BY ORDER OF THE COMMANDER AIR INTELLIGENCE SURVEILLANCE AND RECONNAISSANCE AGENCY

AIR FORCE AIR INTELLIGENCE, SURVEILLANCE AND RECONNAISSANCE AGENCY INSTRUCTION 33-203

25 MAY 2011

Communications and Information

THE AIR FORCE INTELLIGENCE, SURVEILLANCE AND RECONNAISSANCE AGENCY TEMPEST AND EMISSION SECURITY PROGRAM

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

ACCESSIBILITY: Publications and forms are available on the e-Publishing website at **www.e-Publishing.af.mil** for downloading or ordering.

RELEASABILITY: There are no releasability restrictions on this publication.

OPR: AFISRA/A6SE

Certified by: AFISRA/A6 (Col Eric J. Pierce)

Supersedes: AFISRAI 33-203, 18 March 2008

Pages: 34

This instruction implements AFPD 33-2, *Information Assurance (IA) Program*, AFSSI 7700 *Emission Security (EMSEC)*, and the national TEMPEST program for Sensitive Compartmented Information Facilities (SCIF) in the Air Force Intelligence, Surveillance and Reconnaissance Agency (AFISRA). It establishes procedures to control compromising emanations (CE) within AFISRA facilities. It brings AFISRA into compliance with national and Department of Defense (DoD) TEMPEST policies. It requires compliance with Committee on National Security Systems Policy (CNSSP) 300, *National Policy on Control of Compromising Emanations*, and Department of Defense Directive 5200.19, *Control of Compromising Emanations (C)*. This TEMPEST instruction and criteria apply to AFISRA and AFISRA subordinate units worldwide, which operate, maintain, and install systems and equipment used to process National Security Information (NSI). This instruction also applies to AFISRA-gained Air National Guard and Air Force Reserve units and Individual Mobilization Augmentees. This instruction also applies to all AFISRA-collocated units/organizations on Security Hill, Lackland AFB and Port San Antonio and their respective buildings and facilities. This instruction does not apply to AFISRA activities whose non-AFISRA hosts provide TEMPEST or technical security. Contact the host's security officials for guidance. Refer recommended changes and questions about this publication to the Office of Primary Responsibility (OPR) using the AF Form 847, *Recommendation for Change of Publication*; route the AF Form 847 from the field through the appropriate functional's chain of command to AFISRA/A6SE, 102 Hall Blvd, Ste 231, San Antonio TX 78243-7099. Maintain records created as a result of the prescribed processes identified in this

directory in accordance with (IAW) AFMAN 33-363, *Management of Records*, and dispose of them IAW the AF Records Disposition Schedule (RDS) found on the Air Force Portal link at **https://www.my.af.mil/afrims/afrims/afrims/rims.cfm**. Contact supporting records managers as required.

SUMMARY OF CHANGES

This revision updates the guidelines for TEMPEST and EMSEC for the Air Force Intelligence, Surveillance and Reconnaissance Agency. The changes reflect the replacement of DCID 6/9 by ICD 705 and an increased emphasis on the TEMPEST accreditation process. It also includes new information on smart card readers, digital senders and cryptographic equipment. A definition of RED processor has been added as well as a reference to the NSA cable installation standards. Dual monitor separation requirements have also been clarified. The mandatory TEMPEST CBT requirement has been removed.

Chapter 1—INTRODUCTION **4**

1.1. The AFISRA TEMPEST Program. 4

1.2. The AFISRA TEMPEST Philosophy. 4

Chapter 2—HEADQUARTERS FUNCTIONS **7**

2.1. Authority. 7

2.2. Directorate of Communications (AFISRA/A6). 7

2.3. Directorate of Logistics, Installations and Mission Support (AFISRA/A4/7). 7

2.4. The Directorate of Plans, Requirements and Programs (AFISRA/A5/8/9). 8

2.5. The Security Office (AFISRA/SO): 8

2.6. HQ AFISRA and HQ AFISRA-Collocated Units. 8

2.7. Engineering and Installation. 8

2.8. Maintenance. 9

2.9. Acquisition. 9

Chapter 3—UNIT RESPONSIBILITY **10**

3.1. AFISRA Units. 10

3.2. Unit TEMPEST Officer. 10

Chapter 4—PERSONNEL **12**

4.1. Documentation. 12

4.2. When Using Electronic Equipment. 12

4.3. TEMPEST Training Requirement. 12

Attachment 1—GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION **13**

Attachment 2—INSTALLATION CRITERIA 17

Attachment 3—VIDEO EQUIPMENT 22

Attachment 4—SECURE VOICE EQUIPMENT 23

Attachment 5—ADMINISTRATIVE TELEPHONES 24

Attachment 6—ENTERTAINMENT AND PUBLIC ADDRESS SYSTEMS 25

Attachment 7—FIBER OPTIC CABLE 26

Attachment 8—TACTICAL EQUIPMENT 28

Attachment 9—FACILITY SHIELDING AND SHIELDED ENCLOSURES 29

Attachment 10—GROUND MAINTENANCE 30

Attachment 11—WIRELESS DEVICES 31

Attachment 12—OFFICE EQUIPMENT 33

Chapter 1

INTRODUCTION

1.1. The AFISRA TEMPEST Program. This instruction describes the AFISRA TEMPEST program related to the Air Force, the National Security Agency, Central Security Service (NSA/CSS) and the Defense Intelligence Agency (DIA). AFISRA, as a Field Operating Agency (FOA) of Deputy Chief of Staff, Intelligence, Surveillance and Reconnaissance (HAF/A2) and a Service Cryptologic Component of the NSA/CSS, adopts applicable portions of DoD, USAF, DIA, and NSA/CSS documents to conduct the AFISRA TEMPEST program. The national policy is contained in Intelligence Community Directive (ICD) 705, *Sensitive Compartmented Information Facilities (SCIF)*, the Committee on National Security Systems Policy (CNSSP) 300, *National Policy on Control of Compromising Emanations*, and the Committee on National Security Systems Instruction (CNSSI) 7000, *TEMPEST Countermeasures for Facilities (C)*. The DoD TEMPEST program is contained in DoD Directive 5200.19, *Control of Compromising Emanations (C)*, and DoD 51 05.21-M-I, *Sensitive Compartmented Information Administrative Security Manual*. The Air Force policy is contained in AFSSI 7700, *Emission Security*. Portions of these documents are paraphrased or referenced throughout this document. **Note:** Collateral only areas or facilities of AFISRA units must meet the requirements of the AF EMSEC program. See AFSSI 7700, paragraph 15, for guidance on AFISRA Special Category (SPECAT) facilities.

1.2. The AFISRA TEMPEST Philosophy.

1.2.1. Risk Management. TEMPEST countermeasures will be employed in proportion to the threat of exploitation. Countermeasure assessments will be performed or validated by a Certified TEMPEST Technical Authority (CTTA) to determine what protection, if any, is required. Expenditure of funds over normal installation costs to meet TEMPEST requirements must be approved by a CTTA.

1.2.2. Perimeter Protection. The prime objective of the TEMPEST program at all levels, national to AFISRA and below, is to contain compromising emanations within the inspectable space. Compromising emanations are unintentional signals that, if intercepted and analyzed, would disclose the national security information transferred, received, handled, or otherwise processed by information-processing equipment. These emanations or TEMPEST signals are a function of the TEMPEST characteristics of the information 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. As long as these signals are contained within the inspectable space boundary, the TEMPEST risk is deemed acceptable.

1.2.3. Inspectable Space (IS). IS is defined as the three-dimensional space surrounding equipment that processes classified and/or sensitive information within which TEMPEST exploitation is not considered practical or the legal authority to identify and/or remove a potential exploitation exists and is exercised. The IS may be the base perimeter, a fence around the facility, a building, or a room in a building. The means of escape may be spatial radiation, or conduction through phone lines, power lines, a transmitter, etc. As long as all means of escape are controlled or protected at the perimeter, the area is TEMPEST secure. The IS is determined by the SCIF Accreditation Authority's CTTA or the Air Force CTTA

for collateral areas. The IS for most military installations in the continental United States is the base perimeter.

