which uses BA 4386 magnesium battery (the same battery used in the AN/PRC 77) or D cell alkaline or Nickel-Cadmium batteries. D cells are the same size as BA 30 batteries.

The Watkins Johnson receiver has three interchangeable tuning heads:

- 0.5-30 MHz.
- 20-250 MHz.
- 250-500 MHz.

The other major part of the AN/GRR-8, the WJ-9180-1 Signal Monitor, displays a visual spectrum of the signal activity around the tuned frequency, allowing the operator to fine-tune the desired more precisely. The WJ-9180-1 is not necessary for the operation of the AN/GRR-8, but does allow the operator to see the frequency band in the vicinity of the tuned frequency and therefore tune to a signal more accurately. The Watkins Johnson is an "off the shelf" item; that is, the Watkins Johnson Company did not build it under government contract. It was built first, then sold to the government. It is intended to replace the AN/TRR-33.

OTHER EQUIPMENT

AN/TYK-1OA. The AN/TYK-1OA is a data analysis central position used to transcribe recorded voice signals collected by the monitor positions. It is equipped with two recorder-reproducers (either AN/PNH-4 or AN/UNH-16A, depending on which is used in the monitoring positions) and two telegrapher's mills. It is contained in an S-457 shelter mounted on a 1-1/4 ton truck, M4880 series, and takes its power from either a commercial 115 VAC source or from the PU-620/M generator set.

AN/TYQ-5. The AN/TYQ-5 Data Analysis Central Position is used for control and analysis of data received from the collection positions. It is mounted either as one of three shelters on a low bed trailer as part of a MSA-3A or separately on a 5-ton truck. It requires 10 kilowatts of power.

PRACTICE EXERCISE 2

This exercise is to be worked after you study the lesson. After you complete the exercise, check your answers with the solution sheet.

SITUATION: You are the platoon leader of the SIGSEC Platoon, Co B, (OPSEC), 199th MI Bn (TE), 555th Mi Group (CEWI). Your platoon has been recently activated and all your SIGSEC operators and analysts are recent graduates. SFC Smith, your platoon sergeant, is on leave, so he is not available to assist the members of the platoon. Your platoon is preparing for a monitoring mission in support of a corps command post exercise.

1. PFC Johnson has forgotten how to set up the antennae for the AN/TRR-33. Which antenna should he set up on the rear of the shelter?

   a. AS-1604/G.

   b. Whip antenna.

   c. RC-292.

   2. Which receiver should SP4 Murphy use to monitor FM transmissions?

   a. R-1444.

   b. R-1518.

3. When SP4 Murphy receives a transmission, he should begin to record it. What else should he do?

   a. Copy it on the telegrapher's mill.

   b. Copy it on the typewriter.

   c. Copy it only if he hears COMSEC discrepancies.

   d. Copy it only if it is on a DOD or DA circuit.

4. The OPSEC staff office has given you a list of 35 telephone lines to be monitored during the exercise. You realize your AN/TTR-1A is not capable of monitoring this many lines. How many lines can your equipment monitor?

   a. 13.

   b. 15.

   c. 26.

   d. 30.

5. SP4 Goldberg will be operating the AN/TTR-1A. When he monitors a telephone call, what should he do?

   a. Immediately start recording and copying it.

   b. Start copying it, but not record it until he hears a discrepancy.

   c. Listen for a few seconds to determine whether he should monitor the conversation.

   d. Start recording it, but not copy it until he hears a discrepancy.

PRACTICE EXERCISE 2 SOLUTIONS

1. a (page 763-20)

2. b (page 763-24).

3. a (page 763-25).

4. c (page 763-27)

5. c (page 763-30).