NSTISSAM TEMPEST/2-95
12 December 1995

NSTISS

NATIONAL
SECURITY
TELECOMMUNICATIONS
AND
INFORMATION
SYSTEMS
SECURITY

RED/BLACK INSTALLATION GUIDANCE

FOR OFFICIAL USE ONLY

NSTISS

NATIONAL SECURITY
TELECOMMUNICATIONS
AND INFORMATION
SYSTEMS SECURITY

NATIONAL MANAGER

FOREWORD

1. National Security Telecommunications and Information Systems Security Advisory Memorandum (NSTISSAM) TEMPEST/2-95, *RED/BLACK Installation Guidance* specifies RED/BLACK equipment/system installation guidance, provides an explanation of the TEMPEST policy concept, and addresses RED/BLACK considerations for facilities wherein national security information is processed. This publication supersedes National COMSEC Information Memorandum (NACSIM) 5203, dated 30 June 1982. However, Appendix K of NACSIM 5203 will remain in effect until NACSI 4009, *Protected Distribution Systems*, dated 30 December 1981, is superseded. NACSI 4009 is currently under revision.

2. TEMPEST security is a function of the TEMPEST characteristics of the processing equipment, the way the equipment is installed, the electromagnetic and physical characteristics of the facility, and the geographical environment where the facility is located.

3. The guidance identified herein will be considered by a Certified TEMPEST Technical Authority (CTTA) as part of the potential solution for facilities, system, and equipment that have been identified as requiring TEMPEST countermeasures. Only those specific criteria identified by the CTTA will be implemented.

4. Representatives of the National Security Telecommunications and Information Systems Security Committee may obtain additional copies of this instruction from:

Executive Secretariat
National Security Telecommunications and
Information Systems Security Committee
National Security Agency
Fort George G. Meade, MD 20755-6000

5. U.S. Government contractors are to contact their appropriate government agency or Contracting Officer Representative regarding distribution of this document.

/S/
J. M. McCONNELL
Vice Admiral, U.S. Navy

FOR OFFICIAL USE ONLY

NSTISSAM TEMPEST 2/95A
3 February 2000

AMENDMENT TO ADVISORY MEMORANDUM
TEMPEST 2/95
RED/BLACK INSTALLATION GUIDANCE

Includes change pages in place

THIS DOCUMENT PROVIDES MINIMUM STANDARDS. FURTHER IMPLEMENTATION MAY BE REQUIRED BY YOUR DEPARMENT OR AGENCY

NATIONAL MANAGER

FOREWORD

1. NSTISSAM TEMPEST 2/95, RED/BLACK Installation Guidance has been amended to clarify the recommendations for installation which are presented in Recommendations A through I. Please replace pages 17, 18, 19, 20, 21, 22, 27, 28, 41, and 42 in your current document with the enclosed and destroy the replaced pages. These minor changes have been approved by the TEMPEST Advisory Group.

2. Representatives of the National Security Telecommunications and Information Systems Security Committee (NSTISSC) may obtain additional copies of this instruction from the Secretariat at the address listed below.

/s/
MICHAEL V. HAYDEN
Lieutenant General, USAF

pages changed

NSTISSC Secretariat (V503) • National Security Agency • 9800 Savage Road STE 6716 • Ft Meade MD 20755-6716
(410) 854-6805 • UFAX: (410) 854-6814
nstissc@radium.ncsc.mil

TABLE OF CONTENTS

SECTION 1 - INTRODUCTION 1
1.1. General 1
1.2. Scope 1
1.3. Content 1
1.4. Revision 1
1.5. Policy 1
1.6. Application 1
1.7. Comments and Recommendations 1
1.8. References 2
1.8.1. Government Documents and Publications 2
1.8.2. Government Documents 3
1.8.3. Non-Government Publications 4

SECTION 2 - DEFINITIONS 5

SECTION 3 - RED/BLACK INSTALLATION RECOMMENDATIONS 7
3.1. General 7
3.2. Installation Recommendations 7
3.3. Use of Table 3-1 7
3.4. TEMPEST Guidance 8
RECOMMENDATION A 11
RECOMMENDATION B 13
RECOMMENDATION C 15
RECOMMENDATION D 17
RECOMMENDATION E 19
RECOMMENDATION F 21
RECOMMENDATION G 23
RECOMMENDATION H 25
RECOMMENDATION I 27

SECTION 4 - GUIDANCE FOR TEMPEST INTEGRITY 29
4.1. General 29
4.2. TEMPEST Basics 29
4.2.1. Generation of CE 29
4.2.2. CE Sources 29
4.2.2.1. Functional Sources 29
4.2.2.2. Incidental Sources 29
4.3. RED/BLACK Basics 29

4.3.1. Facility Considerations 30
4.3.2. Physical Security Considerations 30
4.4. Signal Cables 30
4.4.1. Shielded Metallic Cables 30
4.4.1.1. Cable Characteristics 30
4.4.1.2. Shield Termination 30
4.4.2. Optical Fiber Cables 31
4.4.2.1. Applications of Optical Fiber Cable Systems 31
4.4.2.2. Multifiber Cables 31
4.4.2.3. Cable Strength Members or Shielding 31
4.5. Signal Distribution 31
4.5.1. Wireways 32
4.5.2. Patching Equipment 32
4.5.3. Distribution Equipment (Wire Closets) 32
4.5.4. Protected Distribution Systems 32
4.6. Signal Line Isolators and Filters 32
4.6.1. Signal Line Isolation 32
4.6.2. Assessing the Need for Signal Isolation 33
4.6.3. Passive Signal Line Filters 33
4.6.3.1. Lowpass Filters 33
4.6.3.1.1. Analog Signal Line Filters 33
4.6.3.1.2. Inductive-Capacitive (LC) Signal Line Filters 33
4.6.3.1.3. Digital Signal Line Filters 34
4.6.4. Active Signal Line Filters 34
4.6.4.1. Linear Filters 34
4.6.4.2. Saturated Amplifiers 34
4.6.5. Isolators 35
4.6.5.1. Magnetic-coupled Isolators 35
4.6.5.2. Acoustic-coupled Isolators 35
4.6.5.3. Photon-coupled Isolators 35
4.6.5.3.1. Signal Line Isolators 36
4.6.5.3.2. Advantages of Photon-coupled Isolators 36
4.7. Power Distribution 36
4.7.1. The Power Requirement 36
4.7.2. Power Conditioning/Isolation 37
4.7.2.1. Powerline Filters 37
4.7.2.2. Isolation Transformers 38
4.7.2.3. Uninterruptible Power Supplies and Power Regulators 38
4.7.2.3.1. Solid-state UPS (SSUPS) 38
4.7.2.3.2. Rotating UPS 38
4.8. Grounding System 38

4.8.1. Equipotential Plane 38
4.8.2. Single Point Ground 39
4.8.3. Fault Protection Ground 39
4.8.4. Isolated Ground 39
4.9. Administrative Support Equipment 39
4.9.1. Telephone Systems 40
4.9.1.1. TEMPEST Protective Measures 40
4.9.1.2. On-hook Security 40
4.9.2. Paging, Intercom, and Public Address Systems 40
4.9.3. Alarm Systems 40
4.9.4. Miscellaneous Fortuitous Conductors 41
4.9.5. Radio Transmission or Reception Devices 41
4.9.6. Commercial Television System Installation 41
4.10. Other Considerations 42
4.10.1 TEMPEST Zoning 42
4.10.2. Inspectable Space 42
4.10.3. Facility Shielding 42
4.10.4. TEMPEST Suppressed Equipment 42

SECTION 5 - SECURE VOICE SYSTEMS 43
5.1. General 43
5.2. Basis for Minimum Installation Techniques 43
5.3. Installation Guidance 43
5.3.1. General 43
5.3.2. Multiple Terminal Installations 43
5.3.3. Location 43
5.3.4. High-risk Areas 43
5.4. Security Guidance 43
5.4.1. Terminals with Multiple Handsets 43
5.4.2. Location of Equipment 44
5.4.3. High-risk Areas 44
5.5. STU-III Guidance 44

SECTION 6 - SENSITIVE COMPARTMENTED INFORMATION 45
6.1. General 45
6.2. Routing of SCI Cables 45
6.3. Termination Boxes 45
6.4. Distribution Frame 45
6.5. Patch Panels 45
6.6. Multiplexers, Video and Audio Switches, and Other Multiple Circuit Equipment . . 46

6.7. Access Points 46
6.8. Cables 46
6.9. Low-level Signaling 46
6.10. Power and Signal Line Filtering 46
6.11. Standard Service Features 46
6.12. Telephone Lines 47
6.13. RED/BLACK Separation 47
6.14. Additional Requirements 47

SECTION 7 - TRANSPORTABLE SYSTEMS IN A TACTICAL ENVIRONMENT 49
7.1. General 49
7.2. Modes of Operation 49
7.2.1. Fixed Operation 49
7.2.1.1. RED Cables 49
7.2.1.2. Separation 49
7.2.1.3. CTTA Review 49
7.2.2. Field Deployed 49
7.2.3. Vehicular Mounted 49
7.3. Deploying Equipment Away from Transportables 50
7.4. Physical Security 50

SECTION 8 - AIRCRAFT 51
8.1. General 51
8.2. Aircraft Installations 51
8.2.1 . Airborne Operations 51
8.2.1.1. RED Cables 51
8.2.1.2. Separation 51
8.2.1.3. Grounding 51
8.2.2. Ramp Operations 51
8.2.3. Physical Security 51

SECTION 9 - SHIPS 53
9.1. General 53
9.2. Shipboard Installations 53
9.2.1. Underway Operations 53
9.2.1.1. RED Cables 53
9.2.1.2. Separation 53
9.2.1.3. Shielded Cables 53
9.2.1.4. RED Ground 53
9.2.1.5. Cryptographic Equipment Ground 53
9.2.1.6. Cable Distribution 53

9.2.2. In Port Operations 53
9.2.3. Physical Security 53
Comment Form for NSTISSAM TEMPEST2/95 55

THIS PAGE IS INTENTIONALLY LEFT BLANK

SECTION 1

INTRODUCTION

1.1. General. This section contains introductory and administrative information associated with this document.

1.2. Scope. This document defines the guidance to consider during the design of facilities and for subsequent installation of equipment and systems that receive, transmit, manipulate, graph, store, archive, calculate, generate, print, or in any other manner process national security information. This guidance is part of the potential solution for facilities, systems and equipment identified as requiring TEMPEST countermeasures.

1.3. Content. The text includes a brief overview of the TEMPEST national policy and provides RED/BLACK installation guidance that may be identified by the Certified TEMPEST Technical Authority (CTTA) as part of the solution for systems and facilities that require the application of TEMPEST countermeasures.

1.4. Revision. This document correlates to the previous issue (NACSIM 5203) in concept only. The content has been extensively changed and reorganized to reflect current policy considerations and emerging technology.

1.5. Policy. The *National Policy on the Control of Compromising Emanations* (NSTISSP 300) and its implementing instructions, *TEMPEST Countermeasures for Facilities* (NSTISSI 7000), and *NONSTOP Countermeasures* (NSTISSI 7001) establish the policy that certain systems and facilities that process national security information (NSI) must be reviewed by a CTTA. If such a review is required and the review determines that TEMPEST countermeasures are required, the CTTA will consider a variety of methods that can be applied to the system/facility to achieve TEMPEST security. The RED/BLACK guidance contained in this document will be considered by the CTTA along with other measures (e.g., TEMPEST Zoning, TEMPEST suppressed equipment and shielding) to determine the most cost-effective countermeasures to achieve TEMPEST security. Only those RED/BLACK criteria specifically identified by the CTTA will be implemented.

1.6. Application. The guidance contained herein, when specified by a CTTA, is applicable to U.S. Government departments, agencies and contractors.

1.7. Comments and Recommendations. Revisions to this publication will be made as appropriate. Comments and recommendations are encouraged. Government organizations should submit their comments to their appropriate government or agency authority. Department and agency authorities may submit their comments to:

Attn: C3
Department of Defense
National Security Agency
Fort George G. Meade, Maryland 20755-6000

Contractors should submit their comments regarding this publication to their contracting government organization. Industrial firms that have no government TEMPEST-related contact may address their comments to the above address. A comment form is provided at the end of this document for this purpose. When submitting comments, this form may be reproduced or a similar format may be used.

1.8. References. The following references contain information that supplement the information contained herein. The effective editions of these references should be reviewed by persons involved in performing engineering and installation of equipment and systems that process national security information.

1.8.1. Government Documents and Publications. The following government documents and publications form a part of this document to the extent specified herein. Unless otherwise specified, the issues of these documents are those currently listed in the applicable publication index.

AIR FORCE (AF)

TPDL	(C) TEMPEST Profile Data List

DIRECTOR CENTRAL INTELLIGENCE DIRECTIVE (DCID)

DCID 1/21	*(U) Implementation Manual for Physical Security Standards for Sensitive Compartmented Information Facilities*

FEDERAL COMMUNICATIONS COMMISSION (FCC)

FCC Reg Part 15 Subpart J	*(U) Rules and Regulations, Radio Frequency Devices; Computing Devices*

JOINT CHIEFS OF STAFF

JCS Pub 1	*(U) Dictionary of Military and Associated Terms*

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST)

FIPS PUB 94	*(U) Guideline on Electrical Power and ADP Installations*

NATIONAL SECURITY AGENCY (NSA)

ISSO — *(U) INFOSEC Products and Services Catalogue*

Contents:

- Endorsed CRYPTO Products List
- NSA-Endorsed DES Products List
- Protected Network Services List
- Eval Trusted Computer Systems List
- Preferred Products List
- Endorsed Products List
- NSA Degausser Products List

(The above publication is obtained by ordering from the Government Printing Office (GPO) as a single copy or as a yearly subscription. Price is subject to change - it will be given at time of order. Requests for copies or subscription should be addressed to: Superintendent of Documents, U.S. Printing Office, Washington, DC 20402).

