DEPARTMENT OF THE AIR FORCE
Headquarters US
Washington DC 20330-1680

Air Force Qualification
Training Package 2EXXX-202D
1 October 1999

EI Tempest Installation Handbook
(2EXXX Communications-Electronics Specialties)

1. This Air Force Qualification Training Package (AFQTP) standardizes on-the-job training (OJT) and constitutes an approved training program for installation of Tempest equipment, cables, and grounding systems. The AFQTP is used to familiarize the EI Team Chief and members with procedural installation of equipment requiring emission security controls.

2. Review Air Force publishing bulletins and AFIND8 to identify other available training materials. Use this AFQTP in conjunction with other applicable Job Qualification Standards (JQS) or the Career Field Education and Training Plan (CFETP) and locally assigned tasks to identify work center duty positions. Also, use this AFQTP along with other applicable JQSs and the CFETP to evaluate newly assigned personnel and identify individual training requirements.

3. Submit recommended AFQTP improvements/corrections to the 81 TRSS/TSQS, 601 D Street, Keesler AFB, MS 39534-2229.

BY ORDER OF THE SECRETARY OF THE AIR FORCE

OFFICIAL

JOHN W. HANDY, Lieutenant General, USAF
Deputy Chief of Staff/Installations and Logistics

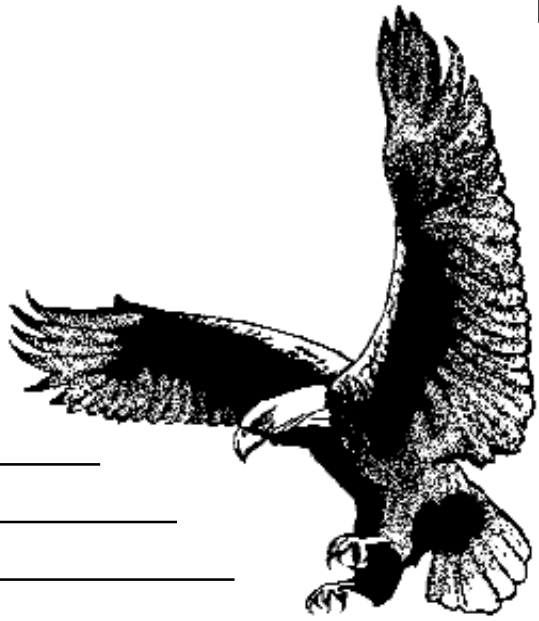
1 Atch
Handbook

---

Supersedes AFQTP 2EXXX, dated 21 May 1998
OPR: HQ USAF/ILMM
OCR: 81 TRSS/TSQR
DISTRIBUTION: X

# *AIR FORCE QUALIFICATION TRAINING PACKAGE 2EXXX-202D*

# EI TEMPEST INSTALLATION HANDBOOK



**1 OCTOBER 1999**

**SUPERSEDES AFQTP 2E0X0-202D**
**DATED 21 MAY 1998**

**FOR OJT USE ONLY**

## CONTENTS

Preface ii
About This Training Package ii
Chapter 1, Introduction to EMSEC
Chapter 2, Spacing
Chapter 3, Wire Way Installation
Chapter 4, Cable Installation
Chapter 5, Equipment Installation
Chapter 6, Grounding and Bonding
Chapter 7, Pre-Shakedown Inspection
Chapter 8, Team Chief Duties

## PREFACE

This handbook is intended for use by Air Force Communications Electronic Engineering Installation (EI) personnel. It provides guidance on the installation of C-E equipment in an environment where emission security (EMSEC) is a consideration IAW RED/BLACK installation criteria. It is primarily designed for the inexperienced EI team member and Team Chief who are unfamiliar with TEMPEST-related installations. Team Chiefs who are familiar with EMSEC and RED/BLACK installation criteria can use the handbook as a reference guide and as a tool to train team members. This handbook does not deal with Standard Installation Practices. Rather it explains the fundamentals and concepts behind EMSEC and RED/BLACK installation criteria. Formal installation training is provided by each EI unit. EI trainers use AFJQS 2EXXX-202B, Standard Installation Practices—Electronics/Inside Plant, to plan, conduct, and document qualification training.

Contents of the handbook are NOT to be used as a basis for inspection or evaluation. This handbook is a specialized publication for familiarization and training purposes only; it is NOT a technical reference.

## ABOUT THIS TRAINING PACKAGE

This training package was originally developed by TSgt Edward L. Hamilton and revised by SSgt Kevin Banks, 81 TRSS Qualification Training Flight, Keesler AFB, MS. The Training and Education Specialist was Mr. Tom Vuncannon. It was initially validated by 485 EIS, Griffis AFB, NY; 738 EIS, Keesler AFB, MS; HQ AFC4/DSS, Scott AFB, IL; and HQ AFCSC/SRM, Kelly AFB, TX. MSgt Allen Thomas, 738 EIS, Keelser AFB, MS, was consulted as the Subject Matter Expert.

For more information on the 81 TRSS Qualification Training Flight and a list of other products that are available, feel free to visit our home page at http://www.keesler.af.mil/81trss/qflight.

# CHAPTER 1
# INTRODUCTION TO EMISSION SECURITY (EMSEC)

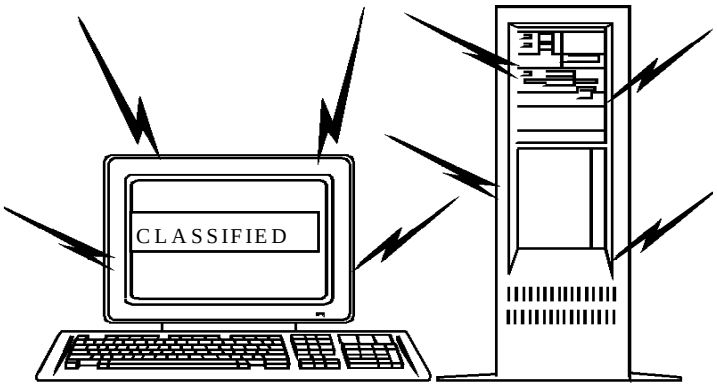
## EMSEC

EMSEC is a short unclassified name referring to investigation and studies of compromising emanations and is comprised of TEMPEST, NONSTOP, and HIJACK. It also refers to those measures used to control compromising emanations. EMSEC is interrelated to the RED/BLACK concept which requires that electrical and electronic components, equipment, and systems processing classified plain text information be kept separate from those that process encrypted or unclassified information. The whole idea of EMSEC and RED/BLACK concept is to prevent or reduce the effects of **compromising emanations.**

Compromising emanations (CE) are unintentional, intelligence-bearing signals which, if intercepted and analyzed, disclose classified information transmitted, received, handled, or otherwise processed by any information-processing equipment.

## EMANATIONS

Emanations are unintended signals or noises appearing external to C-E equipment as information is being processed. Every electronic or electromagnetic device, whether or not designed as a transmitter gives off some electromagnetic signals or emanations. Proper design minimizes emanations given off by a device, but some will always be present.




When a device processes voice or data, it may "leak" information through emanations. An example would be “cross-talk” on

telephone lines where signals leak from one line to another and another person's voice intrudes on your phone call. If strong enough, information-bearing emanations may travel through the air, plumbing, wires, and ventilation systems to areas where enemy agents could recover them. If the signals contain classified information and are intercepted, this information may fall into enemy hands. The potential for compromise exists wherever classified information is processed.

A radio can produce emanations. Does this fall under compromising emanations? Not necessarily. If you remember, compromising emanations refer to classified signals. Most radios that transmit classified information carry encrypted signals. In order for emanations to be compromised, they must be carrying classified information that is not yet encrypted. If the emanations are not carrying classified information or have already been encrypted, then they are not compromising emanations.

## TERMS

Let's take a look at some of the terms used with EMSEC. EMSEC has a language unique to itself. The following are some of the EMSEC-related terms you should be familiar with.

### NATIONAL SECURITY INFORMATION

Information that's been determined, pursuant to Executive Order 12356 or any predecessor order, to require protection against unauthorized disclosure and is so designated. This includes all classified and/or sensitive information as set forth in 10 U.S.C. Section 2315 (Warner Amendment). The Warner Amendment applies to information which is unclassified but which involves intelligence activities, cryptologic activities, command and control of military forces, weapons systems, or is critical to the direct fulfillment of military or intelligence missions.

### BLACK

As it pertains to C-E equipment, transmission lines, and associated wiring, BLACK signifies both physical and electrical areas where data/voice signals are encrypted or unclassified and therefore relatively safe from compromise.

### RED

As it pertains to C-E equipment, transmission lines, and associated wiring, RED signifies both physical and electrical areas where

classified data/voice signals are in plain text (unencrypted) and highly susceptible to compromise.

**RED/BLACK CONCEPT**

The RED/BLACK concept requires electrical and electronic circuits, components, and systems which handle classified unencrypted information (RED) be separated from those which handle encrypted or unclassified information (BLACK). Under this concept, RED and BLACK terminology is used to clarify and to differentiate between circuits, components, equipment, and systems. The terminology also differentiates between the physical areas in which they are contained.

**CONTROLLED ACCESS AREA (CAA)**

The complete building or facility area under direct physical control that can include one or more limited exclusion areas, controlled BLACK equipment areas, or in any combination.

**BLACK EQUIPMENT AREA (BEA)**

BEA is an area in a CAA which contains equipment processing unclassified information or encrypted information.

**RED EQUIPMENT AREA (REA)**

An REA is the space within a CAA which is designated for installation of RED information processing equipment. It also includes associated power, signal, control, ground, and distribution facilities.

**CONTROLLED BLACK EQUIPMENT AREA (CBEA)**

A CBEA is a BLACK equipment area not within a CAA, which is afforded entry control at a security level commensurate with operational requirements. Examples of CBEAs are technical control facilities and radio relay sites supporting CAAs.

**EQUIPMENT RADIATION TEMPEST ZONE (ERTZ)**

An ERTZ is that area or zone established as a result of determined or known equipment radiation characteristics. The zone is a three dimensional space within which a successful hostile intercept of compromising emanations is possible. The ERTZ normally would be associated with equipment in an REA.

### COMMUNICATIONS SECURITY (COMSEC) EQUIPMENT

COMSEC equipment provides security to telecommunications by converting information to a form unintelligible to an unauthorized interceptor and, subsequently, by recovering such information to its original form for authorized recipients. COMSEC equipment also includes equipment specifically designed to aid in, or is an essential element of, the conversion process. COMSEC equipment includes crypto equipment, crypto ancillary (synchronization) equipment, crypto production (equipment used to produce or load keying material) equipment, and authentication equipment.

### PROTECTED DISTRIBUTION SYSTEM (PDS)

A wireline or fiber-optic telecommunications system that includes terminals and adequate acoustic, electrical, electromagnetic, and physical safeguards to permit its use for the unencrypted transmission of classified information.

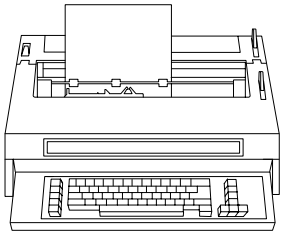
### EQUIPOTENTIAL PLANE

A grounding grid which provides a low-impedance path for signals and currents to return from the load, back to the generator. This system overcomes the limitations of the older single shunt grounding systems which are more inherit to noise and increased use of filters.

Now that the definition of EMSEC and its associated terms has been discussed, let's take a look at how compromising emanations are generated.

## GENERATION OF COMPROMISING EMANATIONS

### HIGH LEVEL DEVICES

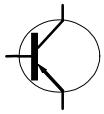


A high level device is any device that uses a high level of energy; i.e., voltages greater than 6 volts and current levels greater than 20 milli amps for its normal operating mode. This is a potential EMSEC hazard because higher levels increase the potential for compromising emanations. As an example, teletype equipment operating above +6 volts, as specified in MIL-STD-188, is considered a high level device.

## LOW LEVEL DEVICES

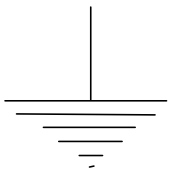
A low level device is any device that uses low level signaling. This is a current driven signal, ±2 volts at 70 micro amps or a voltage driven signal, ±6 volts.

