

**TSG GUIDELINES FOR COMPUTERIZED  
TELEPHONE SYSTEMS**

**TSG STANDARD 2**

**March 1990**

## **PREFACE**

**This standard was prepared by the Telephone Security Group (TSG). The charter members of the TSG are: Department of the Air Force, Department of the Army, Central Intelligence Agency, Defense Intelligence Agency, Department of Energy, Federal Bureau of Investigation, Department of the Navy, National Security Agency, US Secret Service, and Department of State.**

**The TSG is the primary technical and policy resource in the US Intelligence Community for all aspects of the TSCM (technical surveillance countermeasures) program involving telephone systems. The TSG standards contain guidance for providing on-hook security to telephone systems in areas where sensitive government information is discussed. Implementation of TSG standards neither prevents the application of more stringent requirements nor satisfies the requirements of other security programs such as TEMPEST, COMSEC, or OPSEC.**

**TSG Standard I is an introduction to telephone security that provides general information about the TSG standards.**

## **TSG GUIDELINES FOR COMPUTERIZED TELEPHONE SYSTEMS**

### **PURPOSE**

**This standard establishes requirements for planning, installing, maintaining, and managing a computerized telephone system (CTS). The requirements established in this standard are necessary in order to achieve on-hook audio security for computerized telephones located in sensitive discussion areas. For a CTS conforming to this standard, all protected on-hook telephones will be completely isolated from all transmission media and wires that are physically unprotected. This standard requires that the isolation for most telephones be achieved in the CTS itself.**

### **BACKGROUND INFORMATION**

**TSG Standard 1 provides background information on telephone security and explains some of the principles underlying the requirements set in this standard.**

### **APPLICABILITY**

**This standard applies only to systems in which the CTS hardware, system wiring, and stations requiring isolation are located within a physically protected space (PPS). Stations outside the PPS cannot be isolated from the respective unprotected lines by the CTS. If on-hook audio security is required, telephones outside the PPS must be either type-accepted under TSG Standard 3 or 4 or must be protected by an approved isolator or disconnect device in conformance with TSG Standard 6.**

### **DEFINITIONS**

**A glossary of terms is provided for this standard. In some instances, the precise meaning of a technical term used in this standard may be at variance with its general use in industry. In those instances, the term will appear in the glossary with an exact definition of the intent with which it is used in this standard. It is important that the technical terms included in the glossary be understood to have only the specific meanings shown for them.**

**Some additional terms not appearing in this glossary are defined in TSG Standard 1.**

## **MINIMUM SYSTEM REQUIREMENTS**

### **1. Physical Security Requirements**

**a. A PPS must be established to provide positive physical protection for the CTS and all of its parts. This includes all stations, cables, lines, intermediate wiring frames, and distributed CTS modules necessary for the functioning of the stations.**

**b. Only the equipment or wiring not intended to be isolated by the CTS can be located outside the PPS.**

**c. All program media such as tapes or disks must be provided positive physical protection to prevent unauthorized alterations.**

**d. An up-to-date master copy of the program must be maintained for confirmation and/or reloading of the operating program. This master copy must be verifiable as having been protected against unauthorized alteration. It must be kept in a physically protected storage container, separate from all other program media.**

### **2. System Configuration Requirements**

**The system equipment and physical layout must isolate protected stations from all wires and transmission media leaving the PPS. All system wiring interconnections will be organized on wiring frames in accordance with the following paragraphs. The wiring frames will be situated to facilitate their electrical testing and visual inspection.**