National TEMPEST Information Center	*(U) TEMPEST Zone Assignments for Information-Processing Equipment*

NATIONAL SECURITY TELECOMMUNICATIONS AND INFORMATION SYSTEMS SECURITY COMMITTEE (NSTISSC)

NACSI 4009	*(C) Protected Distribution Systems*
NACSIM 5000	*(C) TEMPEST Fundamentals*
NSTISSAM TEMPEST/1-92	*(C) Compromising Emanations Laboratory Test Requirements, Electromagnetics*
NSTISSAM TEMPEST/2-92	*(FOUO) Procedures for TEMPEST Zoning*
NSTISSAM TEMPEST/1-93	*(C) Compromising Emanations Field Test Requirements, Electromagnetics (U)*
NSTISSAM TEMPEST/1-95	*(U) Shielded Enclosures*
NSTISSI No.7000	*(C) TEMPEST Countermeasures for Facilities*
NSTISSI No.7001	*(S) NONSTOP Countermeasures*
NSTISSI No.7002	*(S) TEMPEST Glossary*
NSTISSP No.300	*(C) National Policy on Compromising Emanations*

1.8.2. Government Documents. The following government documents form a part of this document to the extent specified herein. Unless otherwise specified, the issues of these documents are those that are currently listed in the applicable publication index.

HANDBOOKS

MIL-HDBK-411	*(U) Power and Environmental Control for the Physical Plant of DoD Long-Haul Communications*
MIL-HDBK-419A	*(U) Grounding, Bonding, and Shielding for Electronic Equipment and Facilities*

SPECIFICATIONS

MIL-C-17	*(U) Cable, Radio Frequency, Flexible and Semirigid, General Specifications For.*
MIL-C-915	*(U) Cable and Cord, Electrical, For Shipboard Use, General Specifications For.*
MIL-C-23437	*(U) Military Specifications for Cable, Electrical, Shielded Pairs*
MIL-C-24640	*(U) Cable, Electrical, Lightweight for Shipboard Use, General Specifications For.*
MIL-C-24643	*(U) Cable and Cord, Electrical, Low Smoke, For Shipboard Use, General Specifications For.*
MIL-F-15733	*(U) Military Specifications for Filters, Radio Frequency Interference*

STANDARDS

FED-STD-1037	*(U) Glossary of Telecommunication Terms*
MIL-STD-188-100	*(U) Common Long-Haul and Tactical Communications Systems Technical Standards*
MIL-STD-188-111	*U) Subsystem Design and Engineering Standards for Common Long-Haul and Tactical Fiber Optic Communications*
MIL-STD-188-114	*(U) Electrical Characteristics of Digital Interface Circuits*
MIL-STD-188-124	*(U) Grounding, Bonding, and Shielding for Common Long-Haul/Tactical Communication Systems, including Ground Based Communication Electronics Facilities and Equipment*
MIL-STD-220	*(U) RFI Filters, Methods of Testing*
MIL-STD-1310	*(C) Shipboard Bonding, Grounding, and Other Techniques for Electromagnetic Compatibility and Safety.*

(Unless otherwise indicated, copies of Federal and Military specifications, standards, and handbooks are available from the Naval Publications and Forms Center, Attn: NPODS, 5801 Tabor Avenue, Philadelphia, Pa 19120-5099.)

TELEPHONE SECURITY GROUP

TSG 1	*(U) Introduction to Telephone Security*
TSG 2	*(U) TSG Guidelines for Computerized Telephone Systems*
TSG 6	*(U) TSG Approved Equipment*

1.8.3. Non-Government Publications. The following document forms a part of this document to the extent specified herein. Unless otherwise specified, the issue of this document is that currently listed in the applicable publication index.

TELECOMMUNICATIONS INDUSTRIES ASSOCIATION (TIA)

EIA-RS-232	*(U) Interface between Data Terminal Equipment and Data Circuit-terminating Equipment employing Serial Binary Data Interchange*

(Application for copies should be addressed to the Telecommunications Industries Association (TIA), Attn: Standard Sales Office, 2001 I Street NW, Washington, DC 20006)

NATIONAL FIRE PROTECTION ASSOCIATION, INC. (NFPA)

NFPA No. 70-1994	*(U) National Electrical Code® SECTION 250*

SECTION 2

DEFINITIONS

The terms in this document are defined in FED-STD-1037, JCS Pub 1, NACSI 4009, and NSTISSI 7002. For the purposes of this document, definitions are provided for the following terms, some that have been repeated from the foregoing publications for the convenience of the reader.

BLACK Equipment. A term applied to equipment that processes only unclassified and/or encrypted information.

BLACK Optical Fiber Line. An optical fiber that carries a BLACK signal or that originates/terminates in a BLACK equipment or system.

BLACK Line. An optical fiber or a metallic wire that carries a BLACK signal or that originates/terminates in a BLACK equipment or system.

BLACK Wire Line. A metallic wire that carries a BLACK signal or that originates/terminates in a BLACK equipment or system.

Bulk Filtering. The practice of using filters either at the first service disconnect or on each power panel and thereby filtering power to many items of equipment with one set of filters.

Certified TEMPEST Technical Authority (CTTA). An experienced, technically qualified U.S. Government employee who has met established certification requirements in accordance with NSTISSC-approved criteria and has been appointed by a U.S. Government department or agency to fulfill CTTA responsibilities.

Collateral. All national security information classified under the provisions of an executive order, for which special community systems of compartmentation [e.g., non-Special Compartmented Information (non-SCI), General Service Classified Information (GENSER)] are not formally established.

Commercial-off-the-Shelf (COTS). Commercially manufactured equipment that have no TEMPEST countermeasures intentionally built into them.

Common Wall Facility. A facility that shares a building, wall, floor or ceiling with uninspectable areas.

Compromising Emanations (CE). Unintentional signals that, if intercepted and analyzed, would disclose the information transmitted, received, handled, or otherwise processed by telecommunications or automated information systems equipment.

Equipment TEMPEST Zone (ETZ). A required secure distance (Zone) assigned an equipment based on the TEMPEST Electric field radiation characteristics of an equipment compared to the limits of NSTISSAM TEMPEST/1-92 (Zone A $\leq$ Level I; Zone B $\leq$ Level II; Zone C $\leq$ Level III; Zone D $>$ Level III).

Facility TEMPEST Zone (FTZ). A space assignment based on the measured ability of the facility structure to meet the limits of NSTISSAM TEMPEST/2-92.

Hardened Cable Path. A material, container or facility that provides physical protection for the cable and causes a delay to a perpetrator attempting unauthorized penetration or intrusion [e.g., a Protected Distribution System (PDS)].

Inspectable Space (IS). The three dimensional space surrounding equipment that processes classified and/or sensitive information within which TEMPEST exploitation is not considered practical or legal authority to identify and/or remove a potential exploitation exists.

National Security Information (NSI). Information that has been determined, pursuant to Executive Order 12958 or any predecessor order, to require protection against unauthorized disclosure, and that is so designated.

RED/BLACK Concept. Separation of electrical and electronic circuits, components, equipment, and systems that handle national security information (RED), in electrical form, from those that handle non-national security information (BLACK) in the same form. (Under this concept, RED and BLACK terminology is used to clarify specific criteria relating to, and to differentiate between, such items as circuits, components, equipment, systems etc., and also the areas where they are contained.)

RED Equipment. A term applied to equipment that processes unencrypted NSI that requires protection during electrical/electronic processing.

RED Optical Fiber Line. An optical fiber that carries a RED signal or that originates/terminates in a RED equipment or system.

RED Line. An optical fiber or a metallic wire that carries a RED signal or that originates/terminates in a RED equipment or system.

RED Wire Line. A metallic wire that carries a RED signal or that originates/terminates in a RED equipment or system.

TEMPEST Certified Equipment or System. Equipment or systems that have complied with the national requirements of NSTISSAM TEMPEST/1-92 Level I or previous editions.

Uncontrolled Access Area (UAA). The space in and around a building where no personnel access controls are exercised.

SECTION 3

RED/BLACK INSTALLATION RECOMMENDATIONS

3.1. General. There are many variables within a facility that can affect the opportunity for the collection of compromising emanations. Chief among these are the radiation characteristics of the information processing equipment, placement of signal and power cables, presence of fortuitous conductors, radio frequency (RF) attenuation of building materials, and the amount of inspectable space surrounding the facility.

3.2. Installation Recommendations. Table 3-1 summarizes the general RED/BLACK installation recommendations to meet NSTISSP No. 300, NSTISSI No. 7000 and NSTISSI NO. 7001 policy criteria. The matrix of the table for equipment and facilities with TEMPEST zone ratings was derived using guidance in NSTISSAM TEMPEST/2-92, *Procedures for TEMPEST Zoning.* **The cognizant CTTA must be consulted in the initial planning phases for facilities that will process classified information.** This is especially important for large projects where the architectural and engineering design and documentation phase is a major cost item. The CTTA has the responsibility for conducting or validating TEMPEST reviews and recommending TEMPEST countermeasures, including RED/BLACK installation measures. There should be no commitment of funds without CTTA concurrence. Failure to consult the CTTA could result in installation of unnecessary and/or expensive countermeasures or the omission of needed countermeasures.

3.3. Use of Table 3-1. The installation recommendations in Table 3-1 are for RED equipment (boxes along the left side) installed in one of three facility TEMPEST zones (boxes along the top side). The recommendations in the matrix are identified in the pages following the table.

- Facilities are listed by TEMPEST zone rating and surrounding inspectable space (IS). Facility zone ratings are the preferred method to determine facility TEMPEST characteristics since they are derived from the measured RF attenuation provided by the facility structure, the effects of fortuitous conductors, and the surrounding inspectable space. The inspectable space distances should be used only if the facility has not been TEMPEST zoned.

- Equipment TEMPEST zone ratings should be used if available. Zone D has been combined with Zone C for the purpose of defining the recommendations in this section. If an equipment has not been TEMPEST zoned and no TEMPEST profile data is available, the "All Other RED Equipment" category should be used.

- When installing a system that contains equipment with multiple zone ratings, the system should be installed in compliance with the most stringent equipment zone recommendations. For example, if a system containing equipment rated Zone A, Zone B and Zone C is to be installed in a Facility Zone C space, the entire system should be installed to meet equipment Zone C recommendations. The resulting recommendations are identified in the matrix box at the intercept that is three boxes to the right of the Equipment Zone C box and three boxes down from the Facility Zone C box. This identifies Recommendation I.

- Recommendation distances are stated in Metric units. The approximate English equivalents are:

Metric	English
2.5 cm	1 in
5 cm	2 in
15 cm	6 in
30 cm	12 in
50 cm	20 in
1 m	39 in
2 m	79 in
3 m	10 ft
8 m	26 ft
20 m	66 ft
30 m	98 ft
100 m	328 ft

3.4. TEMPEST Guidance. Section 4 contains TEMPEST-related guidance that will assist in the implementation of the recommendations contained in Table 3-1.

	FACILITY ZONE A Or inspectable space less than 20 m (Note 1)	FACILITY ZONE B Or inspectable space greater than 20 m but less than 100 m	FACILITY ZONE C Or inspectable space Greater than 100 m
EQUIPMENT meets NSTISSAM 1/92 Level I (Zone A)	Recommendation **A**	Recommendation **D**	Recommendation **G**
EQUIPMENT meets NSTISSAM 1/92 Level II (Zone B)	Recommendation **B** (Note 2)	Recommendation **E**	Recommendation **H**
EQUIPMENT meets NSTISSAM 1/92 Level III and all other RED equipment (Zone C)	Recommendation **C** (Note 2)	Recommendation **F** (Note 2)	Recommendation **I**

NOTE 1: *Additional precautions may be necessary if inspectable space is less than 8 meters or common wall situations exist.*

NOTE 2: *This installation may create TEMPEST hazards.*

IMPORTANT!

The CTTA has responsibility for conducting or validating TEMPEST reviews and recommending TEMPEST countermeasures, including RED/BLACK installation measures. There should be no commitment of funds without CTTA concurrence. Failure to consult the CTTA could result in installation of unnecessary and/or expensive countermeasures or the omission of needed countermeasures.

Table 3-1. RED/BLACK Installation Recommendations

THIS PAGE IS INTENTIONALLY LEFT BLANK

RECOMMENDATION A

Installing NSTISSAM TEMPEST/1-92 (Level 1) or Zone A RED Equipment in a TEMPEST Zone A Facility

(If not TEMPEST zoned, inspectable space less than 20 meters.)

Note: *Additional precautions may be necessary if the inspectable space is less than 8 meters. Contact your CTTA for specific guidance.*

1. A separation of 50 centimeters should be maintained between any RED processor and:
   a. BLACK equipment (including administrative support equipment).
   b. BLACK wire lines that exit the inspectable space or are connected to an RF transmitter.
   c. BLACK power lines.
   d. Fortuitous conductors that exit the inspectable space.

