TEMPEST

TEMPEST is an unclassified name referring to investigations and studies of compromising emanations. It is sometimes used synonymously for the term "compromising emanations", e.g., TEMPEST tests or TEMPEST inspections. TEMPEST approved equipment or systems are those which have been certified under past or existing TEMPEST specifications or standards.

Historically NAG-1A/TSEC was the earliest TEMPEST standard. NAG-1A was superseded in 1965 by Federal Standard 222, "Radiation Standard for Communication and Other Information Processing Equipment." In 1970 a new series of documents entitled, "National COMSEC/EMSEC Information Memoranda (NACSEM)" replaced Federal Standard 222. These new documents are applicable to equipments in the development stage, during and subsequent to production, and after any modification.

The Defense Communications Agency (DCA) has also issued a series of TEMPEST documents concerned with RED/BLACK engineering. The DCA series of documents will be replaced in the near future by a new Military Handbook (MIL-HDBK-232), Military Standardization Handbook RED/BLACK Engineering—Installation Guidelines, prepared by the Naval Electronic Systems Command.

Since the above TEMPEST documents carry security classifications, they are available only to qualified contractors with security cleared facilities and an established need-to-know. The need-to-know must be established with the contracting Government Organization who will authorize the release of the TEMPEST documents to the contractor. The need-to-know can be established when there is a contract for equipment which must meet TEMPEST requirements. If there is no contract of this type, the contractor must be able to show that the release of TEMPEST documents to him would be of direct benefit to the Government in the future.

Commercial firms with TEMPEST related Government contracts should address inquiries pertaining to TEMPEST to their contracting Government Department or Agency. Commercial firms with no TEMPEST related contracts should address inquiries pertaining to TEMPEST to a Government Department or Agency with whom they have (or have recently had) a classified contract, or (if no such contract exists or has recently existed) to the Director, National Security Agency, ATTN: S22, Fort George G. Meade, MD 20755.

The Air Force is conducting a school on NACSEM at their Cryptologic Depot in San Antonio, Texas. This is open to employees of private organizations under contract with the Air Force. An Air Force contractor desiring training for his employees must forward a written request to the major air command or designated subcommand supervising the contract for which the training is necessary, at least 30 days before the date training should begin (refer to paragraph 112, AFT 205-1). If the contractor does not have a current contract but can show that the training would be of direct benefit to the Government in the future, he may forward his request to Headquarters, U.S. Air Force Security Service, ATTN: SRE, San Antonio, Texas 78243. They will evaluate each request on a case by case basis. It should be pointed out that generally the Government will not pay for such training.

The RED Analog Signal Line Conduction Limits and Digital Signal Line Conduction Limits of NACSEM 5100 are unclassified. These limits for the various categories A through G are shown in Figure 1 and 2. Note that the analog signal limits are given in dB above one microvolt r.m.s. while the digital signal limits are given in dB above one microampere per meter per MHz equivalent r.m.s. sinewave.