## SOLID STATE DEVICES



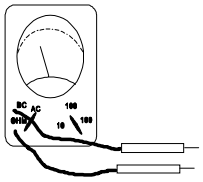
Extremely fast switching action involved in transistor and diode operations produces sharp rising pulses. These are desirable from an equipment design and operational viewpoint, but are very undesirable from an EMSEC viewpoint. Fast rise and fall times, or rapid transitions, produce compromising emanations.

## GROUNDS



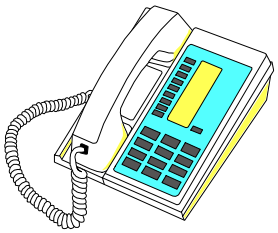
Coupling through grounds can take place directly and also through currents circulating around and between physically separated grounds. RED emanations cannot be picked up and transmitted on a BLACK ground if the RED ground is properly installed.

## TEST EQUIPMENT



When performing a test or alignment on RED and BLACK equipment, use caution to prevent test leads or probes from coupling the RED and BLACK equipment together. This can allow the classified unencrypted information from the RED equipment to be transferred to the BLACK equipment. This is a security compromise.

## TELEPHONES



There are sensitive components in the handset and the ringing element of a telephone. They can easily be activated by signals unintentionally emitted from RED/BLACK equipment. These signals can be picked up and transmitted by a telephone, even when the phone is on hook.

As one can see, there are many ways compromising emanations can be transmitted or coupled. The following procedure helps

reduce the risk of compromise to an acceptable and affordable level.

## EMSEC COUNTERMEASURES REVIEW

The EMSEC countermeasures review is not performed by EI but by the Base EMSEC Manager; however, we'll discuss it here to familiarize you with overall aspects of EMSEC.

### PURPOSE

An EMSEC countermeasures review is the procedure used to determine the appropriate level of required NONSTOP or HIJACK countermeasures for a facility, system, or equipment that processes classified information. It is a two step process:

- In the first step, the Base EMSEC Manager, with assistance from the user, determines the required level of TEMPEST protection as specified in AFSSI 7010, The Emission Security Assessment. In other words, will the user be processing classified information? AFSSI 7010 identifies three parts to the assessments; control of Compromising Emanations, NONSTOP, and HIJACK. The major command Information Protection (IP) office determines the level of TEMPEST protection for major command programs.
- The second step identifies specific RED/BLACK installation procedures needed to achieve the required level of protection for compromising emanations. The Base EMSEC Manager uses AFSSM 7011, The Emission Security Countermeasures Review, along with completion of AFCOMSEC Form 7001 to determine specific RED/BLACK installation procedures.

Installation standards are determined by the Base and MAJCOM IP office which provides inputs to the project engineer. This information is passed down to the EI Team in the Project Package. Let's take a look at RED/BLACK equipment installation concepts.

## RED/BLACK EQUIPMENT INSTALLATION CONCEPTS

It's important for all EI team members to closely follow basic RED/BLACK installation concepts and prevent TEMPEST violations. Let's examine the purpose and goal of the RED/BLACK installation concepts.

### PURPOSE

The purpose of RED/BLACK installation concepts is to ensure standardized installation practices are used for RED equipment,

BLACK equipment in a RED area, and associated wire line runs. If standard guidelines are not followed, RED processing areas could have equipment installed in such a manner as to invalidate their use as a RED processor and create a TEMPEST hazard.

**GOAL**

The goal of RED/BLACK equipment installation concepts is to create physical, electrical, and electromagnetic (EM ) barriers around equipment that processes National Security Information (NSI), and to prevent that information from being exploited by hostile intelligence activities. Design begins by establishing an REA within the CAA. The space is established to contain the RED processing equipment and related support functions with barriers to exclude all other non-related functions. The REA is sized according to separation tables and ERTZ data.

**EQUIPMENT TYPE**

A factor that also affects installation concepts is the type of equipment. C-E equipment that isn't TEMPEST approved is installed differently than TEMPEST approved equipment. But what kind of C-E equipment is not TEMPEST approved?

C-E equipment not TEMPEST approved is RED equipment that does NOT meet the criteria of NSTISSAM Laboratory Test Requirements and Electromagnetics. This will be discussed in Chapter 8, under the Project Review section.

**EMP**

In the RED/BLACK installation standards you'll also run across references to Electromagnetic Pulse (EMP). EMP is a high energy element resulting from a nuclear blast that can be induced into electronic equipment and lines causing component destruction. Let's stop and take a look at the difference between EMP protection and EMSEC protection.

**DIFFERENCES**

The difference between EMP and TEMPEST in RED/BLACK standards are levels, protection, and grounding paths.

- *Levels.* For EMP, high voltage, current, and field strengths are desirable to lessen interference. For TEMPEST, they are low to reduce emanations.
- *Protection.* EMP is concerned with shielding against outside electromagnetic energy affecting installed equipment.

TEMPEST is concerned with shielding to prevent inside electromagnetic energy from escaping outside.

- *Grounding paths.* Both EMP and TEMPEST provide protection for any ground paths required between the outside and inside of a structure. However, EMP and TEMPEST grounding methods differ.

Now that you know how EMSEC countermeasures are assessed and have a basic knowledge of RED/BLACK installation concepts, let's examine EMSEC countermeasures.

## COUNTERMEASURES

Two of the most effective methods of containing compromising emanations are physical placement of conductors and use of shields. Later chapters go into more detail with these and other countermeasures.

### CONDUCTORS

Current can be induced into a wire located near the wire carrying the original current. The amount of induced current depends on several variables such as distance and mutual angles between conductors, as well as the level of original current.

The easiest variables to control are the distance and the mutual angles. Because the intensity of the electromagnetic field surrounding a conductor gets weaker as the distance from the conductor increases, there is less induced current in wires that are widely separated than in wires close together. Also, wires at right angles to each other have minimum mutual induction. Therefore, you must always comply with RED and BLACK conductor separation specifications.

### SHIELDS

The purpose of shields is to reduce the coupling of electrical or magnetic fields into or out of circuits through the use of Electromagnetic (EM) barriers.

### EM BARRIERS

EM barriers must contain any compromising emanations produced by information processing equipment and exclude EM disturbances whether natural or man-made. They consist of perimeter barriers and internal barriers.

- Perimeter barriers are made of the facility entrance plate, power entry, utility entrance, signal entry, facility ground system, and

earth electrode system. We will cover these more in later chapters.

- Internal RED/BLACK EM barriers consist of physical separation between RED and BLACK equipment, power and signal distribution facilities, and patch bays.

### CABLE SHIELDING

The effects of an electromagnetic field produced by a current passing through a wire is reduced in free space, but in many cases, not enough to reduce the radiated signal to a safe level. Cable shields, both nonferrous and ferrous, provide high attenuation to the radiated fields. The cable braids form a nonferrous shield which attenuates electrical radiation. Ferrous material is more effective at higher frequencies and used primarily as a magnetic field shield.

Shielding of signal cables is enhanced by filtering all signal lines which connect RED and BLACK equipment. All cable shields should be terminated to the signal ground or equipotential plane via low impedance paths. RED and BLACK signal and shield grounds should be kept electrically separated until they reach the equipotential ground plane. Convenient electrical fault grounding points, such as conduit, metallic wire ways, enclosed equipment racks, and in some cases, shielded rooms are not to be used for signal grounds.

Shielding methods vary depending upon the type of equipment, physical construction of facility, and hardening requirements for EMP. TEMPEST approved equipment which uses low-level balanced voltage digital signals, shielded cables, and has adequate built-in power and signal/control line filters may not require use of conduit or duct. As a minimum, however, nonferrous shielded cable should be used. Use of conduit or duct as cable shielding is dependent upon the EMSEC assessment and local environment. Filters may also be used and may be required by EMSEC guidelines to suppress emanations at their source. Low level keying and equipment that operates at the same or lower voltage/current levels as associated equipment can also be used. But what about the facility itself?

## FACILITIES

Shielded enclosures are hardened facilities designed to negate EMP threats. They are shielded to prevent EMP damage to equipment and provide EMSEC protection. Inside the facility there are different security and shielding requirements.

### SECURITY

Different areas of the facility are rated for physical security. The physical location of the equipment determines whether an escort is required for the installation team. The most secure area you'll work in is the REA. Escorts to secure areas are provided by the customer unit.

### SHIELDING

Facility shielding requirements are found in AFSSM 7011. A facility may be totally shielded in a self-contained unit or may be part of a two-sided shield.

- Two-sided shields. Two-sided shields are used when TEMPEST approved equipment is used exclusively. The facility entrance plate and equipotential ground plane comprise the two sides. Equipment cases, racks, cabinets, conduits, and ducts comprise the rest of the shield.

As an EI team member, you do not install shielded facilities. This is the responsibility of allied support. However, being knowledgeable of the shielding requirements in your work area can help to bring about security consciousness. This security consciousness will aid you throughout the installation in being aware of potential compromises and discrepancies that can develop into security problems.

## SUMMARY

To properly install C-E equipment in RED/BLACK areas, you must be familiar with EMSEC installation concepts and standards. The information in this chapter is your first step in becoming familiar with these critical requirements. Future chapters cover specific unclassified TEMPEST installation techniques in more detail.

Learn all you can about EMSEC before the installation begins. You, and the Base EMSEC Manager are the key to controlling and preventing compromising emanations.

# CHAPTER 2
# SPACING

Spacing between equipment and transmission lines is a critical factor in preventing compromising emanations. As an EI installer you must be aware of and adhere to spacing requirements identified in your project package and other directives. In this chapter, we'll discuss how RED/BLACK spacing requirements apply to installation standards. As you may recall, ERTZ (Equipment Radiation TEMPEST Zone) is the projected distance from equipment and transmission lines that compromising emanations can travel. Equipment and transmission line spacing requirements, based upon the ERTZ, are designed to minimize reception of compromising emanations. Let's first examine how equipment characteristics influence spacing standards.

## EQUIPMENT CHARACTERISTICS

Basically, three equipment characteristics influence spacing standards: 1) the equipment designation (RED or BLACK), 2) whether or not the equipment is TEMPEST approved, and 3) signaling levels.

## DESIGNATION (RED/BLACK)

C-E equipment is designated RED or BLACK according to the type of traffic it processes. The RED or BLACK designation is a major factor in establishing equipment spacing restrictions. For example, maximum distance is desired between RED and BLACK equipment. Why? Remember, RED equipment carries unencrypted classified information. If located too close to a piece of BLACK equipment, the classified emanations from RED can be picked up and transmitted by the BLACK. Spacing requirements between equipment with the same designation (BLACK-BLACK or RED-RED) are not as stringent. Another spacing determinant is whether or not the equipment is TEMPEST approved.

## NON-TEMPEST APPROVED EQUIPMENT

RED communications equipment that does not meet the criteria of NSTISSAM TEMPEST/1-92 (C), *Compromising Emanations Laboratory Test Requirement Electromagnetics* (U) is not TEMPEST approved. This means it has not been specifically designed with protection against compromising emanations. Therefore, spacing requirements are greater than for TEMPEST approved equipment.

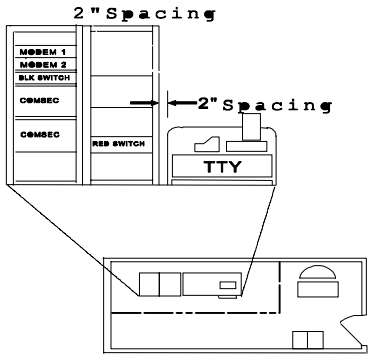
### LEVEL

A high level device is any device that uses a high level of energy, i.e., voltages greater than 6 volts and current levels greater than 20 milli amps for its normal operating mode. For example, teletype equipment operating above +6 volts is considered a high level device as specified in MIL-STD-188. This is a potential TEMPEST hazard and requires greater equipment spacing than for a low level device. A low level device is any device that uses low level signaling. This is a current driven signal, ±2 volts at 70 micro ampere or a voltage driven signal, ±6 volts. Now let's discuss some specifics of equipment spacing.

## EQUIPMENT SPACING

We'll consider specific unclassified equipment spacing requirements based upon equipment characteristics. Keep in mind that actual separation requirements for a particular system end item of equipment is classified CONFIDENTIAL.