Note: *If the separation cannot be maintained, the CTTA must conduct a review to determine whether filters or other countermeasures should be recommended. For existing facilities, the CTTA may request TEMPEST tests be performed to assist in development of the recommendations.*

2. A separation of 5 centimeters should be maintained between any RED line and:
   a. BLACK wire lines that exit the inspectable space or are connected to an RF transmitter.
   b. BLACK power lines.

Notes:

1. Separation distance should be increased to 15 centimeters for parallel runs over 30 meters.

2. RED and BLACK wire lines should not use a common distribution vehicle.

3. RED and BLACK optical fiber lines may use a common distribution vehicle providing that: RED and BLACK optical fiber lines are not mixed within a multifiber cable; when a BLACK optical fiber cable is used in a RED distribution vehicle, there should be an opaque dielectric sheath covering each fiber and there should be no metallic stiffeners or metallic sheath in the BLACK optical fiber cable. When a RED optical fiber cable is used in a BLACK distribution vehicle, in addition to the above, the RED optical fiber cable must be separated from the BLACK distribution vehicle at the point where the BLACK distribution vehicle exits the inspectable space. If the RED optical fiber cable exits the inspectable space, it must be provided appropriate protection (encryption, protected distribution systems [PDS]).

3. Shielded Cables.

a. RED processors meeting the requirements of NSTISSAM TEMPEST/1-92 (Levels I, II, or III) must use optical or shielded wire cables if specified as part of the manufacturer's installation specification, or if specified for compliance with TEMPEST certification.

b. RED wire cables should be shielded and insulated overall.

THIS PAGE IS INTENTIONALLY LEFT BLANK

RECOMMENDATION B

Installing NSTISSAM TEMPEST/1-92 (Level II) or Zone B RED Equipment in a TEMPEST Zone A Facility

(If not TEMPEST zoned, inspectable space less than 20 meters.)

Note: *Additional precautions may be necessary if the inspectable space is less than 8 meters. Contact your CTTA for specific guidance.*

Note: *These installations may create TEMPEST hazards. Contact your CTTA for specific guidance.*

1. A separation of one meter should be maintained between any RED processor and:

    a. BLACK equipment (including administrative support equipment).
    b. BLACK wire lines that exit the inspectable space or are connected to an RF transmitter.
    c. BLACK power lines.
    d. Fortuitous conductors that exit the inspectable space.

Note: *If the separation cannot be maintained, the CTTA must conduct a review to determine whether filters or other countermeasures should be recommended. For existing facilities, the CTTA may request TEMPEST tests be performed to assist in development of the recommendations.*

2. A separation of 5 centimeters should be maintained between any RED line and:

    a. BLACK wire lines that exit the inspectable space or are connected to an RF transmitter.
    b. BLACK power lines.

Notes:

1. Separation distance should be increased to 15 centimeters for parallel runs over 30 meters.

2. RED and BLACK wire lines should not use a common distribution vehicle.

3. RED and BLACK optical fiber lines may use a common distribution vehicle providing that: RED and BLACK optical fiber lines are not mixed within a multifiber cable; when a BLACK optical fiber cable is used in a RED distribution vehicle, there should be an opaque dielectric sheath covering each fiber and there should be no metallic stiffeners or metallic sheath in the BLACK optical fiber cable. When a RED optical fiber cable is used in a BLACK distribution vehicle, in addition to the above, the RED optical fiber cable must be separated from the BLACK distribution vehicle at the point where the BLACK distribution vehicle exits the inspectable space. If the RED optical fiber cable exits the inspectable space, it must be provided appropriate protection (encryption, protected distribution systems [PDS]).

3. Shielded Cables.

a. RED processors meeting the requirements of NSTISSAM TEMPEST/1-92 (Levels I, II, or III) must use optical or shielded wire cables if specified as part of the manufacturer's installation specification, or if specified for compliance with TEMPEST certification.

b. RED wire cables should be shielded and insulated overall.

4. Power lines should be contained within the inspectable space whenever the average power load is less than 100 kVA. If this is not possible, the CTTA must conduct a review to determine whether power line filters should be recommended. For existing facilities, the CTTA may request a TEMPEST test be performed to assist in arriving at the recommendations.

5. RED processors should not be powered from the same circuits as RF transmitters or BLACK equipment with signal lines that exit the inspectable space, except when either the RED equipment or the RF transmitters and BLACK equipment with signal lines that exit the inspectable space are equipped with powerline filters. RED processors should be separated from RF transmitters by a minimum of three meters.

RECOMMENDATION C

Installing NSTISSAM TEMPEST/1-92 (Level III), Zone C or all other RED equipment in a TEMPEST Zone A Facility

(If not TEMPEST zoned, inspectable space less than 20 meters.)

Note: *Additional precautions may be necessary if the inspectable space is less than 8 meters. Contact your CTTA for specific guidance.*

Note: *These installations may create TEMPEST hazards. Contact your TEMPEST authority for specific guidance.*

1. A separation of one meter should be maintained between any RED processor and:

    a. BLACK equipment (including administrative support equipment).
    b. BLACK wire lines that exit the inspectable space or are connected to an RF transmitter.
    c. BLACK power lines.
    d. Fortuitous conductors that exit the inspectable space.

Note: *If the separation cannot be maintained, the CTTA must conduct a review to determine whether filters or other countermeasures should be recommended. For existing facilities, the CTTA may request TEMPEST tests be performed to assist in development of the recommendations.*

2. A separation of 5 centimeters should be maintained between any RED wire line and:

    a. BLACK wire lines that exit the inspectable space or are connected to an RF transmitter.
    b. BLACK power lines.

Notes:

1. *Separation distance should be increased to 15 centimeters for parallel runs over 30 meters.*

2. *RED and BLACK wire lines should not use a common distribution vehicle.*

3. *RED and BLACK optical fiber lines may use a common distribution vehicle providing that: RED and BLACK optical fiber lines are not mixed within a multifiber cable; when a BLACK optical fiber cable is used in a RED distribution vehicle, there should be an opaque dielectric sheath covering each fiber and there should be no metallic stiffeners or metallic sheath in the BLACK optical fiber cable. When a RED optical fiber cable is used in a BLACK distribution vehicle, in addition to the above, the RED optical fiber cable must be separated from the BLACK distribution vehicle at the point where the BLACK distribution vehicle exits the inspectable space. If the RED optical fiber cable exits the inspectable space, it must be provided appropriate protection (encryption, protected distribution systems [PDS]).*

3. Shielded Cables.

a. RED processors meeting the requirements of NSTISSAM TEMPEST/1-92 (Levels I, II, or III) must use optical or shielded wire cables if specified as part of the manufacturer's installation specification, or if specified for compliance with TEMPEST certification.

b. RED wire cables should be shielded and insulated overall.

4. Power lines should be contained within the inspectable space whenever the average power load is less than 100 kVA. If this is not possible, the CTTA must conduct a review to determine whether power line filters should be recommended. For existing facilities, the CTTA may request a TEMPEST test be performed to assist in arriving at the recommendations.

5. RED processors should not be powered from the same circuits as RF transmitters or BLACK equipment with signal lines that exit the inspectable space, except when either the RED equipment or the RF transmitters and BLACK equipment with signal lines that exit the inspectable space are equipped with powerline filters. RED processors should be separated from RF transmitters by a minimum of three meters.

RECOMMENDATION D

Installing NSTISSAM TEMPEST/1-92 (Level I), Zone A RED Equipment In a TEMPEST Zone B Facility

(If not TEMPEST zoned, inspectable space greater than 20 meters but less than 100 meters.)

1. A separation of 50 centimeters should be maintained between any RED processor and:

    a. BLACK wire lines that exit the inspectable space or are connected to an RF transmitter.
    b. BLACK power lines.

Note: *If the separation cannot be maintained, the CTTA must conduct a review to determine whether filters or other countermeasures should be recommended. For existing facilities, the CTTA may request TEMPEST tests be performed to assist in development of the recommendations.*

2. A separation of 5 centimeters should be maintained between any RED wire line and:

    a. BLACK wire lines that exit the inspectable space or are connected to an RF transmitter.
    b. BLACK power lines.

Notes:

1. Separation distance should be increased to 15 centimeters for parallel runs over 30 meters.

2. RED and BLACK wire lines should not use a common distribution vehicle.

3. RED and BLACK optical fiber lines may use a common distribution vehicle providing that: RED and BLACK optical fiber lines are not mixed within a multifiber cable; when a BLACK optical fiber cable is used in a RED distribution vehicle, there should be an opaque dielectric sheath covering each fiber and there should be no metallic stiffeners or metallic sheath in the BLACK optical fiber cable. When a RED optical fiber cable is used in a BLACK distribution vehicle, in addition to the above, the RED optical fiber cable must be separated from the BLACK distribution vehicle at the point where the BLACK distribution vehicle exits the inspectable space. If the RED optical fiber cable exits the inspectable space, it must be provided appropriate protection (encryption, protected distribution systems [PDS]).

3. Shielded Cables. RED processors meeting the requirements of NSTISSAM TEMPEST/1-92 (Levels I, II, or III) must use optical or shielded wire cables if specified as part of the manufacturer s installation specification, or if specified for compliance with TEMPEST certification.

THIS PAGE IS INTENTIONALLY LEFT BLANK

RECOMMENDATION E

Installing NSTISSAM TEMPEST/1-92 (Level II), Zone B RED Equipment in a TEMPEST Zone B Facility

(It not TEMPEST zoned, inspectable space greater than 20 meters but less than 100 meters.)

1. A separation of 50 centimeters should be maintained between any RED processor and BLACK equipment (including administrative support equipment.)

2. A separation of one meter should be maintained between any RED processor and:

   a. BLACK wire lines that exit the inspectable space or are connected to an RF transmitter.
   b. BLACK power lines.

Note: *If the separation cannot be maintained, the CTTA must conduct a review to determine whether filters or other countermeasures should be recommended. For existing facilities, the CTTA may request TEMPEST tests be performed to assist in development of the recommendations.*

3. A separation of 5 centimeters should be maintained between any RED wire line and:

   a. BLACK wire lines that exit the inspectable space or are connected to an RF transmitter
   b. BLACK power lines.

Notes:

1. Separation distance should be increased to 15 centimeters for parallel runs over 30 meters.

2. RED and BLACK wire lines should not use a common distribution vehicle.

3. RED and BLACK optical fiber lines may use a common distribution vehicle providing that: RED and BLACK optical fiber lines are not mixed within a multifiber cable; when a BLACK optical fiber cable is used in a RED distribution vehicle, there should be an opaque dielectric sheath covering each fiber and there should be no metallic stiffeners or metallic sheath in the BLACK optical fiber cable. Where a RED optical fiber cable is used in a BLACK distribution vehicle, in addition to the above, the, RED optical fiber cable must be separated from the BLACK distribution vehicle at the point where the BLACK distribution vehicle exits the inspectable space. If the RED optical fiber cable exits the inspectable space, it must be provided appropriate protection (encryption, protected distribution systems [PDS]).

4. Shielded Cables. RED processors meeting the requirements of NSTISSAM TEMPEST/1-92 (Levels I, II, or III) must use optical or shielded wire cables if specified as part of the manufacturer's installation specification, or if specified for compliance with TEMPEST certification.

5. Power lines should be contained within the inspectable space whenever the average power load is less than 100 kVA. If this is not possible, the CTTA must conduct a review to determine whether power line filters should be recommended. For existing facilities, the CTTA may request a TEMPEST test be performed to assist in arriving at the recommendations.

6. RED processors should not be powered from the same circuits as RF transmitters or BLACK equipment with signal lines that exit the inspectable space, except when either the RED equipment or the RF transmitters and BLACK equipment with signal lines that exit the inspectable space are equipped with powerline filters. RED processors should be separated from RF transmitters by a minimum of three meters.

RECOMMENDATION F

Installing NSTISSAM TEMPEST/1-92 (Level III), Zone C or all other RED equipment in a TEMPEST Zone B Facility

(If not TEMPEST zoned, inspectable space greater than 20 meters but less than 100 meters.)

Note: *These installations may create TEMPEST hazards. Contact your TEMPEST authority for specific guidance*

1. A separation of one meter should be maintained between any RED processor and:

    a. BLACK equipment (including administrative support equipment.)
    b. BLACK wire lines that exit the inspectable space or are connected to an RF transmitter.
    c. BLACK power lines.
    d. Fortuitous conductors that exit the inspectable space.

Note: *If the separation cannot be maintained the CTTA must conduct a review to determine whether fitters or other countermeasures should be recommended. For existing facilities, the CTTA may request TEMPEST tests be performed to assist in development of the recommendations.*

2. A separation of 5 centimeters should be maintained between any RED wire line and:

    a. BLACK wire lines that exit the inspectable space or are connected to an RF transmitter.
    b. BLACK power lines.

Notes:

1. Separation distance should be increased to 15 centimeters for parallel runs over 30 meters.

2. RED and BLACK wire lines should not use a common distribution vehicle.

3. RED and BLACK optical fiber lines may use a common distribution vehicle providing that: RED and BLACK optical fiber lines are not mixed within a multifiber cable; when a BLACK optical fiber cable is used in a RED distribution vehicle, there should be an opaque dielectric sheath covering each fiber and there should be no metallic stiffeners or metallic sheath in the BLACK optical fiber cable. Where a RED optical fiber cable is used in a BLACK distribution vehicle, in addition to the above, the, RED optical fiber cable must be separated from the BLACK distribution vehicle at the point where the BLACK distribution vehicle exits the inspectable space. If the RED optical fiber cable exits the inspectable space, it must be provided appropriate protection (encryption, protected distribution systems [PDS]).

