NTSWG GUIDELINES FOR COMPUTERIZED
TELEPHONE SYSTEMS (CTS)
Supplemental

NTSWG STANDARD 2(a)

March 2001

PREFACE

The Telephone Security Group Standards were initially written back in the early 1980's to prescribe the measures necessary to protect audio discussion against eavesdropping and component manipulation, which permitted eavesdropping of classified discussion. The TSG no longer exists; rather, it has been re-organized and re-chartered as the National Telecommunications Security Working Group (NTSWG). As such, the NTSWG is responsible for security countermeasures for all telecommunications systems and components used within a classified [information] processing area. An adjunct of the old countermeasures program was the development of inherently safe telecommunications systems and devices, which has since fallen dormant in the waning years of the TSG. However, the NTSWG is actively seeking industry participation in that program by clarifying and reducing the previous "overly-restrictive" requirements. This document is dedicated to re-defining the minimum-security requirements for small CTS's such that it will hopefully stimulate industry interest in providing inherently safe telecommunications that can be directly applied to national protection requirements.

All manufacturers, which produce commercial-of-the-shelf (COTS) CTS's, that conform to the requirements contained within this standard are invited to submit their product for NTSWG evaluation and subsequent Type-Acceptance. Which, in turn, will permit the product to be installed, maintained, and managed within US government spaces as a qualified product, affording the necessary protective measures required by government security directives.

TSG Standard 1 is an introduction to telephone security that provides general information about the TSG standards. TSG Standard 2 prescribes the general requirements for planning, installing, maintaining, and managing a computerized telephone system (CTS), which is primarily used by cognizant security authorities for the evaluation and acceptance of CTS' within their physically protected spaces. This standard, NTSWG Standard 2(a), specifically applies to manufacturers of "small" CTSs who provide COTS systems with 30 or fewer stations. Larger systems will be considered, but only on the merits of meeting the minimum requirements contained herein.

NTSWG STANDARDS FOR
COMPUTERIZED TELEPHONE SYSTEMS SUPPLEMENTAL

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 "small" computerized telephone switches 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 connected telephones be achieved in the CTS itself.

APPLICABILITY

This standard applies to all original equipment manufacturers (OEM) that build and install "small" computerized telephone systems. A small system is one that generally supports fewer than 30 (thirty) stations, and does not contain most of the features and remote functionality of their larger counterparts. Systems greater than 30 stations may be submitted for Type-acceptance, but must conform to the minimum requirements stated below.

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.

MINIMUM SYSTEM REQUIREMENTS

1. Physical Requirements

The system must be small enough to be completely installed in a confined space of no more than 160 square feet (the average size of a telecommunications closet), without special environmental controls (power, HVAC, etc.). This closet and the area where the telephones are situated will be known as the physically protected space (PPS).

2. Power Requirements

The system must be able to utilize a standard wall outlet, providing 120VAC, 60-hertz power, (for domestic use), or conforming to international power standards for foreign use. The system must be capable of sustained operation during power failures, such that one station will function as an emergency call-out phone, and system programming will be sustained for more than 72 hours before reprogramming will be necessary.

3. Operational 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 guidelines

- The wiring frames will be situated to facilitate their electrical testing and visual inspection.
- A means must be provided to electrically inspect all transmission paths (trunk lines) leaving the PPS for the presence of audio.
- Internal frames may be used to terminate connections from the CTS to PPS equipment and stations; likewise, station ports that are an integral part of the CTS cabinet are acceptable.
- An external frame must be used to terminate and cross-connect all trunk lines providing service to the CTS. Thus, cross-connect terminations from the external frame to the CTS that are an integral part of the CTS cabinet or back plane are acceptable.
- Subscriber stations of the CTS must be wired only to station port circuits.
- Trunk lines providing service to the CTS must only be terminated to trunk port circuits.
- Additional telecommunications circuits (DSL, ISP, or alarm system services) that are not switched by the CTS must be terminated on a separate and distinct external frame.

The signal isolation between non-communicating port circuits (both trunk and station) 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 time-division multiplex bus is permitted only when the associated station or trunk is off-hook and intended for use. Fundamentally, only a virtual circuit may exist between all internal stations and external trunk lines. Actual circuit paths may only exist when the CTS switching fabric acknowledges a demand for service (i.e., an in-coming call or a user's desire to place an out-bound call) can a trunk be electrically connected to an internal station. During all other time the separation must be -70db or greater.

4. System Configuration Requirements

The wide range of CTS features have been a constant concern of the TSG and now the NTSWG. While many CTS features represent new and enabling technologies, and beneficial attributes, they do not necessarily ensure adequate protection against audio eavesdropping. For example, hands-free automatic answering of calls could permit an unattended phone to go "off-hook" whereby nearby conversations could be listened to or recorded. This feature represents a significant concern to the NTSWG. Likewise, any other hospitality feature, which provides "like" functionality would be a concern. Another feature (of many CTS') that raise security concerns are remote activation of features and remote programming.

To counter these concerns, the NTSWG is asking for assurance from manufacturers that these features can be removed during production, are de-programmable during set-up and initialization, or otherwise protected through adjunct security modifications. Our "best case" would be that remote programming not exist without the addition of a modem or adjunct device, which must be purchased as an option.