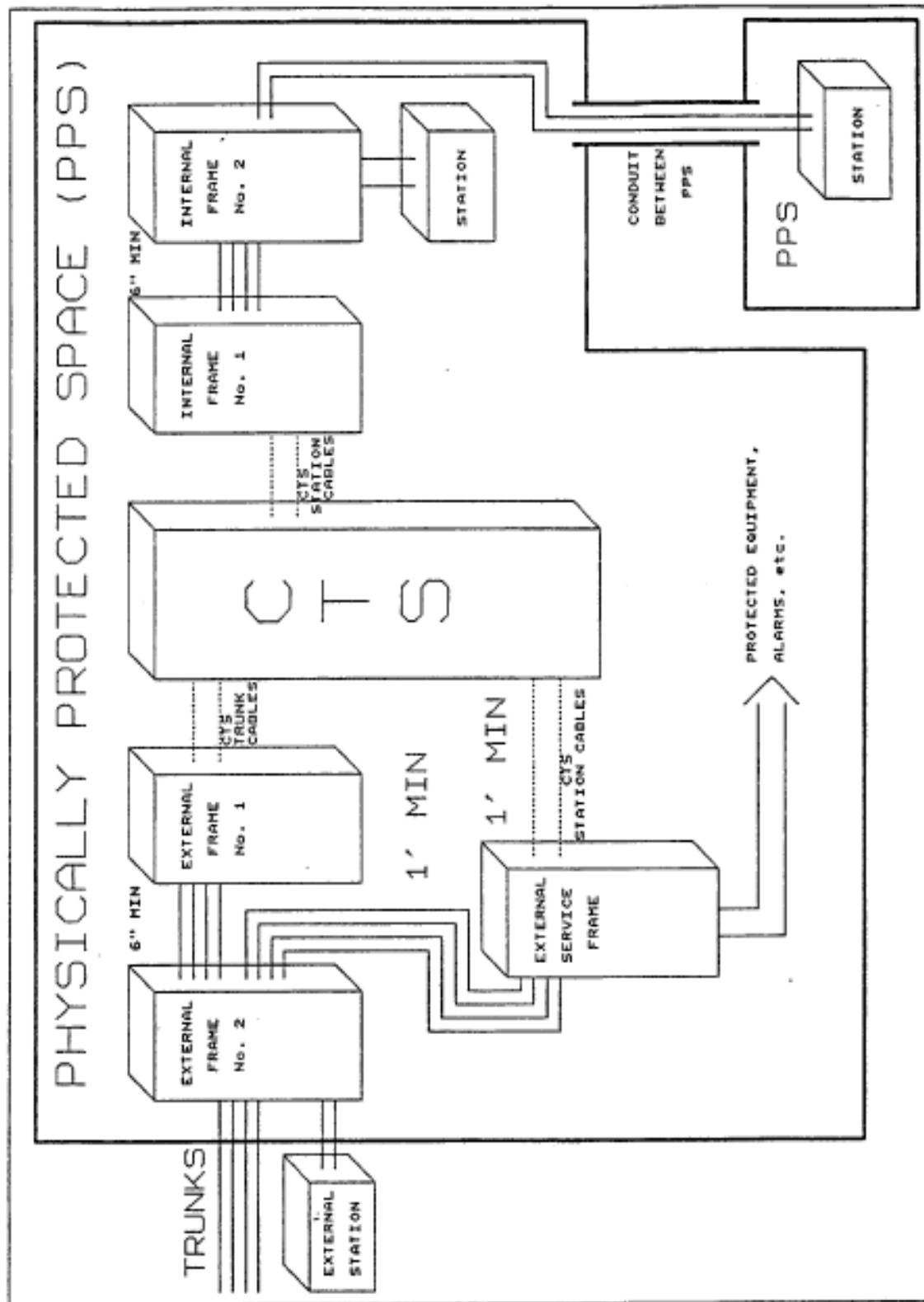
**a. A means must be provided to electrically inspect all transmission paths leaving the PPS for the presence of audio.**

**b. A set of external frames must be installed in the PPS to support CTS connections to the outside.**

**(1) The first external frame must be used to connect active trunks to the CTS. This may be in the form of a conventional telephone connecting block that allows inspection for unauthorized or concealed cross-connects to other frames.**

**(2) The second external frame must terminate all the wiring leaving the PPS. The termination point of incoming central office trunks, referred to as a demarcation point, normally incorporates USOCRJ21X connecting blocks. The demarcation point must lie outside the second external frame. There can be additional frames, as necessary, between the demarcation point and the second external frame.**

**(3) Cabling from the CTS to stations located outside the PPS will terminate on an external service frame. This frame will cross-connect to the second external frame for distribution outside the PPS. If non-CTS services inside the PPS require wiring connections outside the PPS, this wiring will also terminate at the external service frame and be cross-connected to the second external frame.**



**(4) Cross-connects between the external frames will be by separate single pair wires. No extra cross-connects will be permitted beyond the minimum number required to provide the needed-service.**

**(5) External frames will be physically separated by at least six inches from each other and by one foot from any other wiring frames or objects to allow visual inspection. Cross-connects between frames should be dressed neatly so that individual pairs can be visually traced from frame to frame.**

**c. Internal frames will be used to terminate all connections from the CTS to PPS equipment and stations. There must never be any cross-connects between internal and external frames (see figure on page 3).**

**d. Cable from internal and external frames must not be terminated in the same card rack. No two card racks may share common cabling to the wiring frames.**