1.2.4. TEMPEST Zone Testing. In cases of very limited IS or uncertainty exists concerning the amount of protection needed, TEMPEST zone testing could provide some assurance. The TEMPEST Zone Concept considers not only the free space attenuation inherent to the facility's IS, but also the attenuation provided by the physical building structure. This approach requires radio frequency (RF) attenuation measurements be performed to characterize each facility. Subsequent interpretation of the attenuation data according to prescribed criteria allows the partitioning of the facility by zone designations. Once a facility has been "zoned," the zone assignments may be used in conjunction with TEMPEST test data to assure existing equipment and systems are appropriately located and future equipment and systems are designed and built to appropriate TEMPEST requirements. This concept has proven to be extremely effective. Not only have increased flexibility and substantial savings been realized, but most importantly, field testing has shown that facilities using the zoning concept have become increasingly more "TEMPEST Secure." However, zoning only accounts for spatial radiation. Conducted emanations must be considered separately.

1.2.5. Good Engineering and Installation Practices. Although the term is imprecise, these installation practices are the basis of a quality RED/BLACK installation. Good engineering and installation practices are those which provide neat, clean, and orderly installations; protect cabling from inadvertent physical damage; provide a degree of cable accountability; and enhance the electronic security of AFISRA activities. These practices reduce electromagnetic interference, improve operational capability, facilitate ease of operation and maintenance and improve the overall appearance of installed systems.

1.2.6. Separation Distances in National Policy. The separation distances in national policy (NSTISSAM TEMPEST/2-95 and 2-95A) when used in a SCIF are based on RED signal wirelines having one overall shield and are to be used as a minimum. The TEMPEST accreditation of a SCIF identifies the specific RED/BLACK separation requirements. If a separation is not specified, it is AFISRA's policy to maintain a minimum of 20 inches or 50 centimeters between any RED processor and BLACK equipment or BLACK signal wirelines that exit the inspectable space or are connected to an RF transmitter to ensure there is not any physical contact or mutual conduction that would cause a hazard. Contact the AFISRA CTTA to obtain a TEMPEST accreditation or if the minimum separation distances cannot be achieved.

1.2.7. Recommended Method of Signal Distribution. Fiber optic cable is the recommended method of signal distribution in AFISRA SCIFs. It is AFISRA policy to migrate circuits to fiber optic cable whenever feasible. This is based on TEMPEST considerations and future requirements for greater data rates requiring larger bandwidths.

1.2.8. Certification and Accreditation. An important part of Information Assurance (IA) is certification and accreditation (C&A). The C&A process addresses vulnerabilities and threats with the goal of reducing the risk to an acceptable level. TEMPEST/EMSEC is a critical part of the C&A process in both the collateral and SCI environments. TEMPEST/EMSEC is essential in the accreditation of information systems and SCI facilities.

1.2.8.1. For SCI facilities, the accrediting authority (typically DIA or NSA) will provide the organization a TEMPEST accreditation message or letter identifying their inspectable

space, TEMPEST countermeasure requirements and the applicable RED/BLACK separation recommendation of NSTISSAM TEMPEST/2-95 or 2-95A. Information on the DIA accreditation process can be found at: **www.dia.ic.govlhomepage/dalsecurity/fieldltempest**, or calling DIA/DAC-2B at (703) 907-1299. Information on the NSA process is available by calling NSA/I7213 at (410) 854-6611.

1.2.8.2. For collateral areas, AFSSI 7700, Attachment 2 outlines the EMSEC Accreditation Process.

1.2.8.3. The TEMPEST/EMSEC accreditation document is the authoritative document identifying the requirements to contain compromising emanations within the inspectable space and is one of the three accreditations required for a SCIF to become operational with the other two being physical and information system accreditations.

Chapter 2

HEADQUARTERS FUNCTIONS

2.1. Authority. The Commander, AFISRA (AFISRA/CC) retains the authority to accept the TEMPEST risk for all AFISRA facilities. The risk must be accepted in writing and submitted to the appropriate SCIF CTTA.

2.2. Directorate of Communications (AFISRA/A6).

2.2.1. The Enterprise Security Branch (AFISRA/A6SE):

2.2.1.1. Manages the TEMPEST program for the AFISRA.

2.2.1.2. Interprets national and Air Force policy and guidance for the AFISRA.

2.2.1.3. Provides technical guidance for installing AFISRA mission and mission support equipment.

2.2.1.4. Provides guidance to the Directorate of Plans, Requirements and Programs (AFISRA/A5/8/9), Directorate of Logistics, Installations and Mission Support (AFISRA/A4/7), the 690th Network Support Group (690 NSG), and the 668th Alterations and Installation Squadron (668 ALIS) on TEMPEST requirements for new system acquisitions, installations, and upgrades.

2.2.1.5. Evaluates 668 ALIS projects, contractor installations, and in-house projects for AFISRA and AFISRA units to ensure they meet AFISRA TEMPEST criteria.

2.2.1.6. Sends recommendations for the acceptance of the risk of a TEMPEST hazard through the AFISRA/A6 to the AFISRA Commander (AFISRA/CC) for approval or disapproval based on implementation of CNSSI 7000 and the TEMPEST Accreditation, and includes recommendations for corrective action.

2.2.1.7. Performs program reviews of AFISRA units and collocated units, conducts TEMPEST workshops to train new TEMPEST officers and informs current officers of the latest changes in TEMPEST policies and practices.

2.2.1.8. Reviews and coordinates on System Security Plans and System Security Authorization Agreements to ensure TEMPEST compliance.

2.2.2. The HQ AFISRA TEMPEST Program Manager (AFISRA/A6SE) develops, implements, and conducts annual TEMPEST program reviews for AFISRA units and those Lackland AFB and Port San Antonio collocated units identified in paragraph 2.6. Other San Antonio area facilities may also fall under this program as units are relocated. Program reviews will be scheduled and conducted throughout the calendar year. TEMPEST deficiencies are identified, documented and monitored for correction. Periodic updates as defined in the program review report will be submitted to AFISRA/A6SE until all discrepancies are closed. AFISRAICL 90-203 is used for these program reviews.

2.2.3. Recommends to SAF/A6N an individual to serve as the AFISRA Certified TEMPEST Technical Authority.

2.3. Directorate of Logistics, Installations and Mission Support (AFISRA/A4/7).

2.3.1. Logistics Readiness Division (AFISRA/A4R):

2.3.1.1. Coordinates with AFISRA/A6 on all planning efforts for new hardware capabilities to ensure TEMPEST requirements are identified and adequately addressed in the acquisition logistics support planning process.

2.3.1.2. Coordinates with AFISRA/A6 on all support agreements where TEMPEST is involved.

2.3.2. The Civil Engineering Division (AFISRA/A7C) coordinates with AFISRA/A6 on all new systems, facility upgrade requirements, designs and new construction that impact on TEMPEST criteria.

2.4. The Directorate of Plans, Requirements and Programs (AFISRA/A5/8/9).

2.4.1. Ensures all AFISRA policies, directives, and projects consider potential TEMPEST requirements through coordination with AFISRA/A6.

2.4.2. Coordinates with AFISRA/A6 on support agreements where TEMPEST is involved.

2.5. The Security Office (AFISRA/SO):

2.5.1. Coordinates with AFISRA/A6 on all TEMPEST accreditation matters, technical security reports, and surveys for AFISRA-sponsored SCIFs.

2.5.2. Coordinates with AFISRAlA6 on physical security matters as they pertain to TEMPEST within the criteria of ICD 705, DoD 5105.2l-M-l and other SCIF security documents.

2.6. HQ AFISRA and HQ AFISRA-Collocated Units. For consistency across the Lackland AFB and Port San Antonio area including shared spaces, HQ AFISRA directorates and major staff offices and non-AFISRA units collocated on Security Hill, Lackland AFB and Port San Antonio, have the following responsibilities for their respective buildings and facilities:

2.6.1. Each organization appoints a primary and alternate TEMPEST officer to assist the AFISRA TEMPEST Program Manager. These TEMPEST officers must submit an appointment letter to AFISRA/A6 which includes their names, ranks, office symbols, building and room numbers, telephone numbers, NIPRNet and classified (JWICS or SIPRNET) e-mail addresses.