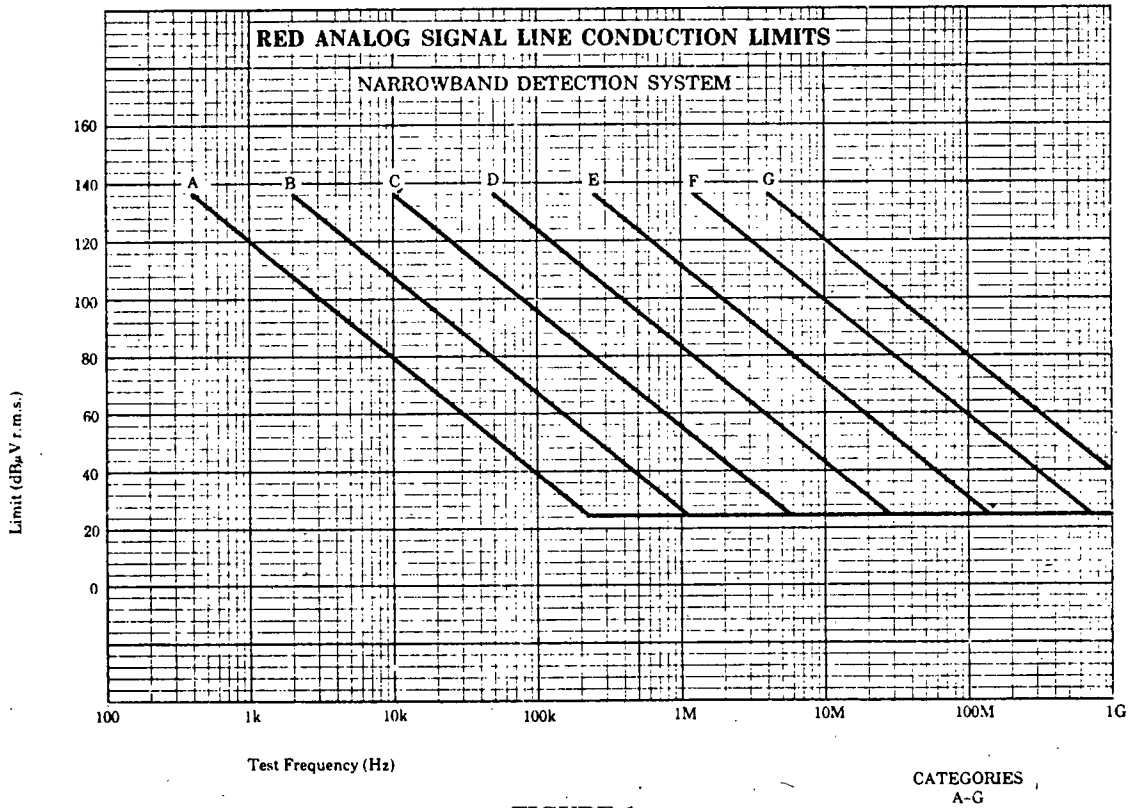

FIGURE 1

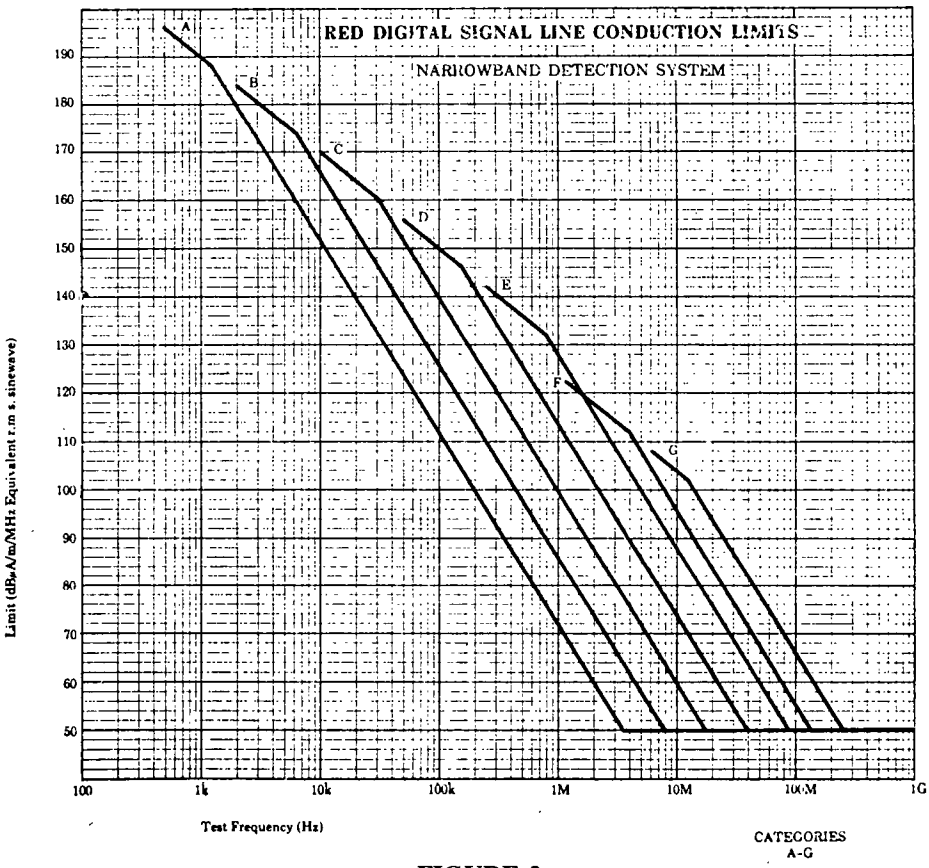

FIGURE 2

TEMPEST TERMS AND DEFINITIONS

Access . . . The ability and opportunity to obtain knowledge or classified information or to be in a place where one could be expected to gain such knowledge.