### TEMPEST APPROVED EQUIPMENT




This figure shows a single-line secure teletype system using TEMPEST approved equipment. Dissimilar RED equipment, such as the teletype and the switch bay, are separated by at least 2 inches (50mm). The separation distance may increase due to specific installation practices such as minimum cable bending radius of the sizes of interconnecting ducts and conduits. The separation distance cannot be less than that established IAW RED/BLACK standards listed in MIL-HDBK-232A, Table 11, NACSIM 5203, Table 3-1, and applicable CM tables in AFSSI 7002. Improper spacing distances could result in a TEMPEST hazard.

### NON TEMPEST APPROVED EQUIPMENT

Figure 2-1, Non-TEMPEST Equipment Spacing, shows a small single-line teletypewriter facility using non-TEMPEST approved, high-level equipment. In this type of installation, the COMSEC equipment establishes a reference for equipment separation. All RED equipment, including distribution frames, are separated from the COMSEC equipment by at least 3 feet (0.9m). Why? Because

emanations from the RED equipment can be picked up and transmitted by the COMSEC equipment, though the COMSEC equipment itself is secure. All BLACK equipment is also separated from the COMSEC equipment by 3 feet (0.9m) resulting in a separation of 6 feet (1.8m) between high level RED and BLACK equipment.

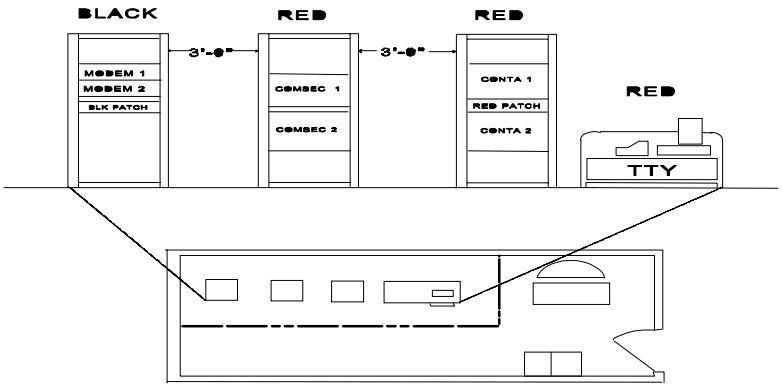



Figure 2-1, Non-TEMPEST Approved Equipment Spacing

For Patch and Test facilities, each RED patch panel is separated from the BLACK patch panel by a distance greater than the longest available patch cords. An alternative method is to use dissimilar patch facilities for RED and BLACK. This is to prevent accidental cross patching between RED and BLACK systems.

## LOW LEVEL DEVICES

Low level BLACK data processing equipment must be installed a minimum of 3 feet (0.9m) from RED data processing equipment. For BLACK voice equipment (i.e., administrative telephones) the separation distance must be a minimum of 3 feet (0.9m). More information about low level spacing requirements is found in MIL-HDBK-232A, Table I, NACSIM 5203, Table 3-1, and the applicable CM tables in AFSSM 7011.

In addition to spacing requirements, all TEMPEST approved equipment should be located at least 3 feet (0.9m) from the walls to provide room for technical inspections and maintenance.

## HIGH LEVEL DEVICES

Just like equipment which is not TEMPEST approved, high-level devices require a minimum separation distance of 6 feet (1.8m)

between BLACK and RED equipment. All RED equipment, including patch panels and distribution frames, must be separated from COMSEC (encryption devices) equipment by at least 3 feet (0.9m). More information about high-level spacing requirements can be found in ML-HDBK-232A, Table II, NACSIM 5203, Table 6-1, and the applicable CM tables in AFSSM 7011.

### VOICE SYSTEMS

Voice systems (telephone systems) installed in secure areas are designated either RED or BLACK. The one that's presently in use is the Secure Telephone Unit (STU III).

- *Administrative telephones* Administrative telephones are considered BLACK. All administrative telephones and their lines must be located at least 6 inches from RED signal lines.
- *STU III.* The Secure Telephone Unit is considered to be a BLACK telephone and is treated as such. However, when a personal computer (PC), fax, or other device which will process classified information is connected to the secure digital data post, the whole system must be reassessed. The STU III must be located at least 3 feet (0.9m) from RED processors if not specified in the Project Package. There must be at least a one meter separation between the STU III and telephone lines. More information about STU III requirements can be found in AFSSI 3007, Operational Security Doctrine for the Secure Voice Telephone Unit II (STU III) Type 1 Terminal.
- *Nondevelopmental Items (NDI).* On rare occasions, systems are installed using commercially available NDIs. These items have not been TEMPEST tested. When NDIs are used as RED processors the design of such items may not accommodate the use of shielded cables. When such a situation occurs, the project engineer will use the separation requirements of high level systems. Consult the Base EMSEC Manager for more information. Now let's look at spacing requirements for wire ways.

## WIRE WAYS

Wire way is a term used to describe conduits, duct work, or other structures used to carry cabling or wiring. Installation of wire ways is covered in AFJQS 2EXXX-202B, SIPT Electronics and Inside Plant. What we're now interested in are the basic wire way spacing requirements.

### BASIC SPACING REQUIREMENTS

Spacing requirements for wire ways are determined by their designation (RED/BLACK), how they are positioned (parallel/perpendicular), and the equipment operating level (high/low).

- *PARALLEL WIRE WAYS.* All conduits or ducts that are in close proximity to each other should be parallel. IAW MIL-HDBK-232A, associated RED and BLACK signal and power runs are separated by 2 inches (50mm). When parallel shielded RED and BLACK signal duct runs exceed l00 feet (30m), increase the separation distance to 6 inches (150mm). Parallel RED signal lines are separated from BLACK power lines by at least 6 inches. Power distribution serving the REA must be separated from BLACK equipment by at least 50mm.
- *PERPENDICULAR WIRE WAYS.* When crossovers are necessary, all conduits or ducts should cross at right angles and with appropriate physical separation. IAW MIL-HDBK-232A, if the RED and BLACK signal lines cross at a 90 degree angle, separation may be reduced to 1 inch (25mm).
- *EQUIPMENT LEVELS.* There are differences between the separation of signal and power wire ways for high-level TEMPEST and low-level TEMPEST equipment. Separation distances for each type are found in MIL-HDBK-232A, Table I; NACSIM 5203, Tables 3-l and 6-l; and the applicable CM tables in AFSSM 7011. Now that you have the basics of spacing requirements, where do you go if you have further questions?

## INFORMATION SOURCES

Separation requirements are listed in various publications, to include MIL-HDBK-232A, NACSIM 5203, Preferred Products List (PPL), and the TEMPEST Profile Data List (TPDL).

### MIL HANDBOOK 232A

MIL-HDBK-232A, RED/BLACK Engineering Installation Guidelines, contains unclassified spacing requirements for RED/BLACK installations. It is available from the Base EMSEC Manager.

### NACISM 5203

NACSIM 5203, Guidelines for Facility Design RED/BLACK Installation, is classified CONFIDENTIAL. It contains classified spacing requirements. It is also available from the Base EMSEC Manager. As an EI team member, you may not need to use it, but

knowledge of its contents may be useful during an installation. Contact the Base EMSEC Manager for access.

**AFSSM 7011**

The Emission Security Countermeasures Review. It provides guidance for making the emission security countermeasures review and spacing requirements for the control of compromising emanations, NONSTOP, and HIJACK.

**APPROVED PRODUCTS LIST (APL)**

This is a listing of equipment which meets NTISSAM TEMPEST l-92 design standards for approved TEMPEST systems. It is also available through the Base EMSEC Manager. It is of more importance to a Team Chief; therefore, we'll discuss its contents in Chapter 8, Team Chief Responsibilities.

**TEMPEST PROFILE DATA LIST (TPDL)**

This publication provides power requirements and physical control space for equipment not meeting NSTISSAM TEMPEST 1-92 design standards. It is classified CONFIDENTIAL and available through the Base EMSEC Manager.

## SUMMARY

Proper equipment and cable spacing is required if you are installing equipment which must meet EMSEC approval. When installing C-E equipment in areas where classified information is being processed, be sure to check your project package against the appropriate spacing standards. Become familiar with spacing requirements and comply with them during every step of the installation.

Spacing requirements for equipment in a classified environment are determined by equipment characteristics. This includes the designation of equipment (RED/BLACK), whether the equipment is TEMPEST approved or not, the classification of information being processed, and the equipment signaling level. In some cases, the type of equipment is also taken into consideration when determining spacing requirements, i.e., separate RED and BLACK patch and test facilities or secure voice terminals. The routing of wire ways also has a bearing on spacing requirements. Spacing for RED and BLACK wire ways differs for parallel routing and perpendicular routing. Spacing information is found in MIL-HDBK-232A, NACSIM 5203, and AFSSM 7011. An Approved Products List and TEMPEST Profile Data List can provide useful information about unique equipment characteristics. Proper

spacing of equipment and wire ways in a RED/BLACK installation minimizes the effects of compromising emanations and provides a secure environment. This is the goal of the installer in a classified environment. In the next chapter, we will discuss wire way installation.

# CHAPTER 3
# WIRE WAY INSTALLATION

## WIRE WAYS

Properly fabricated and correctly installed wire ways are helpful in reducing compromising emanations. All transmission and power lines radiate portions of the signals they carry. Therefore, it's necessary to encase unencrypted data lines and unfiltered power lines in a bonded shield to prevent interception of classified information. This chapter addresses installation of shielded wire ways to reduce compromising emanations. Topics include shielding requirements, principles of wire way installation, and how to mask wire ways. Proper wire way installation will greatly reduce the potential of comprising emanations.

As an EI team member, you must practice accepted installation techniques. This includes grounding and bonding all cases, cabinets, racks, conduits, and wire ways. You also need to ensure shield integrity by eliminating all openings through which compromising emanations can escape. This is done by making sure all panels, covers, and floors are properly installed.

## SHIELDING REQUIREMENTS

Metallic wire ways and conduits provide shielding for the cables they contain. Let's look at the unique requirements for conduit, duct, and junction boxes.

### CONDUIT AND DUCT

Cables for equipment or systems designed to operate in the high-level mode are installed using one overall nonferrous shield and ferrous conduit with compression or trawled fittings or ferrous cable duct. All RED and BLACK signal, control, and power lines, as well as all lines which are not a part of the communications system (door bells, administrative telephones, fire alarms, etc.), are encased in separate conduits or ducts.

Properly installed conduit with appropriate coupling devices provide an adequate shield. Conduit is not required for secure voice terminal wire ways if there are no other electronic devices in the general area. If a telephone is located remote from the terminal, the interconnecting cable should be installed in ferrous conduit.

Flexible conduit may be used for short runs, not to exceed 3m, between wire ways or junction boxes and equipment. However, do not use flexible conduit which contains plastic or non-conducting bushings in fittings. This interrupts shielding continuity.

### JUNCTION BOXES

All junction box apertures must be closed by conduit or ferrous aperture covers. Use RFI gasket material to ensure a complete seal against emanations.

Now that you are aware of basic conduit, duct, and junction box shielding requirements, let's examine TEMPEST wire way installation principles

## PRINCIPLES OF WIRE WAY INSTALLATION

Proper wire way installation reduces the likelihood of magnetic fields interfering with equipment by creating an electromagnetic barrier. The barrier stops free space radiation from coupling onto power or signal lines. Most wire ways enter a secure facility through a common facility entry point. We'll look at entry points in more detail in a future chapter. All you need to know now about the facility entry point is that it's found on the floor plan drawings and is used as the primary point to determine routing of facility wire ways. Now let's take a look at wire way installation techniques.

### WIRE WAY SURVEILLANCE

When possible, wire ways are installed where they can be physically observed within the facility for security purposes. However, facility construction and equipment layout do not always permit surveillance of all wire ways. Open wire ways must pass through walls, floors, or ceilings in the Controlled Access Area (CAA). RED distribution facilities and wire ways should always be exposed to view in the CAA except when passing through floors, walls, or ceilings to other spaces in the CAA. A non-conductive break in the wire way may be rewired at the CAA boundary with the CAA side bonded to the appropriate ground. Wire ways can be permanently installed within the walls, under the floors, or above the ceilings under the following conditions:

1. Conductors are monitored.
2. Accessibility is only from within the CAA.
3. Alarmed barriers are provided to prevent undetected human penetration.