2.6.2. Organizational TEMPEST officers assist the AFISRA TEMPEST Program Manager in their annual TEMPEST program review and are responsible for initiating corrective actions on any documented discrepancies.

2.6.3. Each agency follows the TEMPEST security program developed and implemented by AFISRA/A6. Organizational TEMPEST officers are responsible for coordinating with AFISRA/A6 on any equipment installations or facility modifications that may affect TEMPEST security.

2.6.4. Individual project offices coordinate TEMPEST requirements directly with the AFISRA CTTA in AFISRA/A6 for mission systems.

2.7. Engineering and Installation. The 668 ALIS ensures that all 668 ALIS-installed mission and information systems at AFISRA facilities comply with this TEMPEST instruction.

2.8. Maintenance. The 690 ISS ensures that all mandatory TEMPEST modifications to telecommunication and COMSEC equipment are performed, TEMPEST corrective actions are implemented as required, all telecommunications programming documents encompass TEMPEST criteria as appropriate, and TEMPEST policies and procedures are incorporated into COMSEC annexes to plans.

2.9. Acquisition. AFISRA acquisition organizations ensure TEMPEST considerations are addressed and included in the procurement and life cycle support phases for all hardware capabilities scheduled for deployment to AF ISR activities.

Chapter 3

UNIT RESPONSIBILITY

3.1. AFISRA Units. The AFISRA unit commander will appoint in writing a TEMPEST officer and forward a copy of the appointment letter to AFISRA/A6SE. TEMPEST officers must be appointed at all organizational levels necessary to exercise span of control related to size and geographic dispersion. In some cases, a higher headquarters collocated with a subordinate unit may assume TEMPEST responsibilities. The appointment letter will include their names, ranks, office symbols, building and room numbers, telephone numbers, NIPRNet and classified (JWICS or SIPRNET) e-mail addresses. Submit updates when changes are required. Recommend that the appointed unit TEMPEST officer is from a technical career field and has a working knowledge of electronics. TEMPEST officers can be military, civilian or contractor, but need to have sufficient rank or authority to enforce the requirements of the program.

3.2. Unit TEMPEST Officer.

3.2.1. Serves as the focal point for all unit TEMPEST matters including the TEMPEST accreditation and reaccreditation of SCIFs.

3.2.2. Maintains a reference library of TEMPEST publications. As a minimum, the library must contain NSTISSAM TEMPEST/2-95 and 2-95A, (U//FOUO) RED/BLACK Installation Guidance, AFSSI 7700, Emission Security (EMSEC), AFISRAI 33-203, and AFISRAICL 90-203. For SCIFs include DoD 5105.21-M-1 and ICD 705. The library can be maintained electronically. The TEMPEST Accreditation message or letter must be in the reference library or readily available to the unit TEMPEST officer.

3.2.3. Attends Air Education and Training Command (AETC) course L30ARXXXXX-OT3A, TEMPEST Fundamentals or the TEMPEST workshop conducted by the AFISRA CTTA.

3.2.4. Periodically reviews TEMPEST documents and stays current with TEMPEST issues applicable to the unit's TEMPEST security. Information on the current AF EMSEC program is available at **https://private.afnic.af.mil/intra/emsec**/. Information on the AFISRA TEMPEST program can be found at: **https://www.intelink.gov/wiki/AF_ISR**_ Agency_ Enterprise Security/TEMPEST.

3.2.5. Is knowledgeable of all unit programs, including self-help, for installing or removing equipment or systems which process national security information electrically and ensures TEMPEST integrity is maintained.

3.2.6. Requests approval for the following items from the SCIF accreditation authority through their appropriate security office:

3.2.6.1. RF transmitters.

3.2.6.2. Commercial television systems.

3.2.6.3. Audio systems (with lines that exit the SCIF boundary).

3.2.6.4. Protected Distribution Systems (PDS).

3.2.6.5. Multilevel systems.

Note: Use DoD 5105.21-M-1, Appendix J, TEMPEST Addendum, if a DIA SCIF. Use NSA TEMPEST Accreditation Worksheet, if an NSA SCIF.

3.2.7. Inspects new or modified equipment, systems or facility installations, and ensures discrepancies are corrected before activation. Signs the AF Form 1261, *Command, Control, Communications and Computer Systems Acceptance Certificate*, and AF Form 332, *Base Civil Engineer Work Request*, as applicable.

3.2.8. Annually in September performs a TEMPEST program review of local facilities using AFISRAICL 90-203 modified to fit their TEMPEST Accreditation and any other local requirements. Sends a copy of the completed checklists to AFISRA/A6SE by 31 October and maintains a local file copy until superseded by the next annual program review. Per paragraph 2.2.2, units in the local San Antonio area will be inspected annually by the AFISRA TEMPEST Program Manager. These local program reviews are performed throughout the year instead of in September.

3.2.9. Maintains records of inspections that identify TEMPEST discrepancies and corrective actions in unit files until all discrepancies are corrected. Ensures actions for correcting TEMPEST discrepancies are reported quarterly to AFISRA/A6SE.

3.2.10. Provides information and a copy of the inspection results to the AFISRA CTTA if host base officials or other accreditation authorities inspect the AFISRA unit.

3.2.11. Monitors and guides local self-help activities for TEMPEST compliance.

3.2.12. Guides and assists local staff elements on TEMPEST matters and requests assistance from the AFISRA CTT A as required.

3.2.13. Maintains unit awareness of the TEMPEST program requirements through unit training programs, commander's calls, visual aids, etc.

3.2.14. Submits TEMPEST testing requirements or requests for evaluations to AFISRA/A6SE as required.

Chapter 4

PERSONNEL

4.1. Documentation. All AFISRA personnel who prepare or process requirements documents, operations plans, policies, directives, self-help installation projects, and any other document that proposes processing classified information electronically will ensure TEMPEST is considered. This requirement also applies to engineering proposals that result in operating, procuring, maintaining, or installing AFISRA equipment and systems, which process national security information. Contact AFISRAlA6SE for appropriate TEMPEST criteria and a standard statement.

4.2. When Using Electronic Equipment. All personnel will fully comply with TEMPEST policies and operating procedures when using electronic equipment that processes national security information.

4.3. TEMPEST Training Requirement. The AFISRA CTTA will periodically provide TEMPEST user awareness training material to unit TEMPEST officers to ensure users of classified information systems understand the TEMPEST program and their responsibilities. Unit TEMPEST officers will ensure material is disseminated to unit personnel and report completion to the AFISRA CTTA during annual program reviews.

BRADLEY A. HEITHOLD, Maj Gen, USAF
Commander

Attachment 1

GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

References

AFI 32-1065, *Grounding Systems*, 1 October 1998

AFPD 33-2, *Information Assurance (IA) Program*, 19 April 2007

AFMAN 33-214 Volume 1, *(S) Emission Security Assessment (U)*, 15 September 2003

AFMAN 33-363, *Management of Records*, 1 March 2008

AFSSI 7700, *Emission Security (EMSEC)*, 24 October 2007

AFSSI 7702, *Emission Security Countermeasures Review*, 30 January 2008

AFSSI 7703, *Communications Security: Protected Distribution Systems (PDS)*, 26 August 2008

AFISRAICL 90-203, *Management of TEMPEST Inspections in AF Intelligence, Surveillance and Reconnaissance Agency Sensitive Compartmented Information Facilities*, TBD

CNSSP 300, *National Policy on Control of Compromising Emanations*, April 2004

CNSSI 7000, *(U) TEMPEST Countermeasures for Facilities (C)*, May 2004

DCID 6/9, *Physical Security Standards for Sensitive Compartmented Information Facilities*, 18 November 2002

ICD 705, *Sensitive Compartmented Information Facilities*, 26 May 2010

Joint DoDIIS/Cryptologic SCI Information Systems Security Standards, 1 January 2006

DoDD 5200.19, *Control of Compromising Emanations (C)*, 16 May 1995

DoD 5105.21-M-1, *Sensitive Compartmented Information Administrative Security Manual*, August 1998