**e. Subscriber stations of the CTS and trunk lines must be wired only to CTS port circuits. The signal isolation between noncommunicating port circuits must exceed 70 dB. Audio coupling between port circuits is permitted only when their associated stations or trunks are off-hook. Coupling between a port circuit and a CTS distribution or multiplex bus is permitted only when the associated station or trunk is off-hook.**

**f. Stations inside the PPS will not share CTS port circuits with stations outside the PPS. Stations inside the PPS will not have the same directory number as any station outside the PPS.**

**g. When CTS programming is stored electronically inside the CTS, for CTSs in which removable programming media are not used, the system must be capable of generating a complete memory listing for comparison with the master program copy.**

### **3. CTS Operations Characteristics**

**Some CTSs offer operational features that are not consistent with good audio security practice. Such features may cause the CTS to execute electronic functions that are expressly prohibited. In general, prohibited functions can compromise the isolation that must be provided by the CTS under this standard. When an operational feature of the CTS uses a prohibited function, the feature must be positively disabled in hardware.**

**The following paragraphs define both required and prohibited characteristics of a CTS.**

**a. The off-hook condition of a subscriber station must be initiated by the user at the station. However, the CTS can place the station on-hook.**

**(1) The CTS, by itself, can never place a station off-hook. A person operating the CTS, or with access to CTS software, can never initiate any action that will take a station off-hook. The CTS cannot hold a station off-hook when the user places the station on-hook.**

**(2) The on-hook condition of a subscriber station absolutely must be under the control of the user. The ability of a user to place a station set on-hook must never be dependent on the rest of the system or on any system response or any other activity in the system. In addition to a station user, the CTS can place a station on-hook.**

**The on-hook condition of any station must not be dependent on CTS programming.**

**The on-hook condition cannot be canceled by the CTS, nor by anyone with access to the station mounting cord wiring.**

**(3) The transition from off-hook to on-hook may be directed by the user or by the CTS. If directed by the user, it may not be inhibited by the CTS. The transition from on-hook to off-hook can be directed only by the user, but there is no prohibition against necessary supporting action by the CTS.**

**(4) A station may not be used if any internal microphonic element can be electrically connected to, or caused to transmit audio to,**

the mounting cord when it is on-hook.

b. Incoming calls to subscriber stations will always require manual answering. Annunciation is the only response a station is permitted to make to an incoming call. The following features of some subscriber equipment are prohibited:

- Voice-activated call answering.
- Automatic call answering by any means, including telephone answering machines or ADP terminals.
- "Hands-free" answering.

c. Any feature allowing remote or trunk line access to CTS services must be disabled. CTS services should be accessible only from subscriber stations or equipments.

d. Remote diagnostic, maintenance, or programming functions are prohibited except as specified in paragraph 4c.

#### **4. Management of the Computerized Telephone System**

As part of the ongoing management of the CTS, assurance is needed that the system will never be changed in a manner that could compromise its built-in security measures. Accordingly, some administrative procedures governing the management of the CTS are suggested in the following paragraphs. Elements of these procedures include:

- Physical security.
- Personnel security.
- Management of system configuration, hardware, software, and layout.
- Appropriate technical security countermeasures.

a. Access to station equipment, CTS components, wiring, and distribution frames within the PPS must be limited to personnel with appropriate security clearances. Uncleared maintenance and installation personnel may be used only if closely escorted by cleared, technically competent escorts who can ensure the system's security integrity.

b. The system software should be modified only from established maintenance stations located inside the PPS. Positive barriers must be established to prevent software modifications from originating anywhere else. Routine remote maintenance or diagnostics may be conducted only from cleared remote diagnostic support (RDS) facilities over secure communication links, except as specified in paragraphs 4c and 4d.

c. In an isolated instance, if a remote maintenance procedure over an unsecured communication link is necessary, it may be provided by an uncleared RDS facility with the following restrictions:

(1) The RDS facility must not be able to access the CTS except through a port dedicated to infrequent RDS activity.

(2) Unless in use, the RDS port must remain disconnected from all trunks and lines leaving the PPS. If ancillary equipment such as modems or telephones are necessary for connection, they must be completely disconnected when not in use.