4. Protected Distribution System (PDS) standards are complied with IAW AFSSI 3030, Protected Distribution Systems.

**Protected Distribution Systems (PDS).** PDS requirements are applied when RED cable distribution must leave a CAA and go through a less secure area before entering another CCA.

**Security standards.** The degree of required security depends upon the level of classification of the information, security level of areas crossed, and responsiveness of security force. Certain PDS classes and installations require rewiring alarms or visual surveillance. Surveillance requirements vary depending on PDS classes, physical locations, installation techniques, and type of data/information passing through the PDS.

**Installation standards for PDS.** Portions of the PDS are normally exposed to surveillance. All joints and covers are welded and pull boxes and accesses kept to a minimum. Where pull box access is required, covers are equipped with approved locks and intrusion detection devices. All junction or terminal boxes should be equipped with an RFI (Radio Frequency Interference) gasket cover.

## RED/BLACK INSTALLATION

To install BLACK wire ways, follow the guidelines in TO 3l-l0-l2, (Metal Ducts and Conduits), Sections II and III. Guidelines for running RED wire ways are found in NACSIM 5203 (Guidelines for Facility Design and Red/Black Installation) and AFSSM 7011 (The Emission Security Assessment).

- ***Conduit/Duct.*** Where positive batteries between RED and BLACK runs are necessary and extra physical protection is required, use totally enclosed ducts and conduits. RED and BLACK cables are never run in the same conduit or duct except in special cases. Separate RED and BLACK power distribution facilities need not be provided in a CAA where only low level signaling and TEMPEST approved equipment are utilized. In this case all power in the CAA will be considered BLACK, and RED information processing equipment can be connected directly to the same power.

When installing wire ways, remember to use the proper spacing distances discussed in Chapter 2. Also, if ducts/conduits must cross, ensure the crossings are perpendicular. Ducts and conduits should be grounded and unpainted to provide electrical continuity and all sections and covers firmly bonded. Use RFI gasket material with junction box covers to ensure a complete seal against emanations.

- ***Junction Boxes***. Junction boxes are installed IAW TO 31-10-12 (Metal Ducts and Conduits). If they are a part of a PDS their joints and covers must be welded or locked with an approved three-position, changeable combination padlock.
- ***RED/BLACK Power Panels.*** Power panels require no special installation other than placement. Use separate panels for RED and BLACK. Do not mix technical and non-technical power. Non-technical power is supplied to office air conditioning, heating, lighting, housekeeping, and creature comforts. Technical power is power associated with mission equipment. It includes environmental equipment designed to keep communications equipment within proper operating temperatures and lighting for equipment maintenance.

Technical and non-technical power is distributed in separate ducts/conduits. BLACK processing equipment or utility equipment will not be powered from filtered power panels. To do so could allow classified (RED) emanations from the filtered power panel to be picked up and transmitted on the unclassified (BLACK) wire ways. TO 31-10-24 (Grounding, Bonding and Shielding), Chapter 8, and MIL-HDBK-232A, cover installation of BLACK power panels in more detail. MIL-HDBK-232A, NACSIM 5203, and AFSSM 7011, cover specific installation criteria for RED power panels.

**MARKING WIRE WAYS**

All signal, power, and ground lines, components, equipment and systems within or serving a CAA which handle classified signals or modulation should be distinctly marked with red tape or paint at intervals of approximately 1.5m. An exception is conduit carrying RED signal ground feeders outside the building in a controlled area. All of the following cables should be marked RED.

1. Those carrying NSI.
2. Those between the encrypted side of crypto equipment and individual subscriber set or terminal equipment.

Wire ways that are not a physical element of the C-E processing system are identified as BLACK and not normally marked. This includes utilities such as smoke detectors, thermostats, etc. When BLACK components are very few, they may be distinctly marked with a 1 inch wide strip of black tape or paint at 5 foot intervals instead of marking RED components. On components colored black, another color such as white may be used to accentuate the black tape or paint.

## SUMMARY

Proper installation of shielded cable, conduit, duct, and junction boxes is required to prevent compromising emanations and qualify the facility as TEMPEST approved. Basic installation techniques identified in the 31-10-series TOs apply. However, you must comply with the additional shielding measures and hardware locations specified in MIL-HDBK-232A, NACSIM 5203, AFSSM 7011, and AFSSI 3030. Your project package should specify, in clear terms, precisely how to install TEMPEST approved wire ways. Be sure to follow the package and guidelines provided in the applicable references. The next chapter addresses the distribution of cabling in the newly installed wire ways.

# CHAPTER 4
# CABLE INSTALLATION

To meet TEMPEST specifications and further reduce the potential of compromising emanations, you must always comply with specific cable installation standards. Cables must be protected and shielded throughout the facility from the point of entry to their final termination point. Any break in shielding or incorrect routing could result in radiation of compromising emanations.

This chapter addresses requirements for installing cables in secure areas. This takes into consideration shielding, routing, equipment types, and wire terminations. We'll also discuss the purpose of filters, their application, and their basic installation techniques. The information in this chapter, along with guidance in your project package, the 31-10-series TOs, NACSIM 5203, and AFSSM 7011, will prepare you to meet TEMPEST installation standards in secure facilities.

## INSTALLATION REQUIREMENTS

Prior to actually installing cables and signal lines you must be familiar with basic secure area cable routing, shielding, cross-connect and termination requirements. Factors which affect the degree of emanations given off by a cable include the type of cable and the methods of cable termination and cross connection. The type of equipment and signal levels also influence how wire lines are installed. Cable shields provide very effective emanation suppression.

### FIBER OPTICS

Fiber optic systems should be used in place of metallic cables whenever possible and when cost effective. They have several EMSEC advantages over conventional metallic cables.

- Optical fibers are nonmetallic; therefore, they do not radiate electromagnetic energy and since the transmission medium is light, they aren't as easily affected by electromagnetic fields. This effectively eliminates crosstalk.
- Fiber optics are non-conducting so fiber optic systems are not subject to ground loops or shorting problems nor are they prone to pick up stray emanations.
- Fiber optic systems are not subject to the transmission of common-mode signals.

- Transmission security is improved since intrusion without detection is more difficult for fiber optic systems than metallic cables. Physical tapping is necessary to sample data and results in physical evidence of tampering. Also, if properly designed, equipped, and installed, you can use the detectable reduction in signal level as an alarm sensor.

Installation standards for fiber optic systems are not the same as those for conventional metallic cables. The installation standards are:

- ✔ Use fiber optic systems in place of shielded metallic wires.
- ✔ Route a RED fiber optic cable which traverses a BLACK area to allow for easy detection of intrusion.
- ✔ When you transmit RED and BLACK information through individual fibers bundled together or in a multifiber cable, you must provide an opaque separation between the RED fibers and the BLACK fibers and separate the sending and receiving equipment according to the countermeasures review.
- ✔ When individual RED and BLACK fibers are run in the same distribution facility, cover each fiber with opaque cladding and separate the sending and receiving equipment according to the countermeasures review.
- ✔ Do not use RED fiber optic cables with metal strength members or conductive cladding to traverse BLACK areas and vice versa. This same requirement applies to armored fiber optic cables. Any such metal component in the cable is a fortuitous conductor.
- ✔ Mark the RED fiber as you would any other conductor.
- ✔ Running RED fibers with BLACK metallic cables is permitted.
- ✔ Do not run BLACK fibers with RED metallic cables.
- ✔ The sending and receiving units must meet the same EMSEC countermeasure requirements as any other RED processor in the area.

## CABLE SHIELDS

A basic EMSEC requirement is each cable in a secure facility should have at least one overall nonferrous shield, such as the shield on a multi-pair cable. When TEMPEST approved equipment is used, signal cables with at least one overall nonferrous shield can be installed using cable ladders and trays. Unshielded wiring must be installed in totally enclosed duct and conduit. For equipment operating in the high level mode, all

cables, shielded and unshielded, must be installed with ferrous conduit with compression or threaded fittings or ferrous cable duct.

Cables with overall nonferrous shields are used for RED signal and cable lines and also for BLACK lines. The shields of all cables within a RED equipment area (REA), BLACK equipment area (BEA), and controlled access area (CAA) are grounded at one end. Neither cable shields nor ground conductors will be used as a return path for RED signal, clocking, or control signals. Shielding requirements for BLACK cables are listed in MlL-STD-188-124A. Shielding requirements for RED cables are in NACSIM 5203 and AFSSM 7011. There are two types of control/signal cables used for TEMPEST installations: twisted pair and coaxial.

- *Twisted pair*. Twisted pair is normally found in multi-pair cables such as 25-pair telephone cable. It possesses an overall shield or individual pair shields, and is the most common type of cable used for data, control, and audio signal transmission.
- *Coaxial.* Coaxial cable is used for special purpose high frequency applications. Some variations are triaxial, coaxial with an additional special purpose shield; twinaxial, a twisted pair encased in dielectric foam covered in braided shield; and quadraxial, twinaxial with an additional shield. These additional shields greatly reduce unintentional emanations.

**CABLE ROUTING**

All signal and power lines enter and exit a secure facility through two separate entry points located in the cable and power entrance vault. Vault access is restricted to maintenance personnel with the required security clearance.

- Equipment that isn't TEMPEST approved may radiate emanations from interconnecting cables. Signals may also be induced into cables passing through an Equipment Radiation TEMPEST Zone (ERTZ) which exit the facility. To reduce interconnecting cable emanation hazards, ensure all cables are afforded proper protection. The use of shielded cables and metallic wire ways provide protection by placing an EM barrier between the cable and the radiated signals.
- *RED distribution*. Remember, you must <u>never</u> run RED and BLACK signal cables in the same wire way, conduit, or duct unless the cable is fiber optics and approved by your Base IP Office. In the REA, cables between equipment may be double shielded if the cable volume makes wire ways impractical. RED signal grounds may be run with RED signal lines. If the

equipment is TEMPEST approved and using low level signaling, metallic distribution is not needed provided the RED cables have at least one overall non-ferrous shield. Further emanation protection is provided by filters.

Complete accountability of all wires and cables within or passing through a secure area will be clearly marked, labeled, or tagged according to purpose. Unused wiring in cables will be grounded within the controlled areas and clearly marked as such.

- *Power distribution.* TEMPEST approved COMSEC equipment may be connected to unfiltered BLACK power panels. BLACK processors can be serviced from unfiltered power panels external to a CAA. All power must be run in ferrous metallic distribution facilities separate from signals and grounds.

- *Telephone lines.* Telephone signal lines are not distributed with other signal cables. Where possible, telephone cables are installed in conduit from the facility wire closet or from the Key Switching Unit (KSU) to a point as close to the telephone as operationally possible. In facilities processing classified information, telephone lines may require filtering or isolation. Within a CAA, telephone lines are routed from the entrance connector blocks in conduit using shielded cable.

The specific use of each telephone conductor is accounted for at the point of entry. This is done by labeling or log/journal entries. This accountability also applies to unused conductors terminated at the point of entry and connected to appropriate connector blocks.

**EQUIPMENT TYPES**

As mentioned earlier, the type of processing or equipment being installed also affects cable installation requirements. Some examples of equipment and installation requirements are:

- *Radios*. In the REA of Command and Control facilities, cables for voice communication equipment, such as microphones or radio telephone headsets, are distributed in dedicated conduit. Cable separation requirements are the same as for administrative telephones. Radio Frequencies (RF) in the REA must also be filtered to reduce compromising emanations. Filters are discussed later in this chapter.

- *Modems.* Modem input and output signal distribution is typically BLACK. Normal routing of audio signals is from modem to analog frame, and patch bay to distribution frame

(DF). Cabling is normally twisted pair with each pair shielded. Cables are also routed in metallic wire ways, ducts, or conduits.

- *Administrative telephones.* Line distribution of administrative telephones in the CAA is separate from other wire distribution. All administrative phone cables entering the facility should either be properly separated from other cables, filtered, or isolated.

- *Data processing.* For data communications, the input is digital and, in some cases, encrypted. An example of this is the teletype in a secure area. All single cables in a facility will have at least one overall non-ferrous shield.

- *Secure voice.* For a STU III installation, the cable shielding will be bonded to the connector shell at both ends. Other information can be found in AFSSI 3007, Operational Doctrine for the Secure Telephone Unit III (STU-III) Type 1 Terminal.