NSA/CSS Policy 6-15, *(U) NSA/CSS Secure Telephone System (C)*, 31 March 2006

NSTISSAM TEMPEST/2-95 and 2-95A, *(U//FOUO) RED/BLACK Installation Guidance*, 3 February 2000

NTISSI No. 4002, *(U) Classification Guide for COMSEC Information (S)*, 5 June 1986

NSTISSI No. 7001, *(U) NONSTOP Countermeasures (S)*, 15 June 1994

NSTISSI No. 7002, *(U) TEMPEST Glossary (S)*, 17 March 1995

NSTISSI No. 7003, *Protected Distribution System (PDS)*, 13 December 1996

TSG 1, *Introduction to Telephone Security*, March 1990

TSG-2, *TSG Guidelines for Computerized Telephone Systems*, March 1990

TSG 6, *TSG Approved Equipment*, June 2006

Adopted Forms

AF Form 332, *Base Civil Engineering Work Request*

AF Form 847, *Recommendation for Change of Publication*

AF Form 1261, *Command, Control, Communications and Computer Systems Acceptance Certificate*

Abbreviations and Acronyms

AETC—Air Education and Training Command

AFNIC—Air Force Network Integration Center

AFI—Air Force Instruction

AFMAN—Air Force Manual

AFISRA—Air Force Intelligence, Surveillance and Reconnaissance Agency

ANG—Air National Guard

C&A—Certification and Accreditation

CE—Compromising Emanations

CNSSP—Committee on National Security Systems Policy

CNSS—Committee on National Security Systems

COMSEC—Communications Security

CSA—Cognizant Security Authority

CTTA—Certified TEMPEST Technical Authority

DIA—Defense Intelligence Agency

DoD—Department of Defense

EMSEC—Emission Security

IS—Inspectable Space

ISD—Inspectable Space Determination

JWICS—Joint Worldwide Information Communications System

KVM—Keyboard, Video and Mouse

MAJCOM—Major Command

NIPRNet—Non-Secure Internet Protocol Router Network

NSI—National Security Information

NSA—National Security Agency

NTSWG—National Telecommunications Security Working Group

OPR—Office of Primary Responsibility

PDS—Protected Distribution System

RF—Radio Frequency

SCI—Sensitive Compartmented Information

SCIF—Sensitive Compartmented Information Facility

SIPRNet—Secret Internet Protocol Router Network

SPECAT—Special Category

TAD—Telephone Answering Device

USAF—United States Air Force

Terms

Certified TEMPEST Technical Authority (CTTA). An experienced, technically qualified government employee who has met established certification requirements according to National Security Telecommunications and Information Systems Security Committee—approved criteria and has been appointed by a United States Government department or agency to fulfill CTTA responsibilities.

Cognizant Security Authority (CSA)—. The single principal designated by the Senior Official of the Intelligence Community to serve as the responsible official for all aspects of security program management with respect to the protection of intelligence sources and methods.

Collateral Information—. All national security information classified under the provisions of an executive order, for which special community systems of compartments (e.g., Sensitive Compartmented Information) are not formally established.

Compromising Emanation. Unintentional signal that, if intercepted and analyzed, would disclose the information transferred, received, handled, or otherwise processed by any telecommunications or automated information—systems equipment.

Countermeasures—. 1) That form of military science that by the employment of devices and/or techniques, has as its objective the impairment of the operational effectiveness of enemy activity; 2) any action, device, procedure, technique, or other means that reduce the vulnerability of an automated information system.

Countermeasures Review. A technical evaluation of a facility that identifies the inspectable space, the required countermeasures, and the most cost—effective way to apply required countermeasures.

Emanation—. Unintended signals or noise appearing external to equipment.

Emission Security (EMSEC). The protection resulting from all measures taken to deny unauthorized persons information of value that might be derived from communications systems and cryptographic equipment intercepts and the interception and analysis of compromising emanations from cryptographic—equipment, information systems, and telecommunications systems.

Facility. 1) A real—property entity consisting of one or more of the following: a building; a structure; a utility system, pavement, and underlying land; 2) a physically definable area, which contains classified national security information-processing equipment.

Hazard—. A measure of both the existence and the compromising nature of an emanation. Hazards exist if, and only if, compromising emanations are detectable beyond the inspectable space.

Information Systems—. The organized collection, processing, transmission, and dissemination of information, in accordance with defined procedures, whether automated or manual. In information warfare, this includes the entire infrastructure, organization, and components that collect, process, store, transmit, display, disseminate, and act on information.

Inspectable Space. The three—dimensional space surrounding equipment that processes classified national security or sensitive information within which TEMPEST exploitation is not considered practical or where legal authority to identify or remove a potential TEMPEST exploitation exists and is exercised.

Labeling—. Consists of a tag identifying the signal on the cable.

Marking—. Consists of a color band or similar identifier on a cable to identify the level of classification of the information on the cable.

National Security Information—. Information that has been determined, pursuant to Executive Order 12958, Classified National Security Information, April 17, 1995, or any predecessor order to require protection against unauthorized disclosure, and is so designated.

RED and BLACK Concept—. Separation of electrical and electronic circuits, components, equipment, and systems that handle classified plain text (RED) information in electrical signal form from those, which handle unclassified or encrypted (BLACK) information in the same form.

RED Equipment (Processor)—. A term applied to equipment that processes unencrypted national security information that requires protection during electrical/electronic processing. RED processors include monitors, KVM switches, routers, switches, computers and other devices that process RED signals electronically.

TEMPEST—. A short name referring to the investigation, study, and control of compromising emanations from telecommunications and automated information processing systems.

TEMPEST—Certified Equipment. Systems or equipment that were certified within the requirements of the effective edition of NSTISSAM TEMPEST/I-92, Level I, or TEMPEST specifications as determined by the department or agency concerned.

Attachment 2

INSTALLATION CRITERIA

A2.1. Introduction. For ease of implementation of TEMPEST separation and other installation criteria, consideration should be given to creating RED and BLACK areas in mission, office and cubicle environments.

A2.1.1. **Scope.** The installation criteria apply to all AFISRA activities and components including telecommunications centers, which support these activities. At AFISRA activities where the unit is a tenant to another organization, enforce these guidelines to the fullest extent the host base allows. Be aware that criteria can be different between collateral and SCI areas.

A2.1.2. **Purpose.** This guidance is intended to promulgate, clarify, and augment national and United States Air Force installation guidance. When this document and NSTISSAM TEMPEST/2-95, 2-95A or AFSSI 7702 conflict, contact AFISRA/A6SE for guidance.

A2.1.3. **Background.**

A2.1.3.1. In the past, TEMPEST criteria dictated ferrous conduit and ducts, which enclosed both RED and BLACK cabling. Accordingly, operations floors and computer centers were a maze of special plumbing, which became an installer's nightmare.

A2.1.3.2. AFISRA could not fully implement the above guidelines because of the nature of our large mission areas. In theory, all of the system wiring from the receiver outputs, through all processors, recording and printing devices would be RED and all antenna cables would be BLACK. One glance inside an AFISRA signals intelligence (SIGINT) facility would indicate the impracticality of separately enclosing the hundreds of antenna cables, in conduit or duct, throughout their many diverse routings. Accordingly, AFISRA established a policy that the (RF) multi-couplers, preamps, etc., satisfactorily acted as isolation devices between RED equipment and the BLACK antennas (these devices attenuate conducted emanations or stray radiation in the reverse mode, that is, escaping the antennas). Periodic TEMPEST testing of entire field stations over the years has confirmed this theory and no compromising emanations have been found beyond the operations building. Where raised floors are used, AFISRA implemented a requirement to place all RED cables under the raised floor, and to install all BLACK cables overhead to the extent possible.

A2.1.3.3. With the change in the world's threat situation and the proliferation of commercial-off-the-shelf personal computers in the office environment and in AFISRA's large mission areas, previous guidance was no longer practical.

A2.1.3.4. TEMPEST standards such as NSTISSAM TEMPEST/2-95 and AFSSI 7702 have changed to reflect a risk management based approach to security. TEMPEST requirements are now based on criteria such as threat, amount of inspectable space, equipment type, physical control, etc.