3. Shielded Cables. RED processors meeting the requirements of NSTISSAM TEMPEST/1-92 (Levels I, II, or III) must use optical or shielded wire cables if specified as part of the manufacturer's installation specification, or if specified for compliance with TEMPEST certification.

4. Power lines should be contained within the inspectable space whenever the average power load is less than 100 kVA. If this is not possible, the CTTA must conduct a review to determine

whether power line filters should be recommended. For existing facilities, the CTTA may request a TEMPEST test be performed to assist in arriving at the recommendations.

5. RED processors should not be powered from the same circuits as RF transmitters or BLACK equipment with signal lines that exit the inspectable space, except when either the RED equipment or the RF transmitters and BLACK equipment with signal lines that exit the inspectable space are equipped with powerline filters. RED processors should be separated from RF transmitters by a minimum of three meters.

RECOMMENDATION G

Installing NSTISSAM TEMPEST/1-92 (Level I), Zone A RED Equipment in a TEMPEST Zone C Facility

(If not TEMPEST zoned, inspectable space greater than 100 meters.)

1. A separation of 50 centimeters should be maintained between any RED processor and:

    a. BLACK wire lines that exit the inspectable space or are connected to an RF transmitter.
    b. BLACK power lines connected to an RF transmitter.

Note: *If the separation cannot be maintained, the CTTA must conduct a review to determine whether filters or other countermeasures should be recommended. For existing facilities, the CTTA may request TEMPEST tests be performed to assist in development of the recommendations.*

2. A separation of 5 centimeters should be maintained between any RED wire line and:

    a. BLACK wire lines that exit the inspectable space or are connected to an RF transmitter.
    b. BLACK power lines connected to an RF transmitter.

Notes:

1. Separation distance should be increased to 15 centimeters for parallel runs over 30 meters.

2. RED and BLACK wire lines should not use a common distribution vehicle.

3. RED and BLACK optical fiber lines may use a common distribution vehicle providing that: RED and BLACK optical fiber lines are not mixed within a multifiber cable; when a BLACK optical fiber cable is used in a RED distribution vehicle, there should be an opaque dielectric sheath covering each fiber and there should be no metallic stiffeners or metallic sheath in the BLACK optical fiber cable. When a RED optical fiber cable is used in a BLACK distribution vehicle, in addition to the above, the RED optical fiber cable must be separated from the BLACK distribution vehicle at the point where the BLACK distribution vehicle exits the inspectable space. If the RED optical fiber cable exits the inspectable space, it must be provided appropriate protection (encryption, protected distribution systems [PDS]).

3. Shielded Cables. RED processors meeting the requirements of NSTISSAM TEMPEST/1-92 (Levels I, II, or III) must use optical or shielded wire cables if specified as part of the manufacturer's installation specification, or if specified for compliance with TEMPEST certification.

THIS PAGE IS INTENTIONALLY LEFT BLANK

RECOMMENDATION H

Installing NSTISSAM TEMPEST/1-92 (Level II), Zone B RED Equipment in a TEMPEST Zone C Facility

(If not TEMPEST zoned, inspectable space greater than 100 m.)

1. A separation of one meter should be maintained between any RED processor and:

    a. BLACK wire lines that exit the inspectable space or are connected to an RF transmitter.
    b. BLACK power lines connected to an RF transmitter.

Note: *If the separation cannot be maintained, the CTTA must conduct a review to determine whether filters or other countermeasures should be recommended. For existing facilities, the CTTA may request TEMPEST tests be performed to assist in development of the recommendations.*

2. A separation of 5 centimeters should be maintained between any RED wire line and:

    a. BLACK wire lines that exit the inspectable space or are connected to an RF transmitter.
    b. BLACK power lines connected to an RF transmitter.

Notes:

1. Separation distance should be increased to 15 centimeters for parallel runs over 30 meters.

2. RED and BLACK wire lines should not use a common distribution vehicle.

3. RED and BLACK optical fiber lines may use a common distribution vehicle providing that: RED and BLACK optical fiber lines are not mixed within a multifiber cable; when a BLACK optical fiber cable is used in a RED distribution vehicle, there should be an opaque dielectric sheath covering each fiber and there should be no metallic stiffeners or metallic sheath in the BLACK optical fiber cable. When a RED optical fiber cable is used in a BLACK distribution vehicle, in addition to the above, the RED optical fiber cable must be separated from the BLACK distribution vehicle at the point where the BLACK distribution vehicle exits the inspectable space. If the RED optical fiber cable exits the inspectable space, it must be provided appropriate protection (encryption, protected distribution systems [PDS]).

3. Shielded Cables. RED processors meeting the requirements of NSTISSAM TEMPEST/1-92 (Levels I, II, or III) must use optical or shielded wire cables if specified as part of the manufacturer's installation specification, or if specified for compliance with TEMPEST certification.

4. Power lines should be contained within the inspectable space whenever the average power load is less than 100 kVA. If this is not possible, the CTTA must conduct a review to determine whether power line filters should be recommended. For existing facilities, the CTTA may request a TEMPEST test be performed to assist in arriving at the recommendations.

5. RED processors should not be powered from the same circuits as RF transmitters or BLACK equipment with signal lines that exit the inspectable space, except when either the RED equipment or the RF transmitters and BLACK equipment with signal lines that exit the inspectable space are equipped with powerline filters. RED processors should be separated from RF transmitters by a minimum of three meters.

RECOMMENDATION I

Installing NSTISSAM TEMPEST/1-92 (Level III), Zone C or all other RED equipment in a TEMPEST Zone C Facility

(If not TEMPEST zoned, inspectable space greater than 100 meters.)

1. A separation of 50 centimeters should be maintained between any RED processor and BLACK equipment (including administrative support equipment.)

2. A separation of one meter should be maintained between any RED processor and:

   a. BLACK wire lines that exit the inspectable space or are connected to an RF transmitter.
   b. BLACK power lines connected to an RF transmitter.

Note: *If the separation cannot be maintained the CTTA must conduct a review to determine whether filters or other countermeasures should be recommended. For existing facilities, the CTTA may request TEMPEST tests be performed to assist in development of the recommendations.*

3. A separation of 5 centimeters should be maintained between any RED wire line and:

   a. BLACK wire lines that exit the inspectable space or are connected to an RF transmitter.
   b. BLACK power lines connected to an RF transmitter.

Notes:

1. Separation distance should be increased to 15 centimeters for parallel runs over 30 meters.

2. RED and BLACK wire lines should not use a common distribution vehicle.

3. RED and BLACK optical fiber lines may use a common distribution vehicle providing that: RED and BLACK optical fiber lines are not mixed within a multifiber cable; when a BLACK optical fiber cable is used in a RED distribution vehicle, there should be an opaque dielectric sheath covering each fiber and there should be no metallic stiffeners or metallic sheath in the BLACK optical fiber cable. Where a RED optical fiber cable is used in a BLACK distribution vehicle, in addition to the above, the, RED optical fiber cable must be separated from the BLACK distribution vehicle at the point where the BLACK distribution vehicle exits the inspectable space. If the RED optical fiber cable exits the inspectable space, it must be provided appropriate protection (encryption, protected distribution systems [PDS]).

4. Shielded Cables. RED processors meeting the requirements of NSTISSAM TEMPEST/1-92 (Levels I, II, or III) must use optical or shielded wire cables if specified as part of the manufacturer's installation specification, or if specified for compliance with TEMPEST certification.

5. Power lines should be contained within the inspectable space whenever the average power load is less than 100 kVA. If this is not possible, the CTTA must conduct a review to determine whether power line filters should be recommended. For existing facilities, the CTTA may request a TEMPEST test be performed to assist in arriving at the recommendations.

6. RED processors should not be powered from the same circuits as RF transmitters or BLACK equipment with signal lines that exit the inspectable space, except when either the RED equipment or the RF transmitters and BLACK equipment with signal lines that exit the inspectable space are equipped with powerline filters. RED processors should be separated from RF transmitters by a minimum of three meters.

SECTION 4

GUIDANCE FOR TEMPEST INTEGRITY

4.1. General. This section briefly describes the TEMPEST phenomena and the basic installation criteria to achieve TEMPEST integrity of national security information processing equipment and systems. The other appendices in this document contain specific installation and countermeasures guidance for various systems. NACSIM 5000 has additional information on the sources of TEMPEST signals, the types of TEMPEST signals, and the methods of signal propagation.

4.2. TEMPEST Basics. TEMPEST is an unclassified short name referring to investigations and studies of Compromising Emanations (CE). CE are defined as unintentional data related or intelligence bearing signals, which if intercepted and analyzed, disclose the NSI transmitted, received, handled, or otherwise processed by any information processing equipment. These intercepted signals need not be of great magnitude to compromise the NSI. Receiving intercept instruments can make use of even a small amount of energy.

4.2.1. Generation of CE. When equipment process NSI, the possibility exists that CE can be generated. Time and frequency characteristics of these emanations are normally unknown. However, the mechanisms of NSI emanation introduction into an escape medium, characteristics of various equipment under test, and experience allow estimation of their characteristics. In practice the more common types of CE are attenuated RED baseband signals, spurious carriers modulated by RED baseband signals, and impulsive emanations.

4.2.2. CE Sources. To determine the extent of CE and the necessary countermeasures to apply, equipment must be considered individually and as components of a system. Any circuit processing NSI can be a source of CE. A system could emit signals beyond the defined boundaries, even when all equipment and components comprising the system individually meet TEMPEST standards. This could occur because of the interrelationship of components, equipment interface characteristics, lengths, locations and shielding of interconnecting signal and control lines and methods of grounding each unit within the system. There are two basic sources of CE:

4.2.2.1. Functional Sources. Functional sources are those designed for the specific purpose of generating electromagnetic energy. Examples are switching transistors, oscillators, signal generators, synchronizers, line drivers and line relays.

4.2.2.2. Incidental Sources. Incidental sources are those NOT designed for the specific purpose of generating electromagnetic energy, but can generate energy incidental to normal operations. These sources of CE can include all electromechanical and electronic equipment and systems used to process NSI (e.g., communications equipment, recording and duplicating equipment, automatic data processing equipment, and their installations).

4.3. RED/BLACK Basics. The RED/BLACK concept, by definition, establishes areas for placement of equipment processing NSI (RED) that are separate and unique from areas with equipment processing non-NSI (BLACK). The concept is composed of two parts: physical separation and electrical separation.

a. Physical Separation. All equipment, wirelines, components and systems that process NSI are considered RED. All equipment, wirelines, components and systems that process encrypted NSI and non-NSI are considered BLACK. The RED/BLACK concept is to establish

minimum guidance for physical separation to decrease the probability that electromagnetic emissions from RED devices might couple to BLACK systems. Section 3 specifies the recommended separation for different equipment.

b. Electrical Separation. Electrical separation ensures that every signal conductor from a RED device is routed only to another RED device, or is encrypted before connection with a BLACK device. Electrical separation addresses signal distribution, power distribution, and grounding. Switches and/or other devices used to interface between RED and BLACK circuits/equipment should exhibit the following port-to-port isolation characteristics, as applicable:

- 100 dB over the baseband audio frequency range between 0.3 and 15 kHz.
- 80 dB over the baseband video frequency range up to 5 MHz.
- 60 dB over the frequency range from one times (R_d) to ten times the basic data rate ($10R_d$) of the digital signal(s) processed.

4.3.1. Facility Considerations. The most cost-effective application of RED/BLACK countermeasures will vary depending on characteristics of the facility and the equipment operated within the facility. The first step in the selection of proper RED/BLACK controls for the facility is the identification of the facility TEMPEST Zone ratings, equipment TEMPEST Zone ratings, and facility inspectable space. Table 3-1 and Section 3 contain the RED/BLACK installation recommendations as a function of these variables.

4.3.2. Physical Security Considerations. Physical security is a key element in deciding what RED/BLACK countermeasures will be adopted and is an important part of the necessary safeguards for equipment and systems that process NSI. The user is responsible for adopting the requisite physical security standards and procedures according to current directives. Physical security should be addressed at the beginning of any new facility or renovation project. Security officials, the CTTA, and/or others responsible for building construction or modification should be involved during the planning stages of a project.

4.4. Signal Cables. Installations can use shielded metallic cables and nonmetallic optical fiber cables to interconnect signals and to meet RED/BLACK separation recommendations.

4.4.1. Shielded Metallic Cables. Selection of metallic cable types varies according to equipment design. Jacketed multiconductor twisted pair cables consist of insulated, shielded pairs, or a bundle of twisted pairs contained within a single shield. Each shield (of a twisted pair or bundle of twisted pairs) should include an uninsulated and tinned drain wire. This drain wire should have a lay such that it will contact the shield throughout its length. To reduce radiation of CE, metallic cables should have a minimum of one overall braided metallic shield, with the shield terminated at both ends to the grounding network. The shield should not be used as a signal return path. A drain wire is not required in braided copper or outside-plant-type aluminum foil shielded telephone cable.