- *Secure telephone switches.* Signal and control lines utilize cable with an overall non-ferrous shield and the shield is grounded at one end. Wire lines, to include signal, control, and power, are installed in ferrous conduit. This is necessary to provide maximum protection and to isolate RED/BLACK lines and digital and analog systems.

- *Distribution Frame (DF).* DFs provide a means to configure internal equipment for various applications. They connect exiting lines to modems, modems to COMSEC devices, and COMSEC devices to terminal equipment. RED and BLACK DFs are contained in enclosed metallic cabinets. The metallic cabinets should be large enough for maintenance access. Separate DFs are used for RED and BLACK applications.

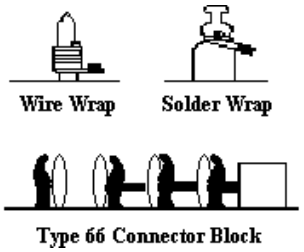
**WIRE TERMINATIONS**

Proper terminations with a minimum of signal loss are required for TEMPEST installations. Shields will be continuous, low resistance runs by proper termination of all joints and splices. Terminate to signal ground at one end only. Shields should not be connected to equipment cabinets; make the cable shield common to AC protective grounds.

Cable shields should be tightly fastened to the cable connector shell with a compression or soldered connection. When assembling a connector, the cable shield must be less than 1 inch (2.5cm) from the point where it breaks away from the individual shielded conductors of the cable. A distance of more than 1 inch

(2.5cm) increases the potential of compromising emanations. If a pigtail is the only method of shield termination that can be used, it should be as short as possible and terminated at one end only. Proper grounding of cable shields allows the shortest possible exposure of unshielded pairs and provides a minimum impedance path to the equipotential ground plane.

As shown in the illustration to the right, there are three basic methods of terminating wire lines. More than likely, specific termination requirements will not be addressed in your project package. The Team Chief must use the method that conforms to existing standards.




Wire wrap is considered the most reliable type termination. Solder lugs are prone to cold solder joins causing a mismatch of impedance. The Type 66 Connector Block makes fast connections to terminals without removing the conductor insulation.

## DISTRIBUTION FRAME CROSS CONNECTIONS

Cross connects are used in DFs to connect incoming and outgoing wire lines to modems, modems to COMSEC devices, and COMSEC devices to terminal equipment. The color code for Secure System cross connects is found in TO 31-10-2, Table 3-14.

- *Spare pairs.* Cables in most facilities are installed with extra conductors to accommodate upgrades. Terminate one end to the signal ground bus in the appropriate distribution frame serving that particular cable. RED conductors will be terminated to RED signal ground and BLACK conductors to BLACK signal ground. All such conductors should be grounded at one end of the cable only. The spare conductors/pairs should be folded back (not cut) and insulated at the other end of the cable. In no case will unused conductors be cross-connected to conductors going to subsequent DFs. Spare pairs which are in place between a BEA and a controlled BLACK equipment area (CBEA) are grounded at the distant end when not in use. An accounting of all conductors is necessary.

- *Telephone Lines*. Telephone lines are terminated at the point of entry and are connected to appropriate connector blocks an the DF.

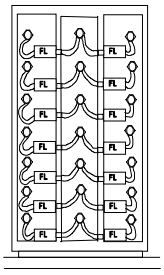
## FILTER INSTALLATION

Filters are often installed in both power and signal lines. Combined with shielding, they suppress most compromising emanations generated by equipment.

### FILTER PURPOSE

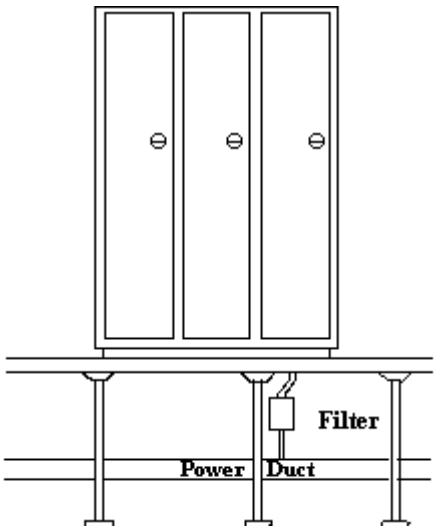
Filters are used to pass desired audio and RF frequencies to the load while shunting unwanted frequencies either to ground or back to the source. Their use is determined by the Project Engineer.

- *Filter Requirements.* Equipment which processes RED information may require filtering of signal lines, power lines, or both. If equipment is TEMPEST approved and there is proper grounding and separation of BLACK conduits from RED runs, then the need for external filtering is greatly reduced or eliminated. In addition to your EI Project Package task instructions, here are some basic guidelines to follow when installing both RED and BLACK filters.



- *RED Filters.* Install RED filters in RFI cabinets as shown in the adjacent illustration. Filters must be firmly bonded to the walls to assure electrical integrity. Provisions must be made at the entrance of the cabinet to bond and terminate the cable shields. The filter cabinet must be firmly bonded to the equipotential ground plane. Within the facility, RED filter cases for RED signal lines are bonded directly to the equipotential ground plane.

- *BLACK Filters.* BLACK signal filtering can be accomplished at the point of exit or within the facility. Within the facility, BLACK signal filters are bonded directly to the equipotential ground plane. BLACK power-line filters are bonded to the equipment chassis and the Fault Protection Subsystem (FPSS). This illustration provides an example of where BLACK power filters are normally installed. Consult your project package for specific filter locations.




Often, control signals associated with a channel are generated in the RED area and must be routed to the BLACK area for control of channel functions. If such signals are routed in the same cable as RED cable signals, they are considered RED. Isolators are often incorporated at the RED/BLACK boundary for these signals.

## ISOLATORS

Within the facility, a RED/BLACK boundary is required for signal lines which must transverse both areas but do not pass through COMSEC devices. This is achieved by using an isolator. The most commonly used isolator is the Optical Isolator.

- *Optical*. An optical isolator consists of a drive module coupled to a receive module via Fiber Optic Cable (FOC). The RED signals are changed into light by the drive module, routed along the fiber optic cable, and transformed back into electrical impulses by the receive module. When in light form, they produce no compromising emanations. In order to limit the number of penetrations of a shield, channels are multiplexed to drive the fiber optic isolator then de-multiplexed after exiting the facility.

- *Location.* The ideal isolation mechanism placement is within the same area as the COMSEC equipment. The installation design must assure the isolation mechanism cannot be bypassed. Isolators may also be used at a point of exit, such as a facility entrance plate or to establish RED/BLACK boundaries.

## SUMMARY

Following proper installation methods, including routing, shielding, and termination of wire lines, will reduce the effect of compromising emanations in a secure area. Fiber optic systems are much more secure than metallic cables and should be used whenever possible. By following the RED/BLACK installation criteria for wire lines and filters, the installation team is on its way to providing secure communications with no signal compromise. The next chapter introduces you to C-E equipment IAW RED/BLACK installation criteria.

# CHAPTER 5
# EQUIPMENT INSTALLATION

Proper installation of COMSEC and associated processing equipment is a major factor in reducing compromising emanations. When installing RED and BLACK equipment in secure facilities, you must follow the procedures in TO 31-10-29, Erection and Assembly of C-E-M Equipment. In addition, you must adhere to RED and BLACK TEMPEST criteria which should be clearly defined in your project package. This includes compliance with equipment spacing requirements discussed in Chapter 2 and other requirements identified in MIL-HDBK-232A and other directives.

This chapter identifies various types of RED equipment and basic installation criteria applied to each type. For the most part, the information contained within was extracted from MIL-HDBK-232A. Having a basic concept of RED and BLACK equipment installation criteria before you start the installation will assist you in completing project reviews and give you an idea of the TEMPEST installation standards you must comply with.

## TYPES OF RED EQUIPMENT

Any device that processes classified information is considered RED equipment. For example, commercial telephones coupled with cryptographic devices can be configured as secure voice switching systems in RED areas. In such cases, the telephone is a RED device. Word processors, as well as mainframe computers or facsimile (FAX) machines, may also be used as RED devices. Even the common electric typewriter can be a RED device. While numerous types of equipment which process classified information can qualify as RED equipment, you need to be familiar with the more common types of RED C-E equipment which you may be installing in telecommunications centers. This includes such items as teletypewriter, secure voice systems, facsimile, video devices, patch panels, ancillary equipment, and storage devices.

### SECURE VOICE SYSTEMS

Most of the secure voice systems in use today interface with specially designed telephone instruments and/or data and facsimile terminals. A RED telephone network must be totally contained within the CAA but may have trunks coupled to the central office if the trunks are encrypted.

### FAX TERMINALS

There are two basic types of facsimile devices, analog and digital. The older analog devices operate at lower speed and require an analog to digital conversion prior to encryption. The newer digital devices do not require signal conversion. No matter which type is used, shielding, filtering and separation requirements still apply.

### COMPUTERS

Computer systems range from small stand-alone word processors to moderate-sized RED digital computerized telephone switches.

### VIDEO DEVICES

When video devices are used as RED processors, they are usually installed in areas where the entire video distribution is confined to a building or small group of buildings. However, there are still grounding, bonding, and shielding requirements for all cables within the video system.

### STORAGE DEVICES

Storage devices include components in which classified information is stored, such as magnetic memory in recorder-reproducers and computer memories. The RED/BLACK considerations for both on- and off-line devices are the same.

### ANCILLARY EQUIPMENT

Ancillary equipment includes such devices as analog to digital and digital to analog converters, line controller units, crypto-bypass devices, line drivers, rate converters, rate buffers, synchronizers, and other units required between the user terminal and the encryption device.

## EQUIPMENT LAYOUT

### EQUIPMENT POSITIONING

Based on connectivity considerations and physical restraints, BLACK equipment is normally grouped together near the Main Distribution Frame (MDF). RED equipment is grouped together and installed some distance away (as directed by separation requirements) from the BLACK equipment and the MDF. Crypto equipment is normally located somewhere between the BLACK and RED equipment. Depending upon the size of the facility, physical layout, and amount of equipment, there may be more than one REA, BEA, and crypto area. One of the main concepts of

equipment layout is to group related equipment together and minimize cable length. Shorter cable runs reduce the probability of emanations and interference.

### BLACK EQUIPMENT IN RED AREAS

BLACK equipment is not normally installed in RED equipment areas. When it must be, strict compliance with the spacing requirements identified in Chapter 2 is required to reduce the possibility of BLACK equipment picking up emanations from RED equipment.

### DISTRIBUTION FRAMES

All signal cables are routed to the MDF. Intermediate Distribution Frames (IDFs) are normally installed in close proximity (RED IDF near RED processors; BLACK IDF near BLACK equipment) to the equipment they serve. All RED and BLACK distribution frames are separately installed and enclosed in a CY-597, CY267S, or equivalent cabinet.

For further information on equipment layout, refer to MIL-HDBK-232A and your project package. If, during the early stages of an installation you identify perceived equipment layout problems, notify your Team Chief and get in touch with the project engineer.

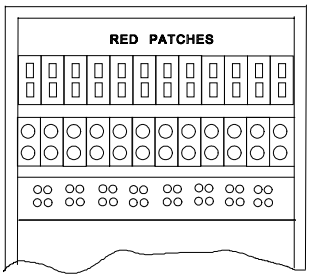
## EQUIPMENT INSTALLATION

To further reduce the effects of compromising emanations, certain installation precautions must be taken when installing both RED and BLACK equipment in secure facilities.

### PATCHING EQUIPMENT

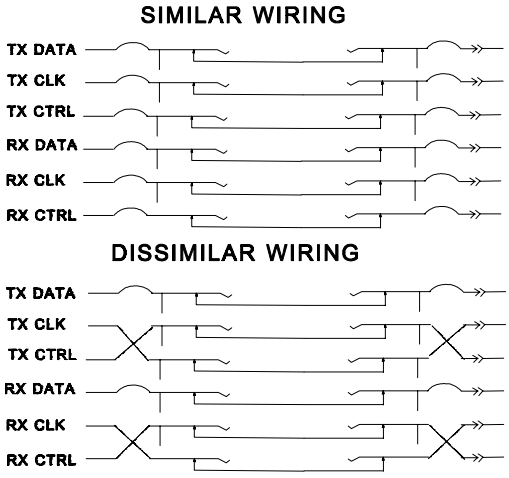
Patch panels are used to test and monitor circuits and substitute equipment or lines when failures occur. Patch panels in patch and test facilities are primarily used to restore and route VF and digital circuits. There must be no means of patching directly from the RED side to the BLACK side or among isolated RED patches. This is accomplished by physical separation, dissimilar patching, dissimilar wiring, and dedicated switching.