A2.1.3.5. The current AFISRA TEMPEST policy is based on good engineering and installation practices and all wire line cabling having one overall nonferrous shield. Although the term "good engineering and installation practices" is nebulous, it is the

basis of documents such as NSTISSAM TEMPEST/2-95 and 2-95A, MIL-HDBK-419A, and AFSSI 7702 which attempt to define and explain these practices. For clarity, consider good engineering and installation practices as those which provide neat, clean, and orderly installations; protect cabling from inadvertent physical damage; provide wire line accountability; and enhance the electronic security of AFISRA activities. These practices reduce electromagnetic interference, improve operational capability, facilitate ease of operation and maintenance and improve the overall appearance of installed systems.

A2.1.3.6. Specific installation standards for an individual facility are identified in the TEMPEST accreditation and usually reference documents such as NSTISSAM TEMPEST/2-95, 2-95A, DoD 5105.21-M-l and AFSSI 7702. Additional standards are included in this instruction.

A2.1.3.7. In addition to TEMPEST standards, there may be other installation standards to consider such as the National Electrical Code, local construction standards, and in particular NSA installation standards, which can be found at **http://it.org.nsa.ic.gov/procmgmt/standards**. Failure to follow these standards can result in significant delays, additional costs, and possible denial of services.

A2.2. Signal Distribution and Installation.

A2.2.1. SCIF Cable Shielding Requirements. All RED metallic wire lines installed in a SCIF must have a minimum of one overall nonferrous shield (see NSTISSAM TEMPEST/2-95, section 6). If a metallic cable does not have at least one overall nonferrous shield, install the signal lines in conduit or duct. The AFISRA CITA in coordination with the SCIF accreditation authority must approve exceptions to this.

A2.2.1.1. Fiber Optic Cable. A fiber optic cable is the recommended method of signal distribution in AFISRA SCIFs. It is AFISRA guidance to migrate circuits to fiber optic cables when feasible. This guidance is based on TEMPEST considerations and future requirements for greater data rates requiring larger bandwidths. Fiber optic cable does not have an electromagnetic field that would cause a TEMPEST problem and does not require shielding or separation.

A2.2.1.2. Analog Signal Cables. Cables equipped with foil-type shields that generally provide adequate shielding for analog signals.

A2.2.1.3. Digital Signal Cables. Cables carrying digital data signals require a foil or braided shield that provides a minimum coverage of90 percent. Connect the shields to the RF-tight EMI (electromagnetic interference) connectors on each end so that 360-degree continuity between the cable shield and the connector is achieved.

A2.3. Distribution System Requirements.

A2.3.1. Separate unclassified, collateral, and SCI-signal lines as outlined in NSTISSAM TEMPEST/2-95, paragraphs 4.4.2.2 and 6.8.

A2.3.2. Terminate cable shields directly to the signal ground bus on the Intermediate Distribution Frame (IDF) and at the terminal block.

A2.3.3. Termination of cable shields should comply with NSTISSAM TEMPEST/2-95, paragraph 4.4.1.2. Incorrect termination of cable shielding and pigtails may induce TEMPEST emanations.

A2.3.4. Do not use cable shields as intentional current carrying conductors or as signal returns.

A2.3.5. Remove all abandoned and unused cables and conduit unless specifically programmed for use at a later date.

A2.3.6. Wireline separation distances for individual locations are found in the applicable TEMPEST Accreditation letter or message and NSTISSAM TEMPEST/2-95A, Section 3.

A2.4. Identification and Marking Requirements.

A2.4.1. The primary purpose of marking cables is to prevent accidental cross connections that could lead to a security incident. Marking consists of a 1/2, to 1-inch wide color band around the cable. Use GREEN or BLACK for unclassified, RED for collateral classified and YELLOW for SCI. Different color cables or connectors may also be used for marking. Marking and labeling requirements also exist in other standards such as NSTISSAM TEMPEST/2-95, paragraphs 4.4.2.2 and 4.5. Other color schemes may be used as long as they are documented, standardized and well understood by the organization.

A2.4.2. To standardize marking, control placement of signal lines and maintain an accountability of the signal lines between systems. Mark and label all signal lines at both ends unless both ends can easily be seen (i.e., short patch cables).

A2.4.3. Exceptions.

A2.4.3.1. The above policy applies to lines that run between different racks, hubs, switches, patch panels, etc. Lines contained within the racks do not require marking.

A2.4.3.2. The LADYLOVE operations area will continue to follow the LADYLOVE site Installation Standard.

A2.4.3.3. Other site exceptions are determined on a case-by-case basis and are to be approved by the AFISRA CTTA, AFISRA/A6SE.

A2.4.4. Mark all cables entering or leaving systems or racks containing equipment of multiple classifications regardless of where these systems or racks are installed.

A2.4.5. Mark the duct or conduit approximately every 25 feet and upon entering and exiting a wall or ceiling. Alternative methods of marking the conduit, such as paint, are acceptable if they clearly identify the highest classification level contained. Before implementing alternate schemes, consider the difficulty of changing the marking if the classification level changes and specific installation standards for some systems which may include marking requirements.

A2.4.6. Equipment classification is determined by the level of information processed and the equipment is typically marked with Standard Form 700 series labels.

A2.4.7. Typically, office and administrative workspaces have equipment and systems (telephone, fax, computer, etc) that are classified at various levels. Mark cables and ducts in the office and administrative areas.

A2.5. Patch Panel Requirements. See NSTISSAM TEMPEST/2-95, paragraph 4.5.2 and Section 6. The requirement to prevent inadvertent cross patching can be met in one of several ways.

A2.5.1. Connectors.

A2.5.1.1. Use different styles of connectors or cabling to distinguish between classification levels.

A2.5.1.2. If using the same connector type for multiple classification levels, different colors of connectors and/or cables for each classification level is also a viable option.

A2.5.2. Separation. Physical separation by a distance, which would eliminate the possibility of cross patching.

A2.5.3. Software. Different software protocol for each level of classified information that will not allow interface with other levels.

A2.5.4. SCI patch panels.

A2.5.4.1. Separate dedicated patch panels must be used for unencrypted SCI and encrypted SCI. BLACK encrypted SCI panel can be used for other BLACK connections.

A2.5.4.2. SCI patch panels must be uniquely wired, using different style jacks or plugs or sufficiently separated from other patch panels to prevent inadvertent cross connects.

A2.6. Separation Requirements:

A2.6.1. Since TEMPEST requirements are based on the location, inspectable space, type of equipment, physical control, etcetera; each unit or facility may have different installation criteria. The unit TEMPEST officer identifies criteria particular to their circumstances according to NSTISSAM TEMPEST/2-95 and 2-95A and as identified in their TEMPEST Accreditation. The Accreditation Authority (Defense Intelligence Agency [DIA] or the National Security Agency [NSA]) provides the TEMPEST criteria to the unit in a message or letter. Keep this letter or message on file. For collateral areas, the Wing IA office will identify the separation requirements using the EMSEC process outlined in AFSSI 7700.

A2.6.2. The separation distances in national policy (NSTISSAM TEMPEST/2-95 and 2-95A) when used in a SCIF are based on RED signal wire lines having one overall shield and are to be used as a minimum. The TEMPEST accreditation of a SCIF identifies the specific REDIBLACK separation requirements. If a separation is not specified, it is AFISRA's policy to maintain a minimum of 20 inches or 50 centimeters between any RED processor and BLACK equipment or BLACK signal wirelines that exit the inspectable space or are connected to an RF transmitter to ensure there is not any physical contact or mutual conduction that would cause a hazard. Contact the AFISRA CTTA to obtain a TEMPEST accreditation or if the minimum separation distances cannot be achieved.

A2.6.3. There are no physical separation requirements between SCI and collateral systems or cables outlined in NSTISSAM TEMPEST/2-95 except those in Section 6. However, sufficient precautions must be taken to ensure that no inadvertent cross connections between these systems occur.

A2.6.4. Many separation requirements use the term wirelines exiting the inspectable space to identify a subset of cabling that requires separation. For clarity, all cabling should be

separated to the extent possible in the context of good engineering and installation practices, but those wire lines that actually exit the inspectable space must be separated because they are available to the adversary. The inspectable space is identified in the TEMPEST accreditation.