(3) Connection between the RDS port and the RDS facility must be established only by a call to the RDS facility that is initiated from a designated station inside the PPS.

d. Specific personnel must be designated to ensure the security of the RDS services. They must ensure all of the following for each RDS operation:

**(1) Verify the immediate need for RDS.**

**(2) Telephone the RDS facility and verify that the support activities can begin and the facility is ready to transmit.**

**(3) Make the necessary connections between the RDS port ancillary equipment, and outgoing trunks or lines.**

**(4) Dial the RDS facility to establish the RDS port connection, and verify with the facility that the connection was established.**

**(5) If the capability exists, monitor in real time (with hardcopy printout) all communications between the RDS facility and the CTS. Terminate the session immediately if any improper activity is noted.**

**(6) If real-time monitoring is not available, or not in an immediately comprehensible form, the following procedure must be accomplished as soon as RDS is terminated: reload the system from the safeguarded master program copy. If the program medium is nonremovable, read the complete memory listing and compare it to the safeguarded master copy. This may cause interruption of CTS service on some systems. If the RDS service cannot be scheduled to make such interruption operationally and administratively acceptable, the system must permit real-time monitoring.**

**(7) When RDS service is terminated, disconnect all connections needed for the RDS service.**

**e. System software or hardware may be changed only by designated, appropriately cleared individuals. Only these individuals are permitted physical access to the programming stations.**

**f. The integrity of the protective measures must be ensured by countermeasures inspections.**

**g. The operating program must be frequently reloaded from the protected master copy to ensure that no unauthorized changes have occurred. A log will be maintained that will indicate the person performing the action and the date and time at which the loading was accomplished.**

**h. Complete copies of all system documentation are to be kept with the CTS in the PPS. This documentation should include instructions, manuals service practices, system configuration records, maintenance records, etc.**

**i. Dial access or barrier codes are not adequate for denying unauthorized access to any CTS feature or control operation: they are unacceptable for this purpose.**

## **ADDITIONAL SECURITY CONSIDERATIONS**

### **Security Enhancements**

The following measures will help maximize the overall security of the CTS but are not expressly required to achieve on-hook audio security.

a. Positive barriers should be placed into the system to prevent access to features that would allow monitoring of station off-hook audio from outside the PPS. Examples include line or trunk verification, executive override, etc.

b. Central dictation features should be disabled.

c. Central loudspeaker paging features should not be activated.

d. All operator consoles should be located within the PPS.

e. The number of central answering positions should be minimized.

f. Except for operator consoles, all stations should be single-line, 2500-type instruments.

g. The call detail recording information to support switching and auxiliary features should be maintained by the CTS only temporarily, unless positive barriers exist to prevent access to this information from outside the PPS.

h. The CTS should not maintain speed calling lists.

i. The CTS and all critical station equipment should be powered by uninterruptable power supplies.

j. The CTS should curtail service for facilities outside the PPS when required to provide priority service for internal communications.

k. All switching, maintenance, or operational conditions set up from a subscriber station should be capable of being selectively canceled at an operator console inside the PPS.

## **GLOSSARY**

### **CALL DETAIL RECORDING (CDR)**

A record maintained by the computerized telephone system (CTS), or auxiliary equipment of specified types of calls. Typically a CDR system will record the CTS identity, date, time, duration of call, called number, and trunk group type. Also called Station Message Detail Recording (SMDR).

### **CARD RACK**

A circuit card rack, card subrack, card cage, or shelf that is a mounting for computerized telephone system circuit cards. The card rack has edge connectors to receive the circuit cards and is equipped with all the wiring and hardware needed to house and interconnect the system circuit assemblies.

### **COMMON CONTROL CABINET**

A cabinet that contains equipment supporting more than one subnetwork of a CTS. See also: Module.

### **CTS (COMPUTERIZED TELEPHONE SYSTEM)**

A generic term used to describe any telephone system that uses centralized stored program computer technology to provide switched telephone networking features and services. CTSs are referred to commercially by such terms as computerized private branch exchange (CPBX), private branch exchange (PBX), private automatic branch exchange (PABX), electronic private automatic branch exchange (EABX), computerized branch exchange (CBX), computerized key telephone systems (CKTS), hybrid key systems, business communications systems, and office communications systems.

### **DISCONNECT**

A device that (1) inserts a break at some point in the normal hard-wire conduction path that exists between a telephone and its telecommunications medium, and (2) only when the telephone is in the in-use state, establishes a temporary metallic connection across that break.

### **EXTERNAL FRAME**

A wiring frame used to support wiring leaving the PPS.

### **EXTERNAL SERVICE FRAME**

An intermediate frame used to terminate the computerized telephone system (CTS) cabling for stations located outside the physically protected space (PPS) and to terminate wiring associated with non-CTS services leaving the PPS.

## **FRAME (OR WIRING FRAME OR CROSS-CONNECT FRAME)**

A clearly defined point of interconnection between physically separated components of the system. Wiring frames consist of an array of terminal blocks serving to organize the system interconnections that are typically unique to an individual installation. For example, connections between the central office trunks and the computerized telephone system (CTS) switching network; or between telephone sets and the CTS switching network. The types of terminal blocks used are usually some variation of the common 66-type blocks. See also: External Frames, External Service Frames, and Internal Frames.