We recognize that the remote programming feature is an operational requirement for some CTS subscribers and provisions must exist to accommodate those situations. In those instances, the subscriber must be provided a means to add port security measures or some method to ensure that remote programming is only accessed by authorized users (i.e., a DES encrypted modem, remote port security device, etc.). 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.

5. System Programming Requirements

- CTS programming must include the ability for the owner to change any and all factory default passwords.
- System programming may be accomplished through the use of a "feature set," systems administration terminal, a station connected to the programming port (station #10) or through any connected station so long as that station is directly wired to the CTS controller and it is physically located within the PPS.
- CTS's which contain the ability to back-up or store programming onto magnetic media must be configured such that a media lock can be affixed to it (to prevent casual access/use) when not in use.

6. CTS Operational 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. Such as:

- The off-hook condition of a subscriber station must be initiated by the user at the station. However, CTS programming may place an off-hook station out-of-service or on-hook if left unattended.

- 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.

- The on-hook condition of a subscriber station 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.

- CTS operation must provide for a hold or mute feature that will shunt audio from the handset when activated.

- The on-hook condition cannot be canceled by the CTS, or by anyone with access to the station mounting cord wiring.

- 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 the handset is on-hook or in the cradle.

- Speakerphone instruments may be used so long as they can be administratively disabled via CTS programming (thereby limiting the use of two-way audio from the phone when administered). One-way speakerphones are permitted so long as the "one-way" is to permit the placing of a call, but will not allow the transmission of audio without lifting the handset.

- 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.

7. 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 (subsequent revisions/versions of the software load must not diminish the requirements of this document).

- Accordingly, the CTS should not require any special provisions or management beyond that of normal daily use.

- Custom features, not addressed herein, may be permitted so long as they do not impact the audio protection requirements stated above.

- Likewise, custom security features are permitted so long as they are clearly defined in the administration phase of CTS installation and initialization, and so long as they are not substitutes for the fundamental security requirements contained in this document.

ADDITIONAL SYSTEM CONSIDERATIONS

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

- 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.

- Central dictation features should be disabled.

- Central loudspeaker paging features should be de-activated.

- All operator consoles should be located within the PPS.

- The number of central answering positions should be minimized.

- 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.

NTSWG TYPE-ACCEPTANCE PROGRAM

A viable and important approach for telephone security, which has long been employed by the US Government, is the concept of the *type-accepted telephones.* This is a telephone instrument or system of telephones, which by virtue of its design and construction (and documented laboratory audio test results) have proven that they do not facilitate the loss of audio.

Type-acceptance Application Process

Manufacturers who produce small CTS, which meet or exceed the minimum security requirements contained within this standard, may submit a Type-acceptance request to the chairman of the NTSWG. The Type-acceptance package must contain a product description, a detailed description of how it meets or exceed the minimum requirements, and any other details pertaining to the product's intrinsic or inherently safe design, and therefore warrants type-acceptance status. The package may include any test data that supports the claim. Submissions may include sample system and proprietary documentation provided that they both may be disposed of by the NTWSG after Type-acceptance. Proprietary information will be properly safeguarded while in the control of the NTSWG, and disposed accordingly when no longer required.

Requirements on product stability

These are applied, for the most part, only to those components of the *type-accepted CTS* that are used to implement minimum-security requirements contained within this document. The manufacturer is largely free to change all non-related areas without affecting its type-acceptance

status. Manufacturers who wish to compete in this market can readily determine if their products are acceptable and, if not, what modifications may be necessary to make them acceptable. Also, the type-acceptance procedure generally defines what portions of the CTS can be subsequently altered by the manufacturer without affecting its type-accepted status. Changes of this sort can be made at the discretion of the manufacturer without involvement of the government.

Product submissions should contain sufficient technical detail to permit NTSWG engineers to ascertain how the system inherently provides protection, or to understand what technical modifications have been implemented to prevent against on-hook and off-hook audio exploitation. Mere advertising collaterals will not suffice, as they tend to market the product, but rarely address the technical merits of the system. Submissions that lack technical detail will be suspended from evaluation until the vendor can be notified and provided adequate time to respond or the product will be returned without testing. Complete submissions will be evaluated and resolved within 90 days from receipt, unless otherwise notified. Once Type-acceptance status is approved, the vendor will be required to submit (within 30 days) a notice of product availability, cost, and purchasing point of contact. This information will be used to produce a Type-acceptance listing to be placed in NTSWG Standard #6.

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 sub-rack, 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.

SMALL CTS (COMPUTERIZED TELEPHONE SYSTEM)

A generic term used to describe any small telephone system that uses centralized stored program computer technology to provide switched telephone networking features and services. Small CTSs are generally categorized by the NTSWG as those with 30 or fewer stations. 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. The term system is used to define the controller (CPU and card rack), back plane, terminal blocks and cross-connects, and associated administration terminals and telephone instruments. The NTSWG distinguishes small CTSs from large ones based on size, functionality, number of subscriber stations, and software features, as well as, the