A2.6.5. A CTTA may modify separation requirements based on a risk assessment.

A2.6.6. RED processors include monitors, KVM switches, routers, switches, computers and other devices that process RED signals electronically.

A2.7. Filters:

A2.7.1. Generally, power line filters are not required for AFISRA facilities in the CONUS. The SCIF Accreditation Authority (DIA or NSA) will specify power line filter requirements in the TEMPEST Accreditation.

A2.7.2. Signal line filters may be required on signal lines exiting the inspectable space on a case-by-case basis. The SCIF Accreditation Authority (DIA or NSA) will specify the filter requirements in the TEMPEST Accreditation. Optical isolators are the preferred method of signal isolation.

A2.8. Protected Distribution Systems (PDS). SCIF accreditation authority (DIA or NSA) approval must be obtained for a new PDS or to modify an existing PDS, before system installation or modification begins. For DIA SCIFs, see DoD 5105.21-M-I, Appendix J, TEMPEST Addendum. For NSA SCIFs, use the NSA TEMPEST Accreditation Worksheet. Additional PDS installation requirements may be found in NSTISSI Number 7003 or NSA/CSS Policy 3-12. AFSSI 7703 provides AF PDS policy and installation requirements.

A2.9. Isolation Requirements. Fortuitous conductors, which service or transit the secure area such as water lines, sewer lines, steam pipes, and any other metallic structures, are considered a means of escape for classified information. The SCIF Accreditation Authority will specify the isolation requirements for fortuitous conductors in the TEMPEST Accreditation. These typically consist of non-conductive breaks or grounding criteria.

A2.10. Cryptographic Equipment. Because the national policy does not address cryptographic equipment, the AFISRA will follow the installation criteria for cryptographic equipment located in AFSSI 7702.

Attachment 3

VIDEO EQUIPMENT

A3.1. Classified. Install secure video equipment as a RED processor according to the installation requirements of your TEMPEST accreditation, NSTISSAM TEMPEST/2-95, 2-95A or AFSSI7702.

A3.2. Unclassified:

A3.2.1. Ideally, install video equipment in break rooms and other areas where classified information is not discussed or electronically processed. Use it strictly for the convenience of unit personnel. Do not play classified video media on unclassified equipment.

A3.2.2. Cable television brought into the SCIF area is BLACK equipment. Install cable televisions according to the requirements of NSTISSAM TEMPEST/2-95. This applies to television receivers and associated signal lines.

A3.2.3. Television receivers within the SCIF must have the incoming antenna or cable service isolated to ensure TEMPEST and technical security are maintained. See NSTISSAM TEMPEST/2-95A, paragraph 4.9.6 for further details. A video cassette recorder (VCR) or DVD player are not acceptable isolation devices. Optical isolation at the SCIF entry point is the preferred method.

A3.2.4. In some cases, as stated in the TEMPEST Accreditation, commercial TV systems must be approved by the SCIF accreditation authority (DIA or NSA). For DIA SCIFs, see DoD 5105.21-M-I, Appendix J. For NSA SCIFs, use the NSA TEMPEST Accreditation Worksheet.

A3.3. Multilevel Systems. Any system that handles multiple classification levels such as video teleconferencing systems, keyboard-video-mouse switches, display walls, etc. must be specifically approved by the SCIF accreditation authority. Since these systems handle different classification levels in close proximity to each other and by various means, the risk of signal compromise is greatly increased over a system that only handles one classification level. Separation requirements are sometimes difficult if not impossible to meet. Therefore, these systems must either be on approved lists such as the NSA Enterprise Solutions List or be individually evaluated by the cognizant CTTA. The current policy on multi-position peripheral switches is contained in JDCSISSS, Chapter 19, and NSA/CSS Policy 6-28.

A3.4. Dual Monitors. The use of dual monitors is considered an acceptable risk for facilities that have at least 20 meters of inspectable space. The monitors should be configured such that one connects directly to an unclassified computer and the other is connected through an approved KVM switch. The two monitors must be separated by a minimum of 5 centimeters (2 inches). Other BLACK equipment, such as administrative telephones, should be placed the required separation distance from the monitor connected to the KVM switch. Facilities with less than 20 meters or other dual or multiple monitor configurations must contact the AFISRA CTTA for an assessment.

Attachment 4

SECURE VOICE EQUIPMENT

A4.1. Secure Telecommunications. A Secure Terminal Equipment (STE) is considered a BLACK processor and should be installed as an administrative telephone.

A4.1.1. When a STE is connected to a secure fax, computer, or some other classified processor; follow the guidance in NSTISSAM TEMPEST/2-95, paragraph 5.5. A4.1.2. Single line STEs may be used in SCIFs without additional protection. Plug jacks and specialized ringers are not required.

A4.1.3. Multi-line models may be used in SCIFs under the following conditions.

A4.1.3.1. Common ringer is used.

A4.1.3.2. All components and wires of the Key System Unit (KSU) are contained within the SCIF. If a telephone instrument connected to the KSU is located outside the SCIF, contact a CTTA for appropriate countermeasures.

Note: KSU approved for SCIFs are listed in the Telephone Security Group (TSG) 6, Guidelines for Computerized Telephone Systems (CTS).

A4.1.4. Do not use STEs with the speakerphone feature in a SCIF unless retrofitted to disconnect the console microphone and speaker. The Cognizant Security Authority (CSA) may grant waivers for conference rooms or special offices.

A4.2. NSA Secure Telephone System (NSTS). NSA/CSS Policy 6-15 provides installation guidance for the NSTS. NSTS telephones are installed as RED processors. NSA installation standards can be found at **http://it.org.nsa.ic.gov/procmgmtlstandards**. Failure to follow these standards can result in significant delays, additional costs, and possible denial of services.

A4.3. Audio Security. Avoid simultaneous use of secure voice equipment and BLACK telephone equipment. Care must also be taken to preclude inadvertent disclosure of SCI background conversations or data when using collateral secure voice terminals within an SCI area.

Attachment 5

ADMINISTRATIVE TELEPHONES

A5.1. System and Equipment Installation Requirements.

A5.1.1. Three options currently exist for telephone instruments in a SCIF.

A5.1.1.1. Install telephones meeting Telephone Security Group (TSG) Standard 6, published by the National Telecommunications Security Working Group (NTSWG)

A5.1.1.2. Fit TSG 6 telephone isolation devices to each instrument.

A5.1.1.3. Install a computerized telephone switch in compliance with TSG Standard 2.

A5.1.2. All components of the telephone system, Key Telephone System or Computerized Private Branch Exchange, serving AFISRA facilities should be wholly contained within the controlled area of the SCIF. Telephone lines, which egress the facility, are looked at on a case by-case basis by a CTTA.

A5.1.3. Guidance on the use of cordless and cellular telephones in AFISRA SCIFs is provided in JDCSISSS Chapter IS and additional restrictions may be imposed by the Special Security Office.

A5.2. Separation Criteria.

A5.2.1. All unclassified administrative telephones are considered BLACK processors and are to meet the installation requirements of the TEMPEST accreditation, NSTISSAM TEMPEST/2-95, 2-95A or AFSSI 7702.

A5.2.2. Avoid BLACK telephone lines on mission floors and computer and communications centers. If the telephone lines are routed under the raised floor with RED cables, totally encase the phone lines in ferrous conduit or braided shielded cable. AFISRA/A6SE must approve installation of BLACK signal lines under a raised floor.

A5.3. Grounding and Filtering Requirements.

A5.3.1. Ground all spare telephone wires and cable shields to a ground point established at the telephone filter panel or to the equipotential ground.

A5.3.2. Remove all abandoned cables and conduits unless specifically programmed for use at a later date.

A5.3.3. Do not filter or isolate BLACK telephone lines exiting the SCIF unless specified by a CTTA. Any filter requirements will be identified in the facility's TEMPEST Accreditation. If filtering is needed, a digital switch or a fiber optic line may provide sufficient protection.

A5.4. Prohibited Equipment. Speakerphones, headsets, and acoustic coupled equipment are generally prohibited, but may be used if they not do not pass/transmit sensitive audio discussions when they are idle and not in use and are approved by the telephone security officer or Special Security Office.