- *Dissimilar Patches.* Dissimilar patches are used where RED circuits serve different communities. The term communities applies to dedicated circuits that service distinct missions or

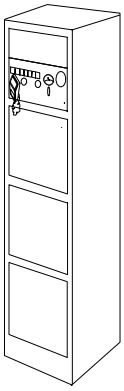


personnel. As shown in the adjacent figure, different types of RED patch jacks are installed to prevent physical connection between different communities or classifications of security.

- *Dissimilar wiring.* Dissimilar wiring is installed which will cause the equipment to become inoperative should a RED/BLACK mispatch occur. See the figure on the right for an example. Dedicated switching, single channel facilities should not use patches at all, but use A-B switches and X-switches to swap equipment.

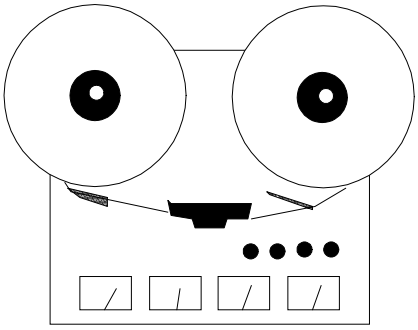



## EQUIPMENT CABINETS



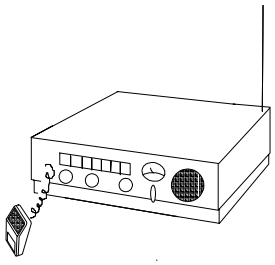
To reduce possible compromising emanations, all rack-mountable RED processing equipment and ancillary equipment is installed in cabinets. The equipment should make bare metal contact with the cabinet. Blank panels are installed on front of all unused cabinet spaces. When properly installed, the panels and closed cabinet doors greatly reduce undesired emanations. Make sure you have a sufficient number of blank panels available. An exception would be RED patch panels with low-level circuits. In this case, front covers are not required.

## MAGNETIC TAPE UNITS



These are normally known as recorders/reproducers in voice communications. They are also used as memory storage units for computer systems. Avoid the common installation practice of removing cabinet sides of a group of units and bolting the chassis together to form a single unit since this arrangement negates the shielding effectiveness of the cabinet. To follow proper RED/BLACK installation criteria, install each unit as a stand-alone device with individual grounding and bonding.

### RADIOS



Radio equipment is not normally installed in secure areas which have TEMPEST restrictions. This is to prevent transmission of classified data or voice. Sometimes, however, radios must be installed within CAAs to support command posts and other specialized operations. In such cases, all microphones and handsets located in REAs are equipped with Push-To-Talk (PTT) and Push-To-Listen (PTL) switches. To safeguard against accidental transmission of classified signals, audio and RF transmission lines are encased in dedicated conduit and equipped with bandpass filters located at the facility entrance plate.

## MARKING EQUIPMENT


The final communications equipment installation step is proper marking of equipment designations. TO 31-10-27, Standard Installations Practices Equipment Designations, is used in marking designations on ground C-E equipment. This includes floor plan positions and group designations. RED information processing equipment will normally be marked with a 1" x 3" red tape or paint mark near the equipment nomenclature label. TSEC nomenclatured material will not be marked. If BLACK components in the CAA are very few, they may be marked instead of RED components. NACSIM 5203 and AFSSM 7011 contain other guidance for marking RED equipment.

## SUMMARY

Proper installation of equipment IAW the 31-10-series TOs, MIL-HDBK-232A, NACSIM 5203, and AFSSM 7011, is required to reduce the effects of compromising emanations and meet TEMPEST criteria. Your project package should specify, in clear terms, precisely how to install all telecommunications equipment in a secure environment. The information in this chapter introduced you to some of the RED/BLACK equipment installation requirements, but certainly not all of them. Familiarize yourself with all special installation requirements before you begin work, the end result will be a professional installation which meets TEMPEST standards.

# CHAPTER 6
# GROUNDING AND BONDING

A properly installed grounding system is a critical factor in reducing compromising emanations. This is because faulty grounds can radiate signals which may be picked up by equipment and transmission lines thus negating all other TEMPEST installation precautions. A TEMPEST approved grounding system is not restricted to just a piece of equipment or even an entire system. It could include an entire work area or, in some cases, the entire building you are working in.

The same degree of criticality also applies to bonding. Bonding serves to eliminate differences in potential between metallic structures, such as wire ways and equipment items. Differences in potential between high level and low level devices could result in a transfer of compromising emanations. Proper equipment, wire way, and ground bonding eliminates differences in potential and greatly reduces radiation of compromising emanations.

This chapter outlines basic principles of grounding and bonding. It includes essential grounding information explained in TO 31-10-24 and also addresses RED/BLACK TEMPEST installation criteria for grounding and bonding.

## GROUNDING SYSTEMS

When installing equipment in secure facilities, you will probably be required to install part of the grounding system. Having a basic knowledge of the purpose of grounding systems and how they are configured helps ensure proper installation and enables you to recognize and correct potential installation problems.

### GROUNDING

Ground is an agreed upon potential to which all signal voltages are referenced. Earth, often considered at zero potential, is almost always the reference point. In addition to serving as a reference point, grounds provide a low resistance path which shunts undesirable currents (lightning, power transients, emanations, etc.) to the reference point.

### FACILITY GROUND SYSTEM

A typical facility ground system consists of the Earth Electrode Subsystem (EESS), a Fault Protection Subsystem (FESS), a signal reference subsystem, and the lightning protection subsystem. To

meet TEMPEST requirements, facilities which house classified information processing equipment require a more elaborate and more expensive facility grounding system than other types of C-E facilities. Since grounding is such a crucial factor in preventing compromising emanations, you should be familiar with the basic elements of a facility ground system.

- *Earth Electrode Subsystem (EESS).* The EESS is the common point to which the signal reference subsystem and the lightning and fault protection systems are tied (bonded). The equipotential ground plane is also bonded to the EESS. The EESS consists of a ring ground, around the facility, augmented by an array of varying length rods driven in the ground near the facility entrance plate to provide low impedance to earth. When installed correctly, the EESS resistance to ground is less than 10 ohms.
- *Fault Protection Subsystem (FPSS).* The FPSS, sometimes called “the safety ground", is designed to protect personnel and equipment from dangerous voltages caused by electrical circuit faults. The subsystem consists of ground leads which are electrically separated from the power distribution system phase and neutral conductors. The ground leads are also separated from the signal reference subsystem ground leads. This subsystem terminates on the power ground terminal of the equipment and the ground stud in the power panel and ties into the EESS. Maximum acceptable impedance of this subsystem is 10 ohms. All TEMPEST approved facilities must have an FPSS installed IAW TO 31-10-24 and MIL-HDBK-232A.
- *Lightning Protection Subsystem.* This subsystem provides a safe path to earth for lightning and other transient voltages that may enter a facility. There are no special EMSEC requirements associated with the lightning protection subsystems installed in secure facilities. It’s normally done as part of allied support by the host base.
- *Signal Reference Subsystem.* This subsystem serves as the common signal ground reference throughout the facility. It provides a path to the EESS for induced static and noise and serves as a ground plane for HF signals between equipment. Radiation of compromising emanations is greatly reduced by this subsystem. In some secure facilities, an equipotential signal plane comprised of a metallic sheet or grid is frequently installed under, over, or beside all equipment in the technical area. All signal ground runs are bonded to the equipotential ground plane. Other facilities utilize RED/BLACK single

point signal grounding systems instead of an equipotential plane.

**EQUIPOTENTIAL GROUND PLANE**

An equipotential ground plane is often installed in secure facilities to reduce the effects of compromising emanations. This ground plane is most effective when it extends under or above all RED and BLACK equipment. This includes distribution frames, patch panels, and RED/BLACK processing equipment. In some cases, physical facility construction may dictate installation of a vertical plane; however, a horizontal plane is more effective than a vertical plane in coupling unwanted signals to earth. An equipotential ground plane is considered earth for the signal reference subsystem regardless of elevation or location. The plane is banded (welded or brazed) to the main steel structure of the building and to the EESS at multiple points.

**GROUNDING METHODS**

While a good portion of the facility ground system installation is accomplished by allied support. EI teams frequently run grounds for all subsystems and tie them into the EESS. Therefore, you must be familiar with RED/BLACK grounding runs and how to connect signal grounds, EESS grounds, and how to ground cable ladders, conduit, and duct.

**EQUIPOTENTIAL PLANE CONNECTIONS**

All equipment racks, cabinets, and cases are grounded to the equipotential ground plane using #6 AWG stranded copper wires. Separate ground wires are normally run for each equipment end item of each equipment rack. Ground conductors must be continuous and not spliced at any point. Ground runs are bonded to the plane and bolted to grounding studs which are welded to each rack or cabinet. Equipment cases are grounded through the rack/cabinet ground or are equipped with individual grounding conductors. If a cabinet case ground is not provided, you must install a ground terminal as near the power entrance point as possible.

**SIGNAL GROUND CONNECTIONS**

RED and BLACK signal grounds are established by direct connections to the equipotential ground plane which is bonded to the EESS. For unbalanced signaling, the signal ground is established by a direct connection from an isolated signal ground bus in the RED distribution frame to the equipotential ground

plane and the earth electrode subsystem. A BLACK signal ground is used to provide a signal ground reference in the BLACK distribution frame.

### CABLE SHIELD CONNECTIONS

Cable shields for both RED and BLACK signal lines are circumferentially bonded to the equipotential ground plane. Cable shields surrounding individually shielded lower frequency signal lines are grounded at one end. For grounding of existing RED/BLACK equipment and systems installed before MIL-HDBK-419A, Vol. II, was written, refer to MIL-HDBK-419A, Section 2.4, for guidance.

### CABLE DUCT CONNECTIONS

Cable ducts are grounded at one end. The duct is then bonded to the equipotential ground plane at the shortest distance between the duct and the ground plane. This is done by bonding the cabinets to the plane since the duct is tied to the cabinets. Cable ducts carrying AC power will be grounded to the AC protective ground bus in the power panel.

### POWER LINE CONNECTIONS

Correct hookup of FPSS ground conductors to equipment housings, cabinets, racks, conduit, ducts, distribution boxes, junction boxes, and other hardware is essential for the protection of personnel and equipment, and suppression of compromising emanations. FPSS ground conductors are normally green. The neutral and FPSS ground conductors are bonded together at the first service disconnect or service transformer and further bonded to the EESS. This is the only intentional grounding of the neutral conductor that’s permitted by MIL-STDS and National Electric Codes (NEC). If an end item of equipment does not have a ground terminal, you must install one on the equipment case near the power entrance point. In shielded facilities, the FPSS conductor does not penetrate the shield, rather, it's bonded to the shield on the inside and outside. Refer to your project package, TO 31-10-24, MIL-STD-188-124, and MIL-HDBK-232A, for FPSS ground conductor installation guidance. Now that we've discussed grounding, let's look at bonding.

## BONDING

Bonding is the electrical connection established between two metallic surfaces to provide a low impedance path between them. A good bond is mechanically strong, resists corrosion and stress,

and exhibits the same mechanical and electrical properties as the material which is bonded together. Common bonding methods include welding, brazing, soldering, or by compression bolts, nuts, clamps, and straps. Proper bonding is required to ensure the integrity of grounding subsystems and thereby reduce the chances of compromising emanations.

**BONDING METHODS**

Welding or brazing, though not done by EI teams, is the preferred method of bonding. In some cases, soldering is also acceptable; however, never use solder bonds for the FPSS or the lightening protection subsystems. The method of bonding frequently employed by EI teams is pressure connectors. Various types of pressure connectors are available, but they should only be used if called for in your project package. More information about bonding is found in TO 31-10-24, Grounding, Bonding, and Shielding.

**EESS**

The EESS is normally constructed using No. 1/0 AWG 7-strand copper wire, which is buried in the earth at a depth of at least 1.5 feet below the surface. The wire is bonded by welding or brazing to 10-foot copper-clad steel rods driven into the earth around the facility at intervals not to exceed 20 feet. Welding or brazing is also the preferred method of connecting all ground subsystems to the EESS.