4.4.1.1. Cable Characteristics. Cables should have an overall shield composed of 85 to 90 percent tinned copper braid coverage. Consider the following when selecting cables; voltage breakdown, insulation type, jacket material and color. Effective shielding for a cable is achieved by meeting the requirements of MIL-C-23437 and by using proper cable shield termination. Crosstalk can appear on adjacent pairs. Refer to MIL-C-23437 for specific measurement techniques.

4.4.1.2. Shield Termination. Both ends of the overall shield should have 360 degree terminations. Shields for twisted pairs and bundles of twisted pairs are normally terminated at both ends. Designers and installers must be aware that terminating cable shields at both ends

can cause signal ground loop problems resulting in TEMPEST emanations or safety concerns. In these cases, the designers and installers should consider terminating the cable shield at one end only, or replacing the cable with a nonmetallic optical fiber cable. Long pigtail and long ground wire shield terminations drastically reduce shielding effectiveness and in certain frequency ranges can completely nullify the inherent shielding capability of a cable. If pigtail termination is required, the pigtail should be as short as possible and should be bonded to a low impedance radio frequency ground such as ground, plate, chassis or wide ground bus. A long slender ground wire is not an effective RF ground and can instead be an effective antenna.

4.4.2. Optical Fiber Cables. A fiber optics system converts an electrical signal to an optical signal, transmits the signal through an optical fiber, and converts the signal to an electrical signal at the receive end of the fiber. Although optical converters can create TEMPEST emanations from the electrical portion of their circuitry, optical systems have several advantages over metallic signal cables when used to transmit RED information:

- Because optical fibers are nonmetallic, they do not conduct or radiate radio frequency interference (RFI). Optical fibers are virtually unaffected by electromagnetic fields (i.e., electromagnetic interference (EMI) or RFI), effectively eliminating cable crosstalk.

- Because there are no cable grounds, systems are not subject to ground loops.

- Optical fiber cable systems are not subject to the transmission of common mode signals.

- Optical fiber cable systems are not damaged from lightning strikes through the optical fiber cable, although the cable can be severed.

4.4.2.1. Applications of Optical Fiber Cable Systems. Optical fiber cable systems can be used in RED and BLACK distribution systems to prevent the unintended transmission of TEMPEST signals outside the inspectable space. Specific optical systems can also be approved as a PDS (see current PDS standard) for secure transmission of plain text NSI to remote areas of the same security classification. While optical fiber cables used for this purpose will not radiate CE, the cables are still vulnerable to tampering, requiring appropriate physical security as with any RED cable. See MIL-STD-188-111 for interoperability and performance standards of optical fiber cable systems for military application.

4.4.2.2. Multifiber Cables. Multifiber cables within the same cladding should be restricted to either RED or BLACK information to preclude compromise through misconnections. Separate RED and BLACK dielectric multifiber cables can be routed in a common RED distribution system provided the end equipment are managed to preclude misconnections. All optical fiber cables should be clearly marked, labeled or tagged as RED or BLACK according to purpose to maintain complete accountability. Unused optical fiber cables should be marked as such.

4.4.2.3. Cable Strength Members or Shielding. A strength member included in some multifiber cables can be made of steel or other metal. Such a metal component in the cable could be a fortuitous conductor. Therefore, treat RED optical fiber cables with metal strength members and/or conductive shielding (cladding) the same as metal lines. They should not traverse BLACK areas unless installed in an approved PDS system.

4.5. Signal Distribution. A signal distribution system provides for the routing of BLACK or RED cables and consists of wireways and interconnect facilities. The typical encrypted communications system requires an interconnect medium to connect the terminal equipment to the encryption device, the encryption device to the modulator-demodulator (modem), and the

modem to the line or carrier equipment. This medium is usually a technical control or patch and test facility containing patching and distribution equipment. The signal distribution design should:

- Provide an orderly scheme to route signal cables among and between equipment by using good engineering practices.
- Provide accountability for all signal cables with sound administrative and operational accounting.
- Prevent RED cables from becoming intermixed or inadvertently coupled to any BLACK cables by selection of cables, wireways, interconnect facilities, and isolation techniques.

4.5.1. Wireways. Wireways provide convenient methods to control the routing of signal cables to prevent mixing cables by controlling access to the route. Properly installed wireways can also aid in shielding cables contained therein and thereby reducing electromagnetic radiation. RED and BLACK cables should use separate wireways with physical separations as recommended in Section 3. Many signal lines that egress the inspectable space are contained in a pipe, conduit, duct or other conductive material. This outer physical layer can become a fortuitous conductor and could require isolation. A CTTA will determine if isolation is required, the best location for the break and the length of pipe.

4.5.2. Patching Equipment. Patching equipment is usually a series of jack fields wired in the normal through configuration. This permits equipment to be connected through all elements to the line or carrier equipment. Patch cords enable use of spare equipment or cable pairs when performing routine maintenance or eliminate downtime due to equipment or wiring malfunctions. Install separate RED and BLACK jack fields to maintain the separation recommendation of Section 3. The jack fields should have incompatible connectors to prevent inadvertent RED to BLACK patching. Separate the cabinets or racks from RED and BLACK equipment according to Section 3.

4.5.3. Distribution Equipment (Wire Closets). Wire closets typically are equipment cabinets or rooms designed for hardwired interconnect of cables between equipment. Distribution equipment must be designed with separate RED and BLACK connector blocks to prevent improper connection of RED and BLACK lines. Separation of the connection components and the associated signal line distribution should be according to Section 3.

4.5.4. Protected Distribution Systems (PDS). A signal distribution system containing unencrypted NSI which enters an area of lesser classification, an unclassified area or uncontrolled (public) area must be protected according to the requirements of the current PDS standard.

4.6. Signal Line Isolators and Filters.

4.6.1. Signal Line Isolation. BLACK lines and other electrically conductive materials that egress the inspectable space are potential carriers of CE that can inadvertently couple to the lines. An extensive variety and quantity of BLACK lines and other conductive materials can cross the boundary of the inspectable space of a facility. Various signal line isolation techniques can be used to protect the signal line, the distribution system or other fortuitous conductors from conducting compromising signals beyond secure areas. Before employing these isolation methods, the facility and equipment should be evaluated to determine if the minimum separation recommendations of Section 3 can be met. Consider signal line isolation only if the minimum separation recommendations cannot be met.

4.6.2. Assessing the Need for Signal Isolation. When the minimum separation recommendations of Section 3 cannot be met, there are many factors that combine to determine if a specific facility and equipment complement should use signal line isolation techniques. The CTTA should decide whether compromising signals are detectable on the signal lines in areas where unauthorized personnel could exploit them with little chance of being discovered. Without knowledge of the results of an instrumented TEMPEST test at the site, there will usually be insufficient information to make this decision. Experienced TEMPEST personnel can decide based on known factors that can include equipment TEMPEST characteristics, cable shielding, equipment separation distances from the potential conductors, physical access controls to the distribution of the conductors, the security classification of the NSI processed, and the relative threat of exploitation based on the geographic location of the facility, and the guidelines of NSTISSI 7000. To ensure that the facility is adequately protected for future equipment configurations, consider the frequency of changing, adding and relocating equipment. At a specific facility some conductors require isolation while others do not, based on equipment layout, signal line distribution and other factors. Isolation of conductors may not be possible for reasons like life, safety or prohibitive cost. When conflicts occur, consult the cognizant CTTA to develop the best approach.

4.6.3. Passive Signal Line Filters. Passive filters are installed on signal lines to block signals outside a specified frequency range. Lowpass filters are used to pass the intended baseband signal and greatly attenuate all higher frequency signals. Bandpass filters, which suppress signals above and below a specified frequency range, and highpass filters, which pass signals above a specified frequency, are also available for special requirements. Filters are available with different signal cutoff frequencies to meet the requirements of a variety of signaling rates. Previously, telephone line filters were required to pass only the analog voice signals. To avoid signal degradation or stoppage in digital data transmission on telephone networks, select telephone line filters compatible with the format and speed of the intended signal.

4.6.3.1. Lowpass Filters. Passive lowpass signal line filters should meet the guidance below and the requirements of MIL-F-15733. For most effective performance, signal line filter design should meet the specific requirements for their particular application, however, an existing filter design that approximates the desired characteristics can be more economical. Two types of signals require filtering: analog signals (i.e., voice or the tone output of modems), and digital signals (i.e., mark/space square waves). Filter behavior and performance for each of these types of signals are considered separately.

4.6.3.1.1. Analog Signal line Filters. Analog signal line filters are usually designed to match a balanced 600 ohm signal pair (two 300 ohm filters). These filters can introduce moderate phase and amplitude perturbations in the 1500 Hz to 3300 Hz portion of the passband, even when employed in an impedance matched system. If there is an impedance mismatch to the filter, these perturbations will increase approximately in proportion to the extent of the mismatch. Modems can tolerate a minimum of phase and amplitude distortion introduced by signal line filters. For applications of this type, the options are to use a simple filter designed to introduce minimal phase and amplitude distortion in the frequency band of the modem (0 to 3300 Hz) or to design an expensive, multi-element, compensated filter.

4.6.3.1.2. Inductive-Capacitive (LC) Signal Line Filters. LC signal line filters tend to "ring" when the input signal is a square wave. Using these filters to remove undesired frequency components from digital signals generate stringent design problems. The best square wave performance can be obtained from an LC filter that is both driven and terminated in its characteristic impedance. Some ringing will occur, and there will be 6 dB attenuation of the signaling voltage (i.e., +6 volts to the filter driver will produce + 3 volts out to the line). This degree of signal attenuation is usually not acceptable in a digital system. Two alternate approaches are available to provide minimum desired signal attenuation, with only a moderate

increase in ringing. First, a filter driven with a matched source impedance can be terminated in a high impedance (x10 or higher) without appreciable signal attenuation and with only a moderate increase in ringing. Second, when an inductance input type filter is employed, a low impedance device can be used if the filter is terminated in its characteristic impedance. In general, a filter terminated in its characteristic impedance can be used at a bit rate approaching 1/3 the filter cutoff frequency. If the impedance is substantially mismatched, excessive ringing will occur and the bit rate that can be passed is drastically reduced.

4.6.3.1.3. Digital Signal Line Filters. Filters driven directly from keying contacts must have inductive inputs or there will be excessive contact arcing resulting in rapid contact deterioration. Ringing will be moderate if the filter is terminated in its characteristic impedance. Without proper termination, the filtered signal will have excessive ringing that severely limits the usable bit rate. Filter designs developed to solve specific problems are necessarily expensive. Changing the signal patch to provide a balanced signal pair matching the characteristic impedance of a filter is usually impossible. Most signal line filters are designed for balanced 600 ohm transmission line systems and are available as either dual 300 ohm or 300 ohm units intended to be used in pairs. They have also been designed primarily for analog signals in the 0 to 3 kHz frequency range. Unfortunately, these filters have been employed in many digital applications for which they were not designed. Most digital systems do not employ balanced transmission techniques in that one lead of a transmission pair is driven at -6 volts for space bits, and 0 volts for mark bits. Also, the input impedance of low level digital devices usually is at least 6,000 ohms and can be as high as 100,000 ohms, while the output driving impedance of digital drivers can be only a few ohms. This suggests that 300 ohm analog filters will give unsatisfactory performances in most digital circuits. If filtering is necessary for specific digital applications, special filter designs should be developed that are tailored to the specific problem. An alternative is to change the signaling path to a transmission link using a balanced signal pair with matched source and sink impedances. A standard filter can then be inserted in the transmission link. This alternative is particularly attractive from an engineering viewpoint when the signaling path leaves the inspectable space for a long run.

4.6.4. Active Signal Line Filters. Active filters are frequency selective devices that employ electronic impedance, current, and voltage modifying elements, requiring the application of power to use their filtering properties. As opposed to passive filters, active filters are essentially one-way devices that use impedance mismatch as the primary basis for filtering action. Note also that the phase delay, passband, and stop band characteristics of active filters can be widely divergent from those of standard passive filters. Active filters are more readily adaptable to digital applications than are passive filters and can be specifically designed to process analog signals with a minimum of distortion.

4.6.4.1. Linear Filters. Active linear filters normally consist of linear amplifiers that incorporate frequency selective resistance-capacitance (RC) networks, either as negative feedback elements or in line filter elements, or both. Filters of this type can be configured to be lowpass, bandpass, highpass, or band rejection types. A well-designed active filter provides a greater degree of attenuation of unwanted signals at a higher cost. The small size and versatile characteristics can justify the added cost. Active filters are currently being produced in modular form to produce chips that offer a greater variety of filtering characteristics.

4.6.4.2. Saturated Amplifiers. One type of active filter for digital signals is a combination of saturated input and output amplifiers coupled by means of a single RC network. If an active feed through capacitor is employed between the input and the output compartments, independent power supply provided, and adequate shielding designed into the enclosure, attenuation of transverse mode unwanted signals of at least 100 dB can be obtained. Saturated amplifiers should not be used by themselves because they do not provide common

mode isolation. The provision of an optical path instead of a conducted or capacitive penetration of the RED/BLACK shield adds minimum complexity and enhances security.

4.6.5. Isolators. The common characteristic of isolators is that they can provide dc and ground system isolation between input and output circuits, thus reducing the possibility of signal conducting ground loops. Isolators also offer design possibilities for non-low level signals in and low level signals out, or vice versa, polar-to-neutral-to-polar conversion, and independent dc levels for input and output circuits. To obtain these characteristics, separate power sources are necessary for input and output circuits. Isolators can be subdivided into the following functional types: magnetic-, acoustic-, and photon-coupled devices.