Attachment 6

ENTERTAINMENT AND PUBLIC ADDRESS SYSTEMS

A6.1. Comfort Music.

A6.1.1. AM/FM radios or audio amplifiers and associated equipment are used to provide entertainment or public address capabilities in areas under AFISRA's security cognizance.

A6.1.2. Tape recorders or combination radio receivers and tape recorders are prohibited unless their recording capability is disabled and/or disconnected. As a minimum, this involves disabling the recording head. However, digital voice recorders are allowed for official purposes, but must be inspected and approved by the Security Office (SO). Voice recorders will be secured and handled at the same classification level as the recordings on the device. Users will also comply with all applicable TEMPEST requirements when recorder is in use or when stored in an appropriate container. A log will be used to track device usage.

A6.1.3. Install the system's components (receivers, amplifiers, and speakers) within the SCIF's confines. Install extension speakers at entry control points (ECP), outside the building, or in any area within the same physically controlled (fenced) area where people have at least a SECRET clearance. Contact a CTTA if a signal line exits the controlled area.

A6.1.4. The system is considered a BLACK processor and is to be installed according to the TEMPEST Accreditation, NSTISSAM TEMPEST/2-95, 2-95A or AFSSI 7702. Use shielded cable throughout the system.

Note: Label antenna or speaker cables to identify them as music, television, or public address system cables.

A6.1.5. Microphones of some systems are used to provide unclassified public address announcements (such as fire, disaster preparedness, etc.).

A6.2. Cover Music. This subject is covered separately in ICD 705.

A6.3. Television Receivers. See Attachment 3.

Attachment 7

FIBER OPTIC CABLE

A7.1. Method of Signal Distribution. Fiber optic cable is the recommended method of signal distribution in AFISRA SCIFs. Migrating circuits to fiber optic cable as soon as feasible is based on TEMPEST considerations and future requirements for greater data rates requiring larger bandwidths.

A7.2. General. A fiber optic system converts an electrical signal to an optical signal, transmits the signal through an optical cable and reconverts the signal to electrical form at the other end of the fiber. Optical systems have several significant advantages over conventional cables when used to transmit RED clear text National Security Information (NSI) within AFISRA controlled areas. Fiber optic cables that have no metallic content do not conduct extraneous signals and are unaffected by electromagnetic fields. They are not subject to crosstalk, ground loop problems, or the transmission of common mode signals. They also do not have an electromagnetic field that would cause a TEMPEST problem and do not require any shielding.

A7.3. Applications. Fiber optic systems that have no metallic content can be used to prevent the unintentional transmission of RED information outside the controlled space because they do not create electromagnetic fields, which could be induced on the BLACK fortuitous conductors. A BLACK fiber optic cable may exit a RED area without further filtering or isolation. RED fiber optic cables may be used to traverse BLACK areas when Protected Distribution System criteria are met.

A7.4. Fiber Optic Cable Separation. Fiber optic cables need not comply with the RED/BLACK separation requirements of the TEMPEST Accreditation, NSTISSAM TEMPEST/2-95, 2-95A or AFSSI 7702.

A7.5. Cable Strengthening Member. The strengthening member included in some multi-fiber cables may contain embedded wires or mesh. **Note:** Any conductive component in the cable can act as a fortuitous conductor. For this reason, do not use fiber optic cables with metal or conductive material that egresses AFISRA facilities. Use of this type of cable external to AFISRA SCIFs will be addressed on a case-by-case basis.

A7.6. Multi-fiber Cables. Do not transmit RED and BLACK information within the same multi-fiber cable. Use separate cables with appropriate markings. Use separate fiber optic cables for each classification level (Collateral and SCI) of RED information that is processed. If allowed to use the same SCI cable for JWICS and NSANet, a distinctive marking and labeling scheme must be implemented as the fibers are separated out at each end in order to prevent misconnections.

Note: Large fiber cables that have multiple fiber bundles individually separated by opaque sheathing may be used to carry multiple classification levels. However, each individual bundle must carry only one classification level. The use of this method introduces additional risk of compromise and precautions must be taken to ensure that each bundle is clearly marked and labeled when the bundles are separated out from each other. The large fiber cable must be protected and marked in accordance with the highest level of classification carried by the cable.

A7.7. Common Mode Signal Rejection. Common mode rejection is a measure of how well an electronic device ignores a signal that appears simultaneously and in phase at both the input and

output terminals. A fiber optic system with the source and detector powered from different power supplies or amplifiers will eliminate all common mode signals.

A7.8. Fiber Optic Circuits. Fiber optic cable that has no metallic content exhibits no electromagnetic radiation characteristics; however, it is possible to damage or tap the optical fiber. Therefore, the fiber requires physical protection against damage and tampering.

A7.9. Fiber Optic Media Converters. These devices serve as modems, which convert the electromagnetic signals to light for transmission on fiber optic cables. Install as any other RED or BLACK equipment.

Attachment 8

TACTICAL EQUIPMENT

A8.1. References. See NSTISSAM TEMPEST/2-95 or AFSSI 7702 for Transportable Systems in a Tactical Environment.

A8.2. Tactical System Inspections. Use AFISRAICL 90-203 and modify locally according to NSTISSAM TEMPEST/2-95, 2-95A or AFSSI 7703 to perform TEMPEST inspections on tactical systems equipment. These systems are inspected annually or after a deployment, whichever comes first.

A8.3. Shielded Tactical Systems. Some tactical systems may be fully deployable, self-contained systems that are housed in a shielded enclosure. These shielded enclosures are inspected annually or after the system is moved, whichever comes first.

A8.4. Transmitters. Transmitters in tactical systems not meeting the installation requirements of NSTISSAM TEMPEST/2-95 are required to be evaluated by a CTT A according to NSTISSI 7001 and to meet the requirements of CNSSAM TEMPEST/OI-02.

A8.5. TEMPEST in the Airborne Environment. See NSTISSAM TEMPEST/2-95, Section 8 and ICD 705, for unique aircraft operations and installation.

A8.6. Aircraft Testing. Based on AFSSI 7702, all aircraft carrying AFISRA systems must be tested according to CNSSAM TEMPEST/O1-02 during airborne system procurements and modifications unless otherwise specified by a CTTA.

Attachment 9

FACILITY SHIELDING AND SHIELDED ENCLOSURES

A9.1. General. The use of shielded enclosures and alternative shielding materials must be based on the results of an evaluation performed according to CNSSI 7000. The evaluation must be conducted or validated by the cognizant CTTA. Shielded enclosures are to meet the requirements of NSTISSAM TEMPEST/l-95.

A9.2. Alternative Countermeasure. It is important to realize that shielded enclosures are only used when all other countermeasures are impractical or more costly. It is imperative that the CTTA be involved so that alternative TEMPEST countermeasures are considered before a shielded enclosure, wall, or facility shielding is used. Contact the AFISRA CTTA before any facility shielding is installed. Many alternative shielding products are available to meet specific needs.

A9.3. Window Treatments. Windows are one of the most vulnerable aspects of a facility. Numerous window treatment products have been developed to provide differing degrees of attenuation to various forms of wireless transmissions such as radio frequency and infrared. The TEMPEST Accreditation provided by the cognizant CTTA will identity if window treatments are required. The installation of window blast protection measures provides an excellent opportunity to also add wireless attenuation measures with minimal additional cost.

A9.4. Inspections. Shielding materials must be inspected at least annually for shielding effectiveness.

Attachment 10

GROUND MAINTENANCE

A10.1. Ground System Test. The purpose of a system ground test is to verify effective grounding exists for proper equipment operation and safety.

A10.2. Ground Plates. Accomplish testing at all ground plates on the interior of external walls and columns. Measure value at each ground plate in the fractional ohm range (i.e., approximately 1/10 ohm) at the ANIFLR-9 stations with a complete ground grid under the concrete floor. At non-ANIFLR-9 stations and other facilities without a complete under floor grid (i.e., separate clusters of ground rods only), the measured value will likely be in the low ohm range (i.e., 1 to 5 ohms).