**EQUIPOTENTIAL PLANE**

The equipotential ground plane is bonded to all adjacent structural steel frames by No. 110 AWG stranded wire. It's also bonded to the EESS at multiple points around the facility perimeter. You should bond all equipment signal grounds to the equipotential ground plane with the shortest possible runs of No. 6 AWG stranded wire. All connections should be welded or brazed; however, pressure clamps may be used if called for in your project package. Remember, to provide adequate TEMPEST protection. All equipotential ground plane connections must meet MIL-STD-188-124 and MIL-HDBK-232A specifications.

**POWER FILTERS**

If you are required to install power-line filters, connect a No. 1/0 AWG stranded copper wire between the filter case and facility entrance plate. They are normally installed in one or more central locations and contained in RFI cabinets.

## SUMMARY

Proper installation of signal reference subsystem, lightning protection subsystem, and fault protection subsystem is critical to ensure the containment of compromising emanations. It's unlikely you'll be installing the EESS; however, you may be required to install portions of the equipotential ground plane. Whatever the case, remember that their value can be severely compromised if ground leads are improperly connected to equipment or bonding is not sound. An improperly installed grounding system in a classified environment renders RED/BLACK installation criteria useless. Be sure to follow your project package and consult the references cited in this chapter for installing RED/BLACK grounds and bonding protective subsystems to the EESS. If you have any questions, contact the project engineer or the Base EMSEC Manager for assistance.

# CHAPTER 7
# PRE-SHAKEDOWN INSPECTION

When you have finished your TEMPEST installation, it's time to power up the equipment and start your test and adjustments--right? **Wrong**! EI teams are required to perform a pre-shakedown inspection to ensure the equipment is installed properly in the right locations. When dealing with EMSEC you need to go a little bit further in the inspection process. This is because you must ensure all measures have been taken to suppress compromising emanations **before** initial application of power. This chapter provides basic guidelines on how to conduct a pre-shakedown inspection for compliance with EMSEC installation criteria.

Prior to equipment shakedown tests, you should carefully evaluate the entire installation to ensure the integrity of mechanical supports, wire ways, conduit, shields, and hardware brazing. You must also inspect all power lines, signal lines, and grounds for proper connectivity. Lastly, you must ensure each piece of equipment is installed IAW standard installation practices and it complies with TEMPEST technical specifications. Follow the guidance in your project package, NCCSCR 700-17, and this chapter to double check your work.

## BASE EMSEC MANAGER ASSISTANCE

The Base EMSEC Manager is also obligated to evaluate the installation and uses AFI 33-203 to perform a RED/BLACK EMSEC inspection. Since NCCSCR 700-17 does not cover RED/BLACK inspections in detail and the Base EMSEC Manager should be well versed in TEMPEST installation criteria, it makes good sense that you jointly look over the installation. If possible, request the assistance of the Base EMSEC Manager when you perform your pre-shakedown inspection. Together, you may be able to identify installation discrepancies or future problem areas that can be affected now.

Basically, the remainder of this chapter is a series of items you should look at during your pre-shakedown inspection. It isn’t intended to cover 100% of every possible check; it provides general items to check and what to look for. It's a good idea to inspect one particular area at a time; i.e., equipment layout, conduit, ducts, etc. We’ll start with the power distribution systems.

## POWER DISTRIBUTION

Before starting the pre-inspection, review the applicable project package task instructions and project drawings to refresh your memory. Using the 31-1-series TOs and project package, examine the power distribution that you installed. Pay special attention to RED/BLACK installation criteria in addition to standard installation requirements.

- ✔ Trace power runs, as necessary, from distribution boxes back to source to ensure there are no cross connects between technical and non-technical loads. Verify correct spacing between power runs, and between power and signal runs.
- ✔ Inspect all power panels to ensure RED and BLACK power is distributed separately. Under no circumstances should RED and BLACK power be distributed from the same panel. Ensure RED panels are located in RED areas and BLACK panels are located in BLACK areas. RED panels must be RFI tight.
- ✔ Trace the AC power lines, both RED and BLACK, to each applicable equipment end item. Ensure all power lines are installed in metallic conduit or wire ways and that RED power serves RED equipment and BLACK power serves BLACK equipment. Also, make sure no signal lines were placed in ducts, conduit, or wire ways which contain power leads.
- ✔ When verifying RED and BLACK power distribution to equipment, also check for proper FPSS conductor terminations on equipment ground terminals. Verify correct hookup of power phase and neutral conductors to each equipment end item. BE SURE phase, neutral, and FPSS conductors are NOT reversed.
- ✔ Check RED power conduit, ducts, and wire ways to ensure that RFI gaskets have been correctly installed. Be sure the correct RFI gasket material is used and installed IAW technical instructions.
- ✔ Inspect RED equipment power input to verify correct installation of filters. If power filters are not installed within the RED processing equipment, then RED power must be routed through a filter panel. Trace power leads to ensure proper hookup from power source, through filters, to the RED processing equipment. Also check to ensure bleed resistors (if required) are installed.

Now that you have finished inspecting the power distribution, let's take a look at signal line distribution.

## SIGNAL LINE DISTRIBUTION

When inspecting signal line distribution, keep an eye out for RED/BLACK discrepancies involving spacing, crossover, shielding, and termination. Use your drawings and task instructions in your project package, as well as the TEMPEST directives, to ensure correct signal line distribution.

- ✔ Trace all signal lines from each RED equipment end item through intermediate equipment to termination points. If RED signal lines transverse a BLACK area, they must be encased in a Protected Distribution System (PDS). Make sure the PDS meets all installation criteria specified in MIL-HDBK-232A.
- ✔ Trace BLACK signal lines through intermediate equipment (IDFs, junction boxes, modems, repeaters, etc.) to termination points. Ensure BLACK signal lines are not intermingled with RED and do not transverse a RED area. Be sure BLACK signal lines are NOT run in RED wire ways.
- ✔ Check filters installed in an RFI cabinet to ensure they are firmly bonded to the cabinet walls and the cabinet is firmly bonded to the equipotential ground plane. Also ensure correct installation of RFI gaskets.
- ✔ Verify all signal and control lines are installed in ferrous conduit and all single data processing cables have at least one overall nonferrous shield.
- ✔ Inspect RED conduits and ducts for proper marking as directed by NACSIM 5203 and AFSSM 7011. Ensure all BLACK wire ways are marked IAW TO 31-10-27, if required.

Once you verify correct signal line distribution, closely inspect the equipment.

## EQUIPMENT CONFIGURATION

Use the task instructions and drawings from your project package to inspect the equipment for compliance with TEMPEST installation criteria. Double check to ensure correct equipment placement and adherence to RED/BLACK spacing requirements.

Remember to first identify the equipment type and the keying level. Refer to MIL-HDBK-232A, Tables I and II, as necessary to verify equipment spacing.

- ✔ Check the equipment separation distances for compliance with RED/BLACK spacing criteria. Ensure all blank panels are in place and equipment is properly located IAW the project package.

- ✔ Ensure proper location of all distribution frames (RED in RED area, BLACK in BLACK area). Also, spot check terminations for compliance with TEMPEST criteria.
- ✔ Check location of patch panels and ensure there is proper separation between RED and BLACK jack fields. If physical separation is not feasible, make sure dissimilar wiring or dissimilar jack fields are installed to prevent RED/BLACK cross patching.
- ✔ Check for proper location and distance of administrative telephones and intercoms from RED equipment. In addition to MIL-HDBK-232A, refer to NACSIM 5203 for spacing specifications.

While inspecting the equipment, make necessary floor plan and other drawing corrections. We also recommend any RED processing non-developmental equipment be flagged on the drawings to indicate equipment is not TEMPEST approved.

Again review your project package for other RED/BLACK specifications which should be checked during your pre-shakedown inspection. Make other checks as necessary.

## GROUNDING AND BONDING

When you inspected the signal lines and equipment, you probably also checked part of the grounding system and observed some bonding. It's a good idea to make a final check of grounding hookups and make sure all hardware is correctly bonded. This is a difficult inspection as RED and BLACK ground potentials tied together are not necessarily visible. Make cursory checks; if you find an improper ground connection or incomplete bonds, dig deeper. If the Base EMSEC Manager is not with you on this inspection, it's wise to request his or her assistance to help identify conditions which could cause compromising emanations.

- ✔ Check a portion of equipment signal grounds to ensure the signal reference subsystem is properly connected to the EESS. Ensure separate grounds are run for each piece of equipment.
- ✔ While checking ground termination points, ensure all connections are properly bonded to the EESS. When pressure connectors are employed, make sure they are tight.
- ✔ Trace several signal grounds from equipment to termination point. Make sure each is a single continuous run with no breaks, splices, braids, or solder connections.

## SUMMARY

The purpose of a pre-shakedown inspection is to discover and correct discrepancies prior to equipment shakedown. A thorough inspection at this point is especially important to ensure compliance with RED/BLACK specifications. Take your time and use the collective expertise of the entire team. If you need help, get the Base EMSEC Manager involved. Remember, a good pre-shakedown inspection and correction of installation disparities aid in equipment shakedown and significantly reduce the potential of radiating compromising emanations.

# CHAPTER 8
# TEAM CHIEF DUTIES

Everyone who has been in the EI business for any length of time knows the overall responsibility for an installation rests on the Team Chief's shoulders. The Team Chief oversees it all, from the morale and welfare of the team members, to the quality of work, successful operation, and commissioning of the equipment or facility. In addition to the installation itself, the Team Chief also performs project reviews, pre-implementation surveys, continuous training, and a whole group of documentation. Most Team Chief skills are taught in the Team Chief Academy and learned on the job. This chapter does **NOT** rehash general Team Chief duties. It does, however, explain the extra considerations necessary to comply with TEMPEST criteria as the Team Chief begins a project review and pre-implementation survey. The most obvious place to start is the beginning: the project review.

## PROJECT REVIEW

As an EI Team Chief you've probably performed countless project reviews. Each project has its own individual problem areas which, when identified beforehand, can save a *lot* of frustration and man-hours once the project is underway. Therefore, pay special attention to EMSEC requirements whenever you perform a project review. Following are some TEMPEST-related areas you need to closely scrutinize as you review the package.

### TAB A AND TAB B

The TEMPEST related parts of a project package are found in Tabs A and B.

- *TAB A.* What you are interested in here is the project package cover (AFCC Form l), project number, and portions of the List of Materials (LOM), notably sections 3 and 5, which may contain information on TEMPEST equipment or requirements. These parts of the project package can provide insight as to whether TEMPEST requirements exist. The project number and LOM are covered in more detail later in the chapter.
- *TAB B.* The TEMPEST related items in Tab B are the installation description and special instructions, Table 1 (Drawing List), Table 2 (Publication List), and Task Instructions. Also included are attachments such as Testing Forms, Program Support Agreement (PSA), and C4 Systems

Support Requirements. We'll go into more detail about these later. First, let's consider some references you may need.

**REFERENCES**

Below are a series of references that may come in handy when reviewing a project package for EMSEC restrictions. The number, size, and type of TEMPEST installations performed by your team dictate which publications are required when you perform a project review.

- CSCR 700-17, Chapter 4, of the Team Chief Handbook, provides the guidelines you should follow when performing a project review. Refer to the other directives listed below for specific TEMPEST-related guidance.
- AFI 33-203, The Air Force Emission Security (EMSEC) Program. This security instruction addresses Air Force procedures and policies on controlling compromising emanations.
- AFSSI 3030, Protected Distribution Systems (FOUO). Provides instructions and guidance for placement, cable routing, and inspection/certification of Protect Distribution Systems.
- AFSSM 7011, The Emission Security Countermeasures Review. It provides guidance for making the emission security countermeasures review for the control of compromising emanations, NONSTOP, and HIJACK.
- AFNAG-l, Criteria for Installing Secure Voice Equipment in Fixed Facilities. This document is Confidential. It contains criteria for installing secure voice equipment in communications centers, offices, command posts, and private residences. It explains how to obtain certification to process classified information, and contains checklists for inspecting a facility for compliance with TEMPEST installation criteria.
- MIL-HDBK-232A, RED/BLACK Engineer Installation Guidelines, covers unclassified RED/BLACK standards for TEMPEST installations.
- NACSIM 5203, Guidelines for Facility Design RED/BLACK Installation. This document is classified Confidential (No Foreign Nationals). This publication also provides guidance on RED/BLACK standards for TEMPEST installations.
- Approved Products List (APL). This is an unclassified listing of equipment which meets NACSIM 5100A (Compromising

Emanations, Laboratory Test Requirements, Electromagnetic) design standards for approved TEMPEST systems. It's available through the Base IP Office.