## **HANDS-FREE ANSWERING**

A feature available on some telephones and telephone systems that, when certain types of incoming calls occur, either automatically places the telephone in the in-use state or allows the user, without any manual action, to initiate the in-use state by means of a voice-activated switch

## **INTERNAL FRAME**

A wiring frame used to support wiring to computerized telephone system equipment and stations inside the physically protected space.

## **ISOLATOR**

A device or assembly of devices that has been accepted by TSG as a means to isolate a computerized telephone system or on-hook station from wires that exit the physically protected space. An isolator never establishes a metallic electrical path between the protected equipment and any external wiring.

## **LINE**

The wires or other transmission media that connect the station equipment to the computerized telephone system. The uncontrolled communication circuits of the commercial network.

## **MICROPHONIC**

Any component, regardless of its intended functions, that exhibits transducer behavior to produce an electrical analogue output from an audio-frequency sound pressure waveform input is termed microphonic.

## **MODULE**

The cabinet or cabinets that contain the complete switching equipment for a subnetwork of the computerized telephone system (CTS). Some CTSs divide the internal telephone network into separate subnetworks organized around switching node points. Calls between subnetworks are carried by intermodule links or through a switching node hierarchy. Control of the subnetworks may be accomplished by processors resident in the modules or from a central, common control processor. Any cabinet that contains equipment in support of more than one subnetwork is designated a common control cabinet and not a module cabinet.

## **NETWORK, SUBNETWORK**

A system of individual stations arranged so that any station can communicate with any other station (subject to service constraints imposed on it that are not inherent to the system) by means of temporary connections at central switching nodes.

## **OFF-HOOK**

A station or trunk is off-hook when it initiates or engages in communications with the computerized telephone system (CTS) or with

another station or trunk using a link established through the CTS.

#### **ON-HOOK**

A station or trunk is on-hook when it is not being actively used in communications via the computerized telephone system.

#### **PORT CIRCUIT**

An input/output interface circuit in the computerized telephone system (CTS) that connects the CTS to the communications link or a station or trunk.

#### **PHYSICALLY PROTECTED SPACE (PPS)**

A space inside one physically protected perimeter. Separate areas of equal protection may be considered part of the same PPS if the communication links between them are provided sufficient physical protection.

#### **PSTN (PUBLIC SWITCHED TELEPHONE NETWORK)**

The ordinary dial-up telephone system.

#### **REMOTE ACCESS TO CTS SERVICES**

A computerized telephone system (CTS) feature that allows incoming callers to access the CTS as if they were calling from a CTS station.

#### **REMOTE DIAGNOSTIC SUPPORT (RDS)**

Off-premises diagnostic, maintenance, and programming functions performed on the computerized telephone system via external network trunk connections. There is no universal term in use throughout the telephone industry to designate this feature. Manufacturers refer to it by various descriptive names (such as RMATS and INADS), names unique to particular systems.

#### **STATION MESSAGE DETAIL RECORDING (SMDR)**

Same as Call Detail Recording.

#### **STATION MOUNTING CORD**

A flexible assembly of individually insulated electrical wires enclosed in a common insulating jacket and fitted with terminating connectors; used to provide the electrical connections between the main body of the telephone and the blocks or jacks that terminate the house cabling.

#### **STATION- STATION EQUIPMENT, STATION SET, SUBSCRIBER STATION**

Any telephone, voice terminal console, data terminal, or other component of the network that is connected to a communications port of the computerized telephone system (CTS) and is used to communicate with another station or trunk by means of a temporary connection switched by the CTS

#### **TRUNK**

Any connection from an external network to a communications port of the computerized telephone system (CTS) that can be accessed by station equipment via the CTS switched network. Central office access to the public switched network, private lines, tie lines to another CTS, etc., are examples of trunks.

**TYPE-ACCEPTED TELEPHONE**

Any telephone, specified by manufacturer and model number, that has been evaluated and approved by TSG and given a TSG type-acceptance number. Type accepted telephones incorporate features of design and construction that conform to the criteria stipulated in TSG Standard 3 or 4.

**UNCONTROLLED/UNPROTECTED LINE  
UNCONTROLLED/UNPROTECTED TELECOMMUNICATIONS MEDIUM**

A telecommunications medium, such as a telephone wireline, that is not provided continuous positive physical protection against unauthorized, clandestine intercept of the information it is being used to convey.

**VOICE TERMINAL**

A station or station set that carries voice telecommunication when in operational use.