A10.3. Initial Check. For communication-electronic facilities accomplish the initial check every 90 days for one year to develop a standard against which to compare future measurements. after initial measurements, accomplish periodic testing every 21 months and upon completion of major project upgrades. Erratic readings or problem ground connections should be checked at more frequent intervals. Communication-electronic facilities and ground check requirements are defined in AFI 32-1063, AFI 32-1065 and MILSTD-188-124B. For AFISRA, communication-electronic facilities are those primarily designed for communications purposes including some mission facilities, communications centers, etc. A communications closet with a phone switch and some network equipment does not qualify the facility as a communications-electronics facility. Discussions between the user, base civil engineers and the AFISRA CTTA will be used to resolve discrepancies between facility designations.

A10.4. Ground Checks. Ground checks are accomplished using appropriate test instrumentation designed for testing grounds. Additional guidance can be found in MIL-STD-l88-124B and MIL-HDBK-419A.

A10.5. Ground Checking Responsibilities. Responsibility for the maintenance of exterior grounds falls under the purview of Base Civil Engineering (BCE), AFI 32-1065, *Grounding Systems*. However, the responsibility for checking and validating operations floor and computer center ground connections rests with the user and is also performed according to AFI 32-1065. If the unit does not have the proper personnel or equipment to perform the internal ground checks, contact BCE or a contractor.

A10.6. Ground Check Files. Document results of the initial and periodic readings on a locally prepared chart specifically tailored to each site's requirements and maintain on file. Design the chart to easily identify fluctuations in readings over a period of time.

A10.7. TEMPEST Ground. Any ground specifically required for the effectiveness of a TEMPEST countermeasure (i.e., shielded enclosure, power filter, etc.) or TEMPEST certified equipment must be checked every 21 months. Although RED/BLACK separation is a countermeasure, it should not be considered in the context of the TEMPEST ground.

Attachment 11

WIRELESS DEVICES

A11.1. Purpose. Wireless, especially Radio Frequency (RF), devices and systems pose a particularly significant TEMPEST hazard if not installed using good engineering practices. Devices that fall under this category are radio transmitters, receivers, land mobile radios, receive and transmit pagers, cellular telephones, wireless microphones, cordless telephones, portable data assistants, wireless local area networks, etc. These devices are generally prohibited in a SCIF.

A11.2. Guidance. The DoD Portable Electronic Device policy places wireless devices into high, medium, and low vulnerability categories and provides initial guidance for their use. Guidance is also given in JDCSISSS Chapter 15. Receive-only pagers and infrared devices that convey no intelligence data (text, audio, video, etc.) such as mice, remote controls and pointing devices pose no TEMPEST risk and require no TEMPEST mitigation to be introduced into AFISRA SCIFs. Coordination with and approval from local security officials is required prior to introducing wireless devices into a SCIF.

A11.3. Radio Transmitters. Radio transmitters are inherently BLACK equipment; however, they produce an RF signal that can introduce problems. To preclude these problems, special attention must be paid to the installation. Transmitters that cannot meet the installation criteria of this document, the TEMPEST accreditation and NSTISSAM TEMPEST/2-95 and 2-95A must have additional shielding or be evaluated by a CTTA according to NSTISSI 7001 and tested to meet the requirements of CNSSAM TEMPEST/01-02.

A11.3.1. It is mandatory to locate the transmitter and antenna a minimum of three meters from any RED processor and as close as possible to the point the antenna cable penetrated the SCIF.

A11.3.2. The transmitter will not be powered from the same source as the RED equipment. As a minimum, it should have its own power source back to the SCIF main power panel.

A11.3.3. If the antenna cable exits the controlled space, ensure the RF cables are routed to or through the radio frequency multi-couplers, power dividers, or other RF equipment for isolation and a ground.

A11.3.4. The system should have an exceptionally good path to earth ground.

A11.3.5. When control and signal lines exit the controlled space consult a CTTA.

A11.3.6. Additional separation requirements for transmitter cabling are identified in NSTISSAM TEMPEST/2-95 and 2-95A.

A11.4. Approval Authority. Approval to install a transmitter in a SCIF shall be obtained before system installation begins from the SCIF accreditation authority (DIA or NSA). For DIA SCIFs, use DoD 5105.21-M-1, Appendix J, TEMPEST Addendum. For NSA SCIFs, use the NSA TEMPEST Accreditation Worksheet

A11.5. Transportable Requirements. When the transmitter equipment is contained within a shelter or van, see NSTISSAM TEMPEST/2-95, section 7, or AFSSI 7702, Attachment 2.

A11.6. Built-in Wireless Transmitters. Special care must be taken to not introduce devices with built-in wireless capabilities. In many cases, the user may not realize these capabilities exist. Client System Technicians and Information Assurance Managers must establish and enforce procedures to ensure built-in wireless capabilities are disabled or removed prior to introduction into the SCIF. RED equipment shall not contain any operational RF transmitters, unless it is an NSA approved radio with embedded encryption.

Attachment 12

OFFICE EQUIPMENT

A12.1. Purpose. All telephones and telephone systems installed in AFISRA SCIFs must meet the requirements of ICD 705.

A12.2. Telephone Answering Devices (TAD). TADs can be a Technical and/or TEMPEST security hazard. Therefore, precautions and prior CSA approval is required for a TAD.

A12.2.1. The TAD is used in a single occupant office, whereas the occupant has no one to answer their telephone or cannot forward the calls when they are absent. Other uses of a TAD are addressed on a case-by-case basis.

A12.2.2. Use the TAD model that does not have remote control capability (i.e., cannot call in for messages or have a remote room monitoring capability). As with any telephone equipment, the TAD is government-owned and -procured. No personal equipment is authorized.

A12.2.3. Install a TAD only with an administrative BLACK telephone or STE, if appropriate. Separation of the TAD from other unclassified or classified information processing systems will be according to TEMPEST installation guidelines of NSTISSAM TEMPEST/2-95.

A12.2.4. When no longer needed or defective, destroy the recording media according to applicable procedures for destruction of classified media based on the highest level of information being processed in the immediate area.

A12.2.5. Remove the recording media before performing any maintenance on the TAD.

A12.3. BLACK Computers. Unclassified computers, whether stand-alone or networked, are considered BLACK equipment. Install unclassified computers according to the TEMPEST accreditation, NSTISSAM TEMPEST/2-95, 2-95A or AFSSI 7702. They are also subject to all computer security measures.

A12.4. Facsimile Terminals. See JDCSISSS Chapter 16 for operating instructions for facsimile machines in a SCIF. Install all facsimile machines according to NSTISSAM TEMPEST/2-95 or 2-95A.

A12.4.1. Single mode facsimiles no longer require a System Security Plan for secure or unsecure facsimile machines. However, facsimiles still require approval from the Information Assurance Manager and the security office for operation within a SCIF. Operating procedures and the approval to operate letter must be available at the facsimile machine.

A12.4.2. Dual mode facsimile terminals (classified and unclassified) are no longer authorized per JDCSISSS, paragraph 16.3.1.1.

A12.5. Copiers. Install copiers as RED or BLACK devices according to the level of material allowed to process. Newer digital copiers have capabilities, which are detrimental to security including remote maintenance through modems or RF. Consult with local security officials to evaluate and possibly disable these capabilities.

A12.6. Typewriters. Presently, typewriters are rarely used to type classified information. Because of this, typewriters are not considered a TEMPEST problem and do not require any additional protection.

A12.7. Microwave Ovens. Microwave ovens do not constitute a TEMPEST hazard if they are properly installed. Federal health and safety standards, as well as FCC standards, severely limit microwave emanations from these ovens. Also, the relatively low duty cycles limit TEMPEST vulnerability.

A12.8. Refrigerators, Coffeepots, Toasters. These items are not radiators and are not considered a TEMPEST hazard.

A12.9. Unclassified Area. The creation of a de facto unclassified area is advisable for all equipment not processing classified information. Use partitions, signs, and equipment labels to denote this area. See NSTISSAM TEMPEST/2-95, paragraphs 4.3 and 4.9.

A12.10. Smart Card Reader. Not considered a TEMPEST hazard. Install for ease of use with no mandated separation requirements.

A12.11. Digital Senders. Install as either a RED or BLACK processor depending on the classification of the network it supports.