4.6.5.1. Magnetic-coupled Isolators. The simplest form of a magnetic-coupled isolator is a conventional electromechanical relay. Such a device provides dc isolation, but is limited to low baud rates, and unless it is of a very special shielded design, provides only meager higher frequency attenuation. Another form of magnetic-coupled isolator is the transformer-coupled type that employs a modulated oscillator in the input operating at a frequency at least ten times the highest baud rate, while the output is equipped with either a suitable phase, frequency shift, or amplitude detector. Effective passive filtering of the input and output signal lines is essential to prevent the modulated high frequency signal from coupling out of the isolator onto the input and output lines. Standard relays have been used as isolators in teleprinter (TTY) systems for many years, but their principal capability has been dc isolation and level changing. Transformer-coupled isolators have not been highly successful as digital devices, but as analog devices, transformer coupling is used extensively to provide dc isolation between equipment and balanced input and output lines.

4.6.5.2. Acoustic-coupled Isolators. Acoustic-coupled isolators are similar to transformer-coupled isolators in that both employ a modulated oscillator and suitable detecting devices. In the acoustical device, the oscillator drives a transducer, which in turn excites a receiving transducer through some nonconducting medium. The problems encountered with this type isolator are similar to those of the magnetic-coupled type. Very few applications of this type device have been achieved.

4.6.5.3. Photon-coupled Isolators. Photon-coupled (optical) isolators are available in many different configurations. These range from integrated circuit components (containing a light source and detector and providing only dc and very low frequency isolation) to isolators that employ optical coupling through a waveguide (capable of providing more than 120 dB of both common mode and transverse mode isolation from dc through 10 GHz). This definition applies to both forward and backward (output-to-input) isolation. Common mode signal isolation is the degree of signal attenuation in decibels between the shorted input and the shorted output of the isolation device when the signal source is between the shorted input of the isolation device and ground reference. The measuring equipment is connected between the shorted output and the ground reference. Photon-coupled isolators are available for both digital and analog signal applications. Digital signaling speeds of several million bits per second and analog bandwidths of several megahertz can be accomplished. Photon-coupled isolators use lightwave technologies to couple signals between two points via use of an optical fiber cable. When the optical fiber cable is installed in a waveguide beyond cutoff, the isolator is ideal for use in shielded installations where conducting penetrations are kept at a minimum. Four types of isolators are identified by intended application.

Type	Application
I	digital signals without retiming input (regeneration)
II	digital signals with retiming input (regeneration)
III	analog signals (audio, video, RF modem, wideband, etc.)
IV	telephone circuits (duplex, incoming, supervisory signals)

Table 4-1. Photon-Coupled Signal Line Isolator Types

4.6.5.3.1. Signal Line Isolators. Isolators can provide more than 120 dB isolation (0 to 10 GHz) for lines passing through any equipment or equipment area interface requiring protection. The reason for this stringent requirement is to prevent a conductive or capacitive path for compromising information from the RED equipment area to the BLACK equipment area and the uncontrolled area. Take notice that one line filter cannot perform the function of an isolator, since a conductive path is always present within the passband of the filter. The use of filters is not recommended because ground current loops are generated by the low impedance to ground that the filter inherently has at frequencies above its cutoff frequency. The ground currents present the possibility of compromise.

a. Analog. Analog photon-coupled signal line isolators provide attenuation of the unwanted signals equal to digital isolation in the "backward" direction. In the forward direction, they provide common mode isolation equal to digital isolators, but do not provide transverse mode isolation within the bandwidth of the signal being transmitted. The analog photon-coupled signal line isolators are equal to the best active or passive filters.

b. Photon. A photon-coupled signal line isolator allows the input and output modules to be shielded by a ground plane connected only by a nonconductive optical path through a waveguide penetration. A ground plane can be a shielded room wall, conduit box, or equipment housing. This arrangement assures a high level of signal isolation at all signal rates.

4.6.5.3.2. Advantages of Photon-coupled Isolators. The advantages of using photon-coupled isolators are: (1) elimination of the electrically conductive path of undesired signals between the input and output modules; (2) attenuation of common mode signals by use of waveguides operating below cutoff as attenuators; (3) elimination of undesired transverse mode signals by filtering, pulse reshaping, or pulse regeneration. The isolators are usually mounted inside an RFI cabinet or on the wall of a shielded room. The penetration of the shield is in the form of a waveguide tube through which the optical path passes. The dimensions of the waveguide tube are normally chosen to prevent the passing of RF energy below 10 GHz.

4.7. Power Distribution. The power distribution scheme must be protected from exploitation of CE that might be developed in the system. The scheme must conform to the life and safety provisions of the Occupational Safety and Health Act (OSHA), the National Electrical Code (NEC), and local building codes. MIL-HDBK-411 contains guidance for power distribution design. The following paragraphs address the proper design of a power distribution scheme that will satisfy RED/BLACK recommendations.

4.7.1. The Power Requirement. The power requirements of a facility can be divided into two groups -- power for the mission equipment (technical) and power for the supporting services

(nontechnical). Supporting services include lighting, heating, ventilating, air conditioning, etc. By providing a separate service feeder dedicated to the sensitive equipment and controlling its distribution, the opportunity for unauthorized detection of compromising signals on those lines is reduced. Powerline conduction occurs when plain text information is transferred onto the powerline by RED equipment, or radiated through free space and coupled onto the powerlines. If a facility is processing NSI, power is sometimes divided into RED and BLACK power. RED power provides isolation for those non-TEMPEST approved equipment processing NSI. BLACK power is provided for equipment processing non-NSI because power isolation is not required. This separation prevents conducted emissions from RED equipment being coupled through BLACK equipment to BLACK lines that might egress the inspectable space. Adequate internal filtering permits use of BLACK power for Level I TEMPEST compliant equipment and systems. In addition to separate distribution facilities, the measures outlined in the subsequent paragraphs for containment and suppression of conducted emissions apply to RED power. RED power distribution must be designed such that neither BLACK equipment nor utility equipment is connected to it. The design and installation of power systems require judicious selection of the primary and auxiliary power sources, uninterruptible power supplies (UPS) or other power conditioning equipment, secondary substations, protective measures, and the distribution system to attain the maximum overall system performance with the most cost-effective design.

4.7.2. Power Conditioning/Isolation. Facilities using sensitive solid-state equipment often include devices to condition the electrical power by removing or suppressing harmonic distortion, surges, sags, spikes, and electrical noise. Chiefly, powerline filters, isolation (Faraday shielded) transformers, UPS, and power regulators are used. When the facility transformer is located within the inspectable space and draws an average load of 100 kilovolt-amperes (kVA) or more, filtering the ac power is not required.

4.7.2.1. Powerline Filters. The passive LC filter has long been used to remove unwanted RFI from conductors of all types. Such filtering has been in general use to prevent RFI from interfering with equipment operations. The TEMPEST program employs filters to prevent RFI generated in equipment from escaping as conducted CE. When applied to the treatment of powerlines, two schools of thought exist: bulk filtering for the entire facility, and filtering only equipment as required. Bulk filtering is expensive and generally less effective than filtering at the equipment. Filtering at the component and/or cabinet level is a more practical and economical approach for isolating RED electromagnetic environments from BLACK electromagnetic environments. Vendors' catalogs typically provide detailed information for available filters. If the appropriate filter is not available but is required for secure equipment operation, the following information should be provided to the filter manufacturer for custom design of a filter:

Operating line voltage
Operating frequency
Source impedance
Load impedance
Load current
Desired bandpass frequency
Acceptable insertion loss

Powerline filters are not considered an assured method of adequately suppressing CE. Custom designing powerline filters for each equipment is a preferred method of preventing conducted CE from being introduced on powerlines. The required insertion loss can be more readily attained with equipment filters because saturation of inductors is a lesser problem due to lower current and because impedance mismatch can be minimized due to known characteristics.

4.7.2.2. Isolation Transformers. Isolation transformers are principally used to break ground loops to reduce common mode and differential mode noise. An isolation transformer equipped with triple Faraday shields is very effective in reducing conducted emission in both the power mains and the branch feeds. The transformer can be 1:1 ratio or stepdown. Its installation in the facility should be as close to the load equipment as possible, preferably in the same room. It should also be installed per NEC Article 250-5(d) as a separately derived system and, as such, establishes a new fault protection subsystem. It should not be tied to the green wire serving the power main side, as this defeats the intent of both the NEC for protection and the use of this type of transformer to break ground loops. Further, some isolation transformers can be designed with the ground and neutral conductors being common to the primary and secondary windings. This reduces the isolation effectiveness of the transformer.

4.7.2.3. Uninterruptible Power Supplies and Power Regulators. Many installations using computer or process control equipment employ UPS and voltage regulators as a method of providing glitch free power. Certain aspects of UPS aid in containment of conducted emissions as discussed in the following paragraphs.

4.7.2.3.1. Solid-state UPS (SSUPS). In theory, the SSUPS offers high isolation of conducted emissions by the nature of its operation. SSUPS takes the incoming ac power through a dc converter or rectifier. The filtering section of the rectifier should greatly attenuate conducted emissions. The dc voltage is supplied to an inverter section that synthesizes a sinewave that is filtered to reduce the probability of a conducted emission feeding back to the power mains. For most security processing applications, an SSUPS can be powered from either RED or BLACK power.

4.7.2.3.2. Rotating UPS. Whether a rotating UPS is constructed as a motor generator or a no-break generator using an inertia flywheel, its basic principles of operation provide a degree of isolation between power mains and loads. The typical structure is an ac synchronous motor driving a generator. Such systems offer high immunity of the load from line disturbance. Some configurations do not provide isolation for conducted emissions. This is particularly true if the ac motor is mounted on a common shaft with the generator and in a common housing. If the motor and generator shafts and housings are electrically separated and capacitively decoupled, the emissions can be contained. Systems employing dc motors offer some isolation regardless of the configuration. Better isolation can be achieved if the housings are electrically and capacitively decoupled. In such systems, conducted emissions are suppressed in the dc power supply driving the motor and in the battery system.

4.8. Grounding System. The grounding scheme in a facility is composed of an earth electrode subsystem, lightning protection subsystem, fault protection subsystem, and signal reference subsystem. The signal reference subsystem is either a single point grounding design or a multiple point equipotential ground plane design, and it is of particular interest for control of TEMPEST emanations. Each grounding subsystem has a separate and distinct function as described in MIL-HDBK-419. Standards for grounding and bonding are provided in MIL-STD-188-124. Guidance on the construction of an equipotential grid can be found in Federal Information Processing Standards Publication (FIPS PUB) 94 and MIL-HDBK-419, Volume II. Pertinent aspects of the single point and equipotential grounding methods are described here to highlight the security ramifications of each method.

4.8.1. Equipotential Plane. An equipotential ground plane is a mass, or masses of conducting material that, when bonded together, offers negligible impedance to current flow. In any electrical circuit, it is essential to provide a low impedance path for signals to return from the load back to the generator. Noise in a signal line can often be attributed to the noise signal and current finding a lower impedance return than the intended path. Where filters are employed in circuit design, unwanted signals are removed from the lines and shunted to

another conductor. Any signal shunted to the ground system might circulate through multiple branches of the ground system to return to the source. Due to uncontrolled conductor lengths and impedance mismatches, such signals could be radiated from the conductors. Guidance on the construction of an equipotential grid can be found FIPS PUB 94 and MIL-HDBK-419, Volume II. All equipment signal ground terminals are bonded to the grid with leads as short as possible, but should not exceed 1/20 of the wavelength for the highest frequency of interest.

4.8.2. Single-Point Ground. Sometimes a single-point ground can be the only viable solution for a signal grounding scheme. From the TEMPEST viewpoint, a single point ground can satisfy the grounding requirement at facilities where: (1) no station ground meeting the criteria of MIL-HDBK-419, Volume II exists, (2) station ground exists, but is not accessible, and (3) it is neither cost-effective nor practical to construct an equipotential grounding system.

4.8.3. Fault Protection Ground. The National Electrical Code (NEC), Article 250, requires equipping electrical power installations with a fault protection grounding subsystem. Its purpose is to establish a common reference and to provide an uninterrupted current path from the powered equipment back to the first service disconnect or transformer. When a fault occurs in the equipment, the grounding conductor will cause a circuit breaker to trip and reduce the hazard to personnel. Use of metallic conduits and wireways as a fault return path is not recommended for data processing and communications equipment. The probable electrical discontinuity at conduit or wireway joints can cause a high impedance that will generate noise. Each equipment that is hardwired to the power source or each power outlet servicing equipment should be connected to a dedicated, contiguous green wire protective ground extending to the service disconnect. The protective grounding subsystem is unacceptable as a signal reference ground for the following reasons. First, the NEC does not intend the green wire system to carry current except during a fault. Second, there is no control over the distribution of signals. Third, the power distribution system is susceptible to noise that can disrupt signal circuits.