- TEMPEST PROFILE DATA List (TPDL). This document is Confidential and identifies power requirements and physical control space restrictions for equipment not meeting NACSIM 5100A design standards.
- MIL-STD-188-124B, Grounding, Bonding, and Shielding. This Military Standard establishes certain grounding standards for TEMPEST installations.
- MIL-HDBK-419A V2, Grounding, Bonding, and Shielding for Electronic Equipment and Facilities. This handbook covers basic grounding and bonding and also contains other TEMPEST installation information.
- TO 31-10-24, Grounding, Bonding, Shielding. A technical order providing setup and installation methods for grounding, shielding, lightning suppression, and bonding techniques.

While you may not be required to use every one of the above directives, it's a good idea to have them available. Your unit EMSEC Manager should have them on file. If not, then check with the Base EMSEC Manager. If not on file in your unit publications library, we recommend you establish requirements for the unclassified publications through your Customer Account Representative (CAR).

Now that you're aware of some references you may need to perform a project review, let's briefly discuss project review guidelines as they relate to TEMPEST installations.

## REVIEW PROCEDURES

You should follow standard project package review procedures for TEMPEST installations. As you perform the review, make note of all instructions, requirements, specifications, and restrictions related to TEMPEST criteria. Ensure compliance with TEMPEST requirements.

As you normally would, start off by inventorying all the parts of a project package to ensure it's complete. Starting with the cover sheet on TAB A, review each project package element from beginning to end for potential TEMPEST restrictions.

- ***Tab A***. Tab A consists of AFCC Form 1 and the List of Material (LOM).

1. Review all support letters for TEMPEST related requirements, such as installation of ground planes. Ensure the specifications and references cited in each agreement comply with TEMPEST criteria. For example, if a RED power panel is to be installed by the host base it must be dedicated for RED power requirements and not be used to supply power for existing BLACK equipment.
2. Look over the LOM to identify any RED equipment items. Section 3 identifies minor equipment items with NSNs. It also contains COMSEC equipment supplied by Air Force Intelligence Command. Section 5, Remarks, may contain miscellaneous information relating to TEMPEST criteria. Cross reference these items to the PPL and TPDL to identify applicable TEMPEST restrictions. If the equipment does not meet PPL requirements, then additional measures must be taken during installation to ensure TEMPEST integrity.

- ***Tab B***. Tab B consists of installation description and task instructions.

3. Carefully review each task instruction for compliance with TEMPEST criteria. Make sure the instructions do not create potential for compromise. If you identify possible problems, refer to the above directives or consult your Project Engineer for assistance.
4. Closely review each drawing listed in Table 1, Drawing List, for equipment layout. Ensure the elevation views identify correct locations IAW RED/BLACK installation criteria. Also check equipment location on the floor plans. Refer to the LOM to identify whether or not processing equipment is TEMPEST approved. Look again at the floor plans to ensure correct equipment spacing. Ensure compliance with ERTZ requirements to prevent potential compromises.
5. Check the publication list on Table 2. Are the applicable regulations and TOs needed for the installation called out? Refer to the TEMPEST-related directives listed in this chapter and identify any additional publications you may need during the installation.
6. Review all TAB B attachments to include Testing Forms, the Program Support Agreement (PSA), and any C4 Systems Support Requirements. Check the testing forms to see if a test plan is required and, if so, its classification. Check the PSA to see what the host base support is for the project. Some PSAs task the host base to provide and maintain the COMSEC equipment you install. It states whether TEMPEST

considerations will be required or not. If required, the PSA identifies the customer O&M unit with crypto maintenance responsibility. This is critical because unauthorized personnel working on COMSEC equipment is not only a physical security violation but could result in damaging the TEMPEST integrity of the equipment.

7. Check the C4 Systems Support requirements. There must be task certified personnel to perform operational checks, perform maintenance, and certify the facility after installation by the EI Team. Tasking for this support is made by the on-site EDI team chief and depends upon the non-availability of certified EI team members. Once again, ensure only certified maintenance personnel work on COMSEC equipment in order to prevent security violations and protect equipment TEMPEST integrity.

**DOCUMENTATION**

Review your findings and document them on AFCC Form 262, Record of EI Project Review and, if necessary, AFCC Form l44, Narrative. You may or may not be able to contact the Project Engineer and discuss your findings. Obviously, you can't discuss classified information on the phone. Also, there are certain restrictions when reviewing TEMPEST-related packages, we'll cover these later. For now, let's assume there are no major discrepancies and the project can proceed without any engineering changes. Your next step is to take a team to the project location and perform a pre-implementation survey.

## PRE-IMPLEMENTATION SURVEY

Once on site, you must verify allied support was completed IAW with the PSA and perform a thorough equipment inventory. Pay special attention to ensure full compliance with TEMPEST criteria.

## SITE AND PROJECT INSTALLATION DATA

Inspect the facility against the floor plans to verify equipment can be installed in identified locations. Check to verify equipment location complies with applicable TEMPEST directives and meets all RED/BLACK spacing requirements. If there are deviations to RED/BLACK equipment location and spacing standards, the customer must have a valid waiver.

## ALLIED SUPPORT

TEMPEST-related allied support items you should closely inspect during the pre-installation survey include the grounding system, shielded enclosures (if required), and power distribution. In some cases, your team may be installing part or all of these subsystems. If some of the areas are unfamiliar to you, it may be beneficial to request assistance from the Base EMSEC Manager.

1. Check records of the facility ground system to ensure is does not exceed 10 ohms.
2. Check the records of the Earth Electrode Subsystem (EESS) for compliance with the requirement of 10 ohm maximum resistance.
3. Visually inspect all power runs to ensure they are enclosed in nonferrous conduit and are properly identified. Verify correct distribution of technical power and there is no mixing of technical and non-technical power. Make sure power distribution boxes are properly located and separate boxes are used for RED and BLACK distribution. Check for bleeder resistors in the filter box (if installed).
4. Inspect and verify RED/BLACK areas are properly identified and isolated from each other IAW the project package.

## COMMUNICATIONS SUPPORT

During the pre-implementation survey, you should verify classified equipment and items required to perform operational tests have been received or are on order. Requisitioning such items as COMSEC equipment and ancillary devices, spare parts and circuit board kits, and classified and unclassified crypto keys is normally accomplished by the COMSEC custodian, crypto maintenance workcenter, or both.

## MAINTENANCE SUPPORT

While checking, the status of equipment, you can also coordinate maintenance support to be provided by the O&M unit crypto maintenance work center. Normally the O&M unit for which you are installing the equipment is obligated to support your team by obtaining “C” coded items and providing certified personnel to assist in the installation and perform operational checks and maintenance as needed. The results of their tests are normally used to verify operational capability leading to facility or equipment commissioning. If you have any problems, talk to the O&M unit Chief of Maintenance.

## DOCUMENTATION

During the course of your pre-implementation survey you should be taking notes. Along with obvious discrepancies, you may have numerous questions on items you're not 100% sure of. Prior to documenting your findings, it may be a good idea to check out your findings with the Base EMSEC Manager. He or she may be able to clarify gray areas and verify whether or not a valid discrepancy exists. The best rule of thumb is, if in doubt document it on AFCC Form 250. Remember though, as mentioned previously, you just can't pick up the phone and discuss classified discrepancies with your boss or the project engineer. You must always exercise full security measures when dealing with classified information. Let's look over some of the important security precautions you must always practice.

## DOCUMENTING DISCREPANCIES AND EXCEPTIONS

The whole purpose of this handbook is to identity and discuss the unclassified portions of TEMPEST installations. It would probably be impossible to install equipment in a TEMPEST facility and not become involved with some type of classified information or equipment. While conducting a project review, performing a pre-implementation survey, and during the installation, there will be times when you must discuss classified information with someone. As you already know, there are many restrictions with which you must comply to prevent security compromises. Let's take a look at some security precautions you must apply at all times.

## PRECAUTIONS

Number one is the golden rule to not discuss classified information on the phone or write it down. Everyone knows that; however, a lot of times we may attempt to talk around classified subjects. Obviously, this is a no-no; don't be guilty of possibly exposing classified information in the name of just trying to do your job. Even though you may have the best intentions, it makes little difference in a compromise situation. Most units have at least one STU III terminal. You should have one in your unit, and the communications squadrons in the field should also have them. Discuss classified business over a STU III in the secure mode. Incorporate your questions or findings in a message to the engineer. Make sure the message is appropriately classified before release.

If you are not sure of or cannot locally resolve a problem, classify your work until you receive competent guidance to do otherwise.

The Base EMSEC Manager will assist you in this. It's best to be overly cautious when dealing with potential classified information than to risk a security compromise. If a project exception reveals a security weakness, the completion certificates will be classified. Guidance in this situation can be supplied by the Base EMSEC Manager. Any specific guidance and instructions received will be in writing and classified as necessary.

**DOCUMENTATION PROTECTION**

Just as important as not discussing classified information is making sure documented classified information is afforded the degree of protection dictated by its level of classification. There may be times during the project review, pre-implementation survey, or during or after the installation, when you must document classified information. Most classified documentation requirements are noting discrepancies, updating drawings, or communicating with the project engineer or program manager. Remember, when you must document classified information or deal with classified documents, protect them at all times.

1. If changes to a classified blueprint, photo, or drawing are required, they become attachments to AF Form 1146. While in your possession, take measures outlined in AFR 205-1, Information Security Program, to safeguard classified documents. The Base EMSEC Manager will help you classify documents and determine the proper method to disseminate classified correspondence.

2. AF Form 1261, Information Systems Acceptance, Commissioning and Removal Certificates, is used to document whether or not the installed equipment meets the TEMPEST criteria specified in the Project Support Agreement or Communications-Electronic Project. In the description portion of AF Form 1261, enter only the Standard Facilities and Equipment Listing (SFEL) designator if the equipment is classified. If the equipment is unclassified, the AF Form 1261 is processed normally. Now let's discuss actions to be taken if discrepancies are discovered.

**DISCREPANCIES AND EXCEPTIONS**

Project discrepancies discovered during testing are usually corrected on-the-spot. If they cannot be corrected, they will be exceptions to the project. Rarely will you complete a project without some exceptions. Exceptions to C-E projects are grouped into two categories: minor and major.

1. *Minor* exceptions do not keep the C-E facility or system from meeting operational requirements, but keep it from meeting all installation criteria. A key point here is that the system, equipment, or facility must meet all TEMPEST installation criteria. If it doesn't then it becomes a major exception. Minor exceptions are cleared by the EI Team or by the customer. Document on the AF Form 1261 the exception, forecast date of correction, responsible activity, and the date corrected, if applicable.
2. *Major* exceptions keep the C-E facility or system from meeting the specified operational requirements. This could be the result of not following proper RED/BLACK installation criteria or faulty equipment. The EI team will correct all discrepancies if possible. If not, the facility may not be commissioned until the major discrepancy is cleared or a waiver is approved. In extremely rare cases, the customer will accept the project with a major exception. An Acceptance of TEMPEST Risk (AOR) is generated by the customer through the Base EMSEC Manager, and the AF Form 1261 is signed relieving EI of all responsibility for the project.

## SUMMARY

Performing project reviews for TEMPEST installations is a critical step in the installation process. Carefully examine the project package for any problem areas. The identification and correction of problems at the beginning saves time, manpower, and money when the installation is underway. While performing a pre-implementation survey, ensure all support is available and that there are no deviations from the project package requirements. When dealing with material of a sensitive nature, be sure to take proper security precautions. It’s tempting to try to talk about a TEMPEST problem over the phone with the project engineer; unless the phones are secure, don't try it. By adhering to proper installation methods IAW RED/BLACK installation criteria you can prevent the loss of compromising emanations and enable the Air Force to perform its mission in a secure environment.