Alternating Current (AC) Protective Ground System . . . A ground system which provides a low resistance electrical connection to Earth Ground for the protection of personnel and equipment from AC power potentials, lightning hazards, and electrical circuit failures. The integrity of the system is normally insured by the connection of an insulated green colored conductor between the cases and frames of equipments afforded AC power service. The AC protective ground system is therefore often referred to as the Green Wire Protective Ground.

Black Designation . . . A designation applied to wirelines, components, equipment, and systems which handle only unclassified signals, and to areas in which no classified signals occur.

BLACK Equipment Area(s) (BEA) . . . The space within a Limited Exclusion Area (LEA) which is designated for installation of BLACK information-processing equipment, power, signal, control, ground feeder and distribution facilities

Classified Intermediate Distribution Frame (CIDF) . . . An Intermediate Distribution Frame used for RED wiring.

Combined Distribution Frame (CDF) . . . A distribution frame which serves as both a Main Distribution Frame and Intermediate Distribution Frame.

Communications Security . . . The protection resulting from all measures designed to deny unauthorized persons information of value which might be derived from the possession and study of telecommunications, or to mislead unauthorized persons in their interpretations of the results of such possession and study.

Compromise . . . Any occurrence which results in unauthorized persons gaining access to classified or other information requiring protection.

Compromising Emanation . . . Unintentional data-related or intelligence-bearing signals which, if intercepted and analyzed, disclose the classified information transmitted, received, handled or otherwise processed by any information-processing equipment.

Conducted Signals . . . Electromagnetic or acoustic signals propagated along wirelines or other conductors.

Controlled Access Area (CAA) . . . The complete building or facility area under direct physical control which can include one or more Limited Exclusion Areas, Controlled BLACK Equipment Areas, or any combination thereof. Spaces within a facility which are not under direct physical control but to which access is controlled (administration offices, halls, restrooms) are not a part of the actual Controlled Access Area but are considered as a part of the overall Physical Control Zone.

Controlled Black Equipment Area(s) (CBEA) . . . A BLACK Equipment Area which is not located in a Limited Exclusion Area but is afforded the same physical entry control which would be required if it were within a Limited Exclusion Area.

Equipment TEMPEST Radiation Zone (ETRZ) . . . A zone established as a result of determined or known TEMPEST equipment radiation characteristics. The zone includes all space within which a successful hostile intercept of Compromising Emanations is considered possible.

Fortuitous Conductor . . . Any conductor which may provide an unintended path for intelligible signals; for example, water pipe, wire or cable, metal structural members, and so forth.

Green Wire Protective Ground . . . See Alternating Current (AC) Protective Ground System.

Hardened Cable Path (HCP) . . . See Intrusion-Resistant Communications Cable (IRCC).

Intrusion-Resistant Communications Cable (IRCC) . . . A cable designed to provide substantial physical protection and electrical isolation for the wirelines making up the information-carrying core. When the protective measures used are devices which detect slight changes in the physical or electrical state of the cable and which provide visible or audible indications at a central control point of attempted intrusion, the cable is known as an Alarmed Cable. When the protective measures used are physical protection to provide a penetration delay factor, the cable is known as a Hardened Cable Path.

Isolation Device . . . A device designated to provide isolation and maximum attenuation of undesired signals with minimum insertion loss and distortion of the desired signal.

Limited Exclusion Area (LEA) . . . A room or enclosed area to which security controls have been applied to provide protection to a RED information-processing systems equipment and wirelines equivalent to that required for the information transmitted through the system. An LEA must contain a RED Equipment Area.

Normal Input Keying . . . Low level keying in which battery to the teletypewriter keying contacts is provided by the crypto-equipment.

Off-Line Crypto-Operation . . . Encryption or decryption performed as a self-contained operation distinct from the transmission of the encrypted text, as by hand or by machines not electrically connected to a signal line. See On-Line Cypto-Operation.

On-Line Crypto-Operation . . . The use of crypto-equipment that is directly connected to a signal line, making encryption and transmission, or reception and decryption, or both together, a single continuous process. See Off-Line Crypto-Operation.