4.8.4. Isolated Ground. Although not specifically intended for TEMPEST treatment, an isolated ground power distribution scheme can enhance line isolation concepts. To minimize mutual inductive coupling, the power cable is not run in conduit. This distribution scheme consists of isolated ground outlets, an isolated power distribution panel, and an insulated grounding conductor. The isolated ground outlet is designed with no electrical bond between the grounding terminal and the frame of the outlet. This prevents automatic coupling of the ground to the conduit, which would destroy the isolated ground. The ground conductor should be connected between the grounding terminal on the outlet and the grounding bus in the power distribution panel. The grounding and neutral bus bars should be insulated, isolating them from the distribution panel, conduit, and each other at this point. The grounding conductor is then connected from the ground bus to the grounding point of the facility main power switch gear. At this point it becomes common to the neutral conductor and other grounding conductors used throughout the facility. Only operational equipment should be connected to the power panel. Lights, air handling systems, utility devices and housekeeping equipment should be connected to a separate panel since they can induce unwanted noise into the system. Use of an isolated ground power distribution scheme will effectively isolate TEMPEST equipment from other electrical devices in the facility, but is not intended to replace other required powerline isolation devices.

4.9. Administrative Support Equipment. Any facility processing NSI will likely contain electronic administrative support systems not directly associated with the classified processing. This can include administrative telephones, paging systems, alarm detection systems, building utilities, radio and television receivers, and miscellaneous unclassified computer and communications equipment such as facsimiles, television monitors, video cassette recorders, portable computers, modems and local area network components. If not installed according to

RED/BLACK criteria, these systems can provide a conductive path for TEMPEST emanations to escape the facility. These components are sometimes personally owned and are often portable, which increases the likelihood they can be incorrectly installed in a secure facility. Administrative controls are recommended to establish local procedures to control the location and use of administrative support equipment within a secure facility. The use of wireless systems should be prohibited in all cases.

4.9.1. Telephone Systems. Administrative telephone systems are a potential source for fortuitous conduction of CE due to their proximity to building maintenance areas and their signal line distribution outside the facility. Additional protection is recommended when commercial telephones are located in a RED electromagnetic environment. The most effective protection is provided by line disconnection switches and telephone line optical isolators that use waveguide below cutoff. The use of these devices or telephone filters must be approved by the CTTA. These devices should be considered only when installing, replacing or retrofitting telephone systems.

4.9.1.1. TEMPEST Protective Measures. The separation recommendations of Section 3 apply. Remember that the administrative telephone system and its associated wiring are BLACK. The telephone system cabling should be routed in a separate distribution system. If filters or isolators are required and approved by the CTTA, the lines should be filtered/isolated where they egress the inspectable space or facility. Locating the filters/isolators at the controlled space is not recommended because the equipment TEMPEST zone may extend beyond the controlled space. In addition, fewer filters/isolators will be necessary if the trunk lines rather than the individual phone lines are filtered/isolated.

4.9.1.2. On-hook Security. Telephone systems can exhibit insecurities even when the telephone instruments are on-hook. This happens when RED audio or acoustic signals impinge on microphonic components in the telephone. TSG 1 and TSG 2 provide guidance to prevent on-hook security problems. TSG 6 lists approved and type accepted telephone equipment.

4.9.2. Paging, Intercom, and Public Address Systems. In addition to being a possible fortuitous conductor of TEMPEST emanations, the speakers in paging, intercom and public address systems can act as microphones and retransmit classified audio discussions out of the controlled area via the signal line distribution. This microphonic problem could also allow audio from higher classified areas to be heard from speakers in lesser classified areas. Ideally, such systems should not be used. Where deemed vital, the following precautions should be taken in full or in part to lessen the risk of the system becoming an escape medium for NSI.

- Systems should be totally contained within the inspectable space.
- Voice frequency, lowpass filters should be installed on all cables if they are not totally contained within the inspectable space. This protects against TEMPEST signals on the cables but does not protect against voice modulation of the speakers.
- Equipment should meet the separation recommendations of Section 3.
- Amplifiers should be considered for speakers in higher classified areas to provide reverse isolation to prevent audio from being heard in lesser classified areas.

4.9.3. Alarm Systems. Many facilities employ alarm systems to detect and alert personnel of life threatening or security threatening situations. These systems employ passive or active sensors terminated on an annunciator panel. Such systems can also act as fortuitous

conductors and could require isolation filtering and separation treatment similar to telephone and intercom systems.

4.9.4 Miscellaneous Fortuitous Conductors. Building utilities and other support elements can become fortuitous conductors due to the use of metallic materials. Heating, ventilating and air conditioning systems air ducts, water pipes and gas pipes can require protection depending on their proximity to RED equipment and their distribution into uncontrolled areas. If conductors are identified as likely fortuitous conductors of TEMPEST signals into uncontrolled areas, the normal treatment is to insert a nonconductive section in the plumbing or duct work at the boundary of the inspectable space of the RED equipment. It is important to follow NEC, OSHA and any local building and fire codes when isolating various conductors. Some metallic distribution facilities must be electrically bonded to the building structure or the fault protection subsystem. Some materials can be prohibited in utilities such as sprinkler systems or pressurized systems. Life safety and compliance with all applicable building codes are an overriding concern when considering isolation of fortuitous conductors. For this reason and also due to the quantity and variety of potential fortuitous conductors throughout a facility, isolation of such conductors should be accomplished when practical. There are often alternative procedures to avoid TEMPEST conduction problems with such fortuitous conductors via relocation of equipment, or specific grounding of the fortuitous conductor.

4.9.5 Radio Transmission or Reception Devices. Any device that transmits or receives a radio signal is a potential security risk in a facility processing NSI. The risk is higher for radio transmission devices and in facilities using non-TEMPEST equipment. Traditional station designs place radio communications (combat, net radio, microwave systems, etc.) away from the processing area. If not carefully controlled, other radio devices such as cellular telephones, cordless telephones, wireless local area networks (LANs) or portable satellite communications systems can be installed in a facility near RED equipment. Radio transmission equipment should be prohibited from all classified processing areas. If a mission requirement or space limitation demands that transmitters must be installed in classified processing areas, the separation requirements of Section 3 must be met. For such installations, a CTTA review is required to evaluate the risks of TEMPEST vulnerabilities. Reception devices such as radios, television receivers or receive-only pagers can be installed if authorized by cognizant security authorities and if installed with the separation requirements of Section 3.

4.9.6 Commercial Television System Installation. When commercial television systems are installed in secure areas, the CTTA should determine the countermeasures necessary to prevent a video cable entering the secure area from conducting comprising emanations out of the secure area. The countermeasures depend on the type of cable used to bring the signal into the secure area. If an optical fiber cable is used at the entry point to the secure area, no additional countermeasure is required. If a metallic cable is used at the entry point, it must be a shielded metallic cable and must use an amplifier/attenuator system that must be located at the point where the cable enters the secure area. Only an amplifier/attenuator system that provides one-way filtering should be used. An attenuator could be required if the amplified signal overdrives the television receiver. The attenuator will also provide additional reverse attenuation. The length of metallic cable penetrating the secure area must be kept to a minimum. The use of a VCR as an electronic filter is not allowed, since it does not provide proper filtering. If not installed properly, the VCR can amplify signals in both directions and not provide for one-way

filtering. If a control box is used, it should be collocated with the amplifier/attenuator system. If a VCR is used with this system, it cannot be used to play or record classified information (unless the incoming video cable is disconnected) and must be conspicuously marked advising of this restriction. Amplifiers that can amplify signals in both directions should not be used. Commercial television system equipment and cables should comply with separation guidance in Section 3.

4.10. Other Considerations

4.10.1 TEMPEST Zoning. TEMPEST Zoning is a countermeasure that takes advantage of free space propagation loss and the inherent shielding of a host facility. By profiling a structure's attenuation, TEMPEST Zoning can allow equipment operation with less fear of unauthorized intercept and without the added expense of TEMPEST approved equipment or global shielding. The concept profiles the facility into zones that have varying levels of protection. This is determined by developing attenuation plots of radiated signals in four test bands between 10 MHz and 1,000 MHz compared with reference measurements taken with antennas separated by 20 meters in an open field environment. The TEMPEST Zone profile data for a facility can then be used in conjunction with known TEMPEST zone characteristics of electronic equipment to enable selection and placement of equipment to contain radiated TEMPEST emanations within the predetermined secure areas of the facility. NSTISSAM TEMPEST/2-92 contains details for TEMPEST zoning of facilities.

4.10.2. Inspectable Space. The inspectable space can vary considerably from one facility location to another. It is important to understand the boundaries of the inspectable space surrounding a facility to properly apply RED/BLACK countermeasures. The site designated TEMPEST approval authorities should define and a CTTA should approve the boundary.

4.10.3. Facility Shielding. In certain instances, systems processing NSI are so large and complex that application of TEMPEST protective measures to the equipment can be impossible or exorbitantly expensive. In such cases, the entire facility can be shielded and power, signal and utility penetrations of the shield treated to block and remove conducted CE. This approach should be implemented only after a thorough cast comparison analysis of alternative security countermeasures. Obtain guidance from a CTTA to determine requirements and recommend methods for shielding. NSTISSAM TEMPEST/1-94 contains details on shielding.

4.10.4. TEMPEST Suppressed Equipment. TEMPEST equipment have been tested in accordance with NSTISSAM TEMPEST/1-92 and demonstrated to comply with conducted and electromagnetic radiation limits of Level I, Level II or Level III.

SECTION 5

SECURE VOICE SYSTEMS

5.1. General. A secure voice installation is unique in that the terminals are used both in highly controlled areas and also in minimally controlled areas, or residential type areas.

5.2. Basis for Minimum Installation Techniques. The very nature of the system dictates the flexibility, ease of installation, removal, and reinstallation. Protection of the system is generally afforded via low-level signaling and use of TEMPEST approved equipment or an inspectable space. TEMPEST hazards such as crosstalk are problems that must be considered and their effects minimized. Secure voice systems should be isolated and source suppression fixes should be designed and incorporated by competent engineering and security authorities. System radiation and conduction levels that are in accordance with NSTISSAM TEMPEST/1-92 cannot be achieved through routine installation standards. Engineering fixes, when prudently applied with low-level techniques, do provide requisite protection.

5.3. Installation Guidance.

5.3.1. General. Select the countermeasure that contains the basic considerations for planning a secure voice installation. Where a conflict arises between that guidance and this appendix, the guidance contained herein apply.

5.3.2. Multiple Terminal Installations. When two or more secure voice terminals are installed in the same location, any one of which is capable of operating in a plain or cipher mode, the RED signal leads of each terminal should be installed using separate nonferrous shielded twisted pairs in the same cable or should be installed in separate shielded cables. Additional measures could be required when RED digitized text is transmitted.

5.3.3. Location. Console and automatic switches that could handle RED lines should be located in a secure area.

5.3.4. High-risk Areas. When secure voice terminals are installed in a high-risk area, residence or UAA, the following should be accomplished:

- Cable routing should be such that the cable run is not evident and meets the security requirements while blending with the decor and construction of the residence.
- All components of the system should be installed to prevent casual viewing.
- RED cable runs to remote instruments within the residence should be separated from all other distributions in the residence and should be metallically enclosed.

5.4. Security Guidance.

5.4.1. Terminals with Multiple Handsets. Visually monitor the on-hook or off-hook condition of the other handsets when using terminals with multiple handsets. This requirement is satisfied if all handsets can be viewed from any handset location.

5.4.2. Location of Equipment. The equipment of a secure voice terminal should be located together, and not within the view of uncleared personnel.

5.4.3. High-risk Areas. Due to limitation of physical safeguards and threat of technical surveillance, special considerations are required for these areas.

5.5. STU-III Guidance. The Secure Telephone Unit, Third Generation (STU-III), is a self-contained TEMPEST certified secure telephone device. It can be operated as a voice terminal, or can be connected to a data or facsimile device. When used for secure voice communications only, no additional TEMPEST treatment is required. When a STU-III connects to a RED processor, use a shielded cable with the shield bonded to the connector shell at both ends. If the RED processor is installed in the same general area as the STU-III, meets the separation recommendations of Section 3, and is afforded adequate physical security, no additional treatment is required. If the RED processor is installed in another room and the interconnect cable penetrates a barrier (e.g., a wall), the cable should be encapsulated in rigid conduit or cable duct. The STU-III can also be used as a trunking device to provide an interface with a RED switch. Installation should be in accordance with recommendations specified in this document.

NOTE: *External signal line and power line filters can cause the STU-III terminals to malfunction.*

SECTION 6

SENSITIVE COMPARTMENTED INFORMATION

6.1. General. This appendix sets forth criteria to permit RED sensitive compartmented information (SCI) and RED non-SCI to be processed through components of a single RED distribution system. Where the sharing of a single system is feasible, considerable cost savings can be realized. In some cases, the savings will permit wider application of secure voice and other services that otherwise could not be achieved if separate systems were required. In order to preclude unintentional compromise of SCI in shared systems, the constraints contained in this appendix take precedence over other recommendations. For most cases, the measures prescribed are sufficient to prevent unintentional misrouting of SCI into non-SCI channels and to limit SCI crosstalk into non-SCI circuits to levels that are nondiscernible except by a deliberate instrumented attack. An instrumented attack to exploit SCI crosstalk or other SCI radiated or conducted emanations present in U.S. controlled, non-SCI areas is viewed as unlikely, because only U.S. cleared individuals would have the access to mount such an attack. In most cases, the risk is considered acceptable, but where the cognizant SCI approval authority (Director of Central Intelligence Agency, Director of the National Security Agency, or Director of the Defense Intelligence Agency, as appropriate) deems necessary, additional requirements for safeguarding of SCI may be imposed with CTTA validation of the additional countermeasures. In some cases, the requirements of this appendix may be too restrictive and may be waived by the above authorities to allow both SCI and non-SCI under their cognizance to be processed over a single RED system.

NOTE: *The Director of Central Intelligence provides guidance on physical security for SCI facilities in DCID 1/21.*

6.2. Routing of SCI Cables. All SCI cables should be contained totally within the SCI areas unless installed in a protected distribution system (PDS) approved by the cognizant CTTA.

6.3. Termination Boxes. Separate dedicated termination boxes must be used for SCI circuits. These boxes are for convenience in interfacing the SCI signal cable to the terminal equipment and should be located close to the equipment. SCI termination boxes must be within SCI areas.

6.4. Distribution Frame. Separate dedicated distribution frames (any cabinet or box containing terminal blocks for cable cross connects or interconnects) must be used for SCI circuits. A common SCI/non-SCI enclosure (cabinet, box, etc.) may be used, but a rigid partition must physically separate the SCI and non-SCI areas to preclude inadvertent cross connects or interconnects of SCI to non-SCI circuits. The SCI area must be conspicuously labeled "**Sensitive Compartmented Information (SCI)**." No matter that enclosure is selected, shields of SCI and non-SCI cables must not be tied back or disconnected upon entering a frame, but must continue into their respective areas to reduce the possibility of crosstalk between unshielded conductors. Similarly, SCI and non-SCI cross connects and interconnects must never be grouped together. If two enclosures are used, each with SCI and non-SCI areas, SCI cross connects and interconnects between the enclosures must be via separate conduit or separate overall shield so that separation and isolation from non-SCI circuits is maintained.

6.5. Patch Panels. Separate dedicated patch panels must be used for unencrypted SCI circuits and encrypted SCI circuits. SCI patch panels should be uniquely wired, using different styled jacks and plugs, or be sufficiently separated from other patch panels to preclude inadvertently cross patching SCI circuits to non-SCI (encrypted) circuits. SCI patch panels must be within

SCI areas, or under combination lock if outside SCI areas, with lock combination available only to SCI-cleared personnel.

6.6. Multiplexers, Video and Audio Switches, and Other Multiple Circuit Equipment. Multiplexers, video switches, audio switches and other multiple circuit equipments associated with RED unencrypted signal lines may be used to process both SCI and non-SCI, subject to the following conditions:

a. Plain Text Transmission. The probability of inadvertent plain text transmission of SCI to a non-SCI user due to channel slippage or other causes shall be no greater than one per million.

b. Unwanted Third Party Connection. The probability of an unwanted third party connection to an SCI circuit shall be no greater than one per million.

c. Crosstalk. Crosstalk levels between any channels within an equipment, to include those likely to yield worst case conditions (e.g., adjacent conductors or paths in the same cable, on the same printed circuit board, through the same integrated circuit component, etc.), shall meet the applicable standards below:

- 65 dB minimum audio crosstalk isolation at any frequency between 0.3 and 15 kHz.
- 60 dB minimum video crosstalk isolation at any frequency up to 5 MHz with nonsynchronous sources.
- 30 dB minimum baseband digital crosstalk isolation. Baseband is defined as the frequency range from the digital rate (R_d) to 10 R_d.

6.7. Access Points. Access to all points with breakouts of the SCI circuits must be restricted to SCI-cleared personnel. Access points containing SCI and non-SCI circuits that do not have breakouts of the SCI circuits can be serviced by non-SCI personnel, if escorted by appropriately cleared SCI personnel. These requirements apply both within SCI areas and for protected signal distribution systems external to SCI areas.

6.8. Cables. Separate dedicated cables must be used for SCI circuits, e.g., all conductors within the overall sheath of a cable carrying SCI can be used only for SCI circuits. All metallic cables installed in the signal distribution system must have, as a minimum, one overall nonferrous shield, with the exception that applications requiring coaxial cable must use a cable having a separate insulated shield, e.g., twinaxial or triaxial (preferably twinaxial for data rates up to 1 MHz and triaxial for data rates above 1 MHz). Section 3 and Section 4, paragraph 4.4. provide additional signal line guidance including use of optical fiber cables.

6.9. Low-level Signaling. A design objective of the signal distribution system is that all digital signals comply with the low-level criteria in MIL-STD-188-114. Exceptions must be evaluated and approved on a case-by-case basis by the appropriate accrediting CTTA.

6.10. Power and Signal Line Filtering. The accrediting CTTA should determine the requirement for power and signal line filtering.

6.11. Standard Service Features. Generally, SCI systems should use the standard service features of the overall facility used for secure non-SCI systems such as power, ground systems, etc.

6.12. Telephone Lines. The accrediting authority should determine, on a case-by-case basis, the need for filtering or optical isolation at the point of entry all telephone lines entering an SCI facility containing equipment (TEMPEST approved or not approved) that process SCI data. If the telephone lines have been filtered or optically isolated at the boundary of a lesser classified area prior to entry to the SCI facility, the requirement for additional filters or isolators at the SCI facility boundary should be evaluated by appropriate accrediting CTTA.

6.13. RED/BLACK Separation. The RED/BLACK separation recommendations in Section 3 apply for systems processing SCI data.

6.14. Additional Requirements. Contact the cognizant SCI approval CTTA to ascertain whether additional RED/BLACK and TEMPEST measures are required for facilities processing SCI.

THIS PAGE IS INTENTIONALLY LEFT BLANK

SECTION 7

TRANSPORTABLE SYSTEMS IN A TACTICAL ENVIRONMENT

7.1. General. The primary TEMPEST vulnerability of transportable systems operated in a tactical environment is NONSTOP. This appendix provides guidance to protect against this vulnerability.

7.2. Modes of Operation. Transportable systems can be operated in various modes including;

- fixed or docked to a permanent facility for sixty or more days,
- field deployed to one location less than sixty days,
- vehicular mounted and operated on the move or stopped for less than one day.

Transportable systems can be operated singly or in groups. Groups can be operated with interconnecting cables.

7.2.1 Fixed Operation. Transportable systems operated at a fixed location for sixty or more days shall be installed according to Recommendation I of Table 3-1. In addition, the following recommendations apply.

7.2.1.1. RED Cables. RED wire cables shall be shielded and insulated overall.

7.2.1.2. Separation. RED processors should be separated by one meter from any BLACK equipment with wire lines that exit the inspectable space or are connected to an RF transmitter. If the separation cannot be maintained, the CTTA must conduct a review to determine whether filters or other countermeasures should be recommended. For existing facilities the CTTA could request TEMPEST/NONSTOP tests be performed to determine needed countermeasures.

7.2.1.3. CTTA Review. Vulnerabilities introduced by operating in a tactical environment could affect the requirements for inspectable space definition, power source restrictions and grounding procedures and should be reviewed by the CTTA. The CTTA could request TEMPEST/NONSTOP be performed to determine needed countermeasures.

7.2.2. Field Deployed. Transportable systems deployed in the field for less than sixty days should meet the recommendations in paragraphs 7.2.1.1. and 7.2.1.2.

7.2.3. Vehicular Mounted. If the vehicular mounted systems do not use commercial power and have no conductors egressing the inspectable space, only the following recommendations apply. A CTTA should review all other vehicular mounted systems to determine if additional countermeasures apply.

- RED processors should not be powered from the same circuit breaker panel as RF transmitters.
- RED wires shall be shielded and insulated overall.
- RED wire lines shall be separated by five centimeters from BLACK wire lines and BLACK power lines connected to an RF transmitter.
- RED processors should be separated to the maximum extent possible but not less than five centimeters from BLACK wire lines and BLACK equipment.

Note: The CTTA could request TEMPEST/NONSTOP tests be performed to determine the TEMPEST security of the installation.

7.3. Deploying Equipment Away from Transportables. When deploying equipment to tents or buildings, any shielding provided by the transportable is lost. Field expedient installations may create TEMPEST vulnerabilities. Buildings could have many fortuitous conductors (visible or hidden) that can conduct signals beyond the inspectable space. If such an installation is to be in place for sixty or more days, the CTTA should determine whether any fixed facility installation procedures should be applied.

7.4. Physical Security. The management of inspectable space and the control of conductors leaving the inspectable space must be incorporated in the tactical physical security plan.

SECTION 8

AIRCRAFT

8.1. General. The primary TEMPEST vulnerability of aircraft systems (fixed wing, rotary wing, remote pilotless vehicle) is NONSTOP. This appendix provides guidance to protect against this vulnerability.

8.2. Aircraft Installations. Aircraft installation vulnerabilities can be associated in two categories: airborne operations and ramp operations. The applications of TEMPEST design and countermeasures must consider weight, size, power consumption, cooling requirements and available space.

8.2.1. Airborne Operations. Aircraft systems will be installed according to Recommendation I of Table 3-1. In addition, the following recommendations apply.

8.2.1.1. RED Cables. RED wire cables shall be shielded and insulated overall.

8.2.1.2. Separation. RED processors shall be separated by one meter from any BLACK equipment with wire lines that exit the inspectable space or are connected to an RF transmitter. If the separation cannot be maintained, the CTTA must conduct a review to determine whether filters or other countermeasures should be recommended. For existing facilities the CTTA could request TEMPEST/NONSTOP tests be performed to determine needed countermeasures.

8.2.1.3. Grounding. Grounding onboard an aircraft is critical. While it may appear that the skin and structure of the aircraft provides an equipotential plane, empirical data shows that many current paths exist because of seams, material used and static buildup during flight. In addition, the aircraft structure provides power return, protective ground and signal grounds. These conditions must be considered when designing the grounding scheme. The following guidance supersedes Section 4.

- Protective ground systems should be installed according to MIL-HDBK-419A.
- There should be separate RED and BLACK ground systems. All ground systems should be separated from each other according to the recommendations in Section 3 and connected directly to the aircraft structure. A signal ground should be established at each component level requiring such a return path.
- Internal cable shields should be grounded by the most direct routing to the aircraft structure at one end only as close to the RED source as practical.
- Cable overall shields should be grounded at both ends and at intermediate points as practical.

8.2.2. Ramp Operations. All of the guidance for airborne operations apply for ramp operations. Vulnerabilities introduced by operating in this environment could affect the requirements for inspectable space definition, power source restrictions and grounding procedures and should be reviewed by the CTTA. The CTTA could request TEMPEST/NONSTOP be performed to determine needed countermeasures.

8.2.3. Physical Security. The management of inspectable space and the control of conductors leaving the inspectable space must be incorporated in the ramp operations physical security plan.

THIS PAGE IS INTENTIONALLY LEFT BLANK

SECTION 9

SHIPS

9.1. General. The primary TEMPEST vulnerability of ships is NONSTOP. This appendix provides guidance to protect against this vulnerability.

9.2. Shipboard Installations. Shipboard installation vulnerabilities can be associated in two categories: underway (at sea) and in port.

9.2.1. Underway Operations. Shipboard systems will be installed according to Recommendation I of Table 3-1. In addition, the following recommendations apply.

9.2.1.1. RED Cables. RED wire cables shall be shielded and insulated overall.

9.2.1.2. Separation. RED processors shall be separated by one meter from any BLACK equipment with wire lines that exit the inspectable space or are connected to an RF transmitter. If the separation cannot be maintained, the CTTA must conduct a review to determine whether filters or other countermeasures should be recommended. For existing facilities, the CTTA could request TEMPEST/NONSTOP tests be performed to determine needed countermeasures.

9.2.1.3. Shielded Cables. Shielded cables must meet the applicable requirements of MIL-C-17, MIL-C-915, MIL-C-24640, OR MIL-C-24643.

9.2.1.4. RED Ground. RED equipment must be bonded to ground according to MIL-STD-1310.

9.2.1.5. Cryptographic Equipment Ground. Cryptographic equipment must be bonded according to installation control drawings. In the absence of installation control drawings, bond according to MIL-STD-1310.

9.2.1.6. Cable Distribution. Cables may contain conductors connected to both a RED distribution system and a BLACK distribution system provided the RED conductors are either shielded individually or overall and separately from the BLACK conductors. This guidance supersedes Recommendation I, paragraph 2, Note 2 of Section 3.

9.2.2. In Port Operations. All shipboard systems shall be designed to comply with the requirements for underway operations as approved by the CTTA. Vulnerabilities introduced by operating in this environment could affect the requirements for inspectable space definition, power source restrictions, land line connections, etc., and should be reviewed by the CTTA. The CTTA could request TEMPEST/NONSTOP be performed to determine needed countermeasures.

9.2.3. Physical Security. The management of inspectable space and the control of conductors leaving the inspectable space must be incorporated in the port physical security plan.

THIS PAGE IS INTENTIONALLY LEFT BLANK

COMMENT FORM for NSTISSAM TEMPEST/2-95

Use one form per comment.

Return completed form to:

Attn: C3
Department of Defense
National Security Agency
Fort George G. Meade, Maryland 20755-6000

1. Date:

2. Name of Contributor:

3. Name of Organization:

4. Address of Organization:

5. Reference section in document (page number, paragraph, line number if required; if general comment, describe subject to be discussed):

6. Comment (What should be changed?):

7. Alternative (What should it be changed to?):

8. Rationale (Why should change be made?):

If more space is required for any of the above items, use extra sheet(s) and attach to this form.