Physical Compromise . . . The compromise of information through loss, theft, capture, recovery by salvage, defection of individuals, unauthorized viewing or photography, or by any other physical means.

Physical Control Zone (PCZ) . . . The space surrounding equipment processing classified information, which is under sufficient physical and technical control to preclude a successful hostile intercept of any classified information from within this space.

Protected Wireline Distribution System . . . A communications system to which electromagnetic and physical safeguards have been applied to permit secure electrical transmission of unencrypted classified information, and which has been approved by the cognizant department or agency. The associated facilities include all equipment and wirelines so safeguarded. Major components are wirelines, subscriber sets and terminal equipment. Also known as Approved Circuit.

RED/BLACK Concept . . . The concept that electrical and electronic circuits, components, equipments, systems, and so forth, which handle classified plain language information in electric signal form (RED) be separated from those which handle encrypted or unclassified information (BLACK). Under this concept, RED and BLACK terminology is used to clarify specific criteria relating to, and to differentiate between such circuits, components, equipments, systems, and so forth and the areas in which they are contained.

RED Equipment Area (REA) . . . The space within a Limited Exclusion Area (LEA) which is designated for installation of RED information processing equipment, power, signal, control, ground feeder and distribution facilities.

Signal Ground Point . . . A single designated point in a station to which all RED/BLACK grounds are either directly or indirectly connected. This point serves as the common zero potential reference for the station.

Signal Ground Reference Plane . . . An intermediate focal point between an equipment and the Signal Ground Plane for terminating an equipment's or Terminal System's RED or BLACK ground circuits. The Signal Ground Reference Plane is isolated from the equipment's AC Protective Ground and is connected to the Signal Ground Plane by a Signal Ground Bus.

Signal Ground Reference Point . . . Same as a Signal Ground Reference Plane but serving one of several Limited Exclusion Areas device or equipment or Terminal System.

Signal, Quasi-Analog . . . A quasi-analog signal is a digital signal, after conversion to a form suitable for transmission over a specified analog channel. The specification of an analog channel would include frequency range, frequency bandwidth, signal-to-noise ratio and envelope delay distortion. When this form of signaling is used to convey message traffic over dialed-up telephone systems, it is often referred to as voice data.

Single Point Ground . . . The basic technique used in RED/BLACK installations in which separate ground conductors are used for the various grounding functions (signal, power, hazard, and so forth) with each conductor connected directly or indirectly to a single point (Signal Ground Point).

Spurious Signals . . . Undesired signals appearing external to an equipment or circuit. They may be harmonics of existing desired signals, high frequency components of complex wave shapes, or signals produced by incidental oscillatory circuits.

TEMPEST . . . An unclassified short name referring to investigations and studies of compromising emanations. It is sometimes used synonymously for the term "comprising emanations"; for example, TEMPEST tests, TEMPEST inspection.

TEMPEST Approved Equipment or Systems . . . Equipment or systems which have been certified under existing (NACSEM 5100, KAG-30A, or DCAC 370-D195.2) or past (FED-STD-222) TEMPEST specifications as determined by the command or agency concerned.

TEMPEST Inspection . . . A general term which encompasses various means for conductng facility evaluations to determine the adequacy of TEMPEST control measures; for example, installation-engineering surveys.

TEMPEST Test . . . A laboratory or on-site (field) test to determine the nature and amplitude of conducted or radiated signals containing compromising information. A test normally includes detection and measurement of these signals, and analysis to determine correlation between received signals and potentially compromising transmitted signals.

Terminal Control Unit (TCU) . . . The device in an integrated complex of units constituting a complete Terminal System (TSY) which serves as the single interface point between the TSY and wireline distribution facilities of the Limited Exclusion Area. For example, the control device of a data terminal complex which has card or tape or card and tape devices and which control device is the single interface to the station wireline distribution facilities is considered, for engineering-installation purposes, as the Terminal Control Unit.

Timing Line . . . Line intended for the transmission of timing information, clock pulses, and crypto step.

Uncontrolled Access Area (UAA) . . . The area external or internal to a facility over which no personnel access controls can be or are exercised.

Vocoder . . . A vocoder (voice-operated coder) is a device used to compress the frequency bandwidth requirement of voice communications. It consists of an electronic speech analyzer which converts the speech waveform to several simultaneous analog signals and an electronic speech synthesizer which produces artificial sounds in accordance with analog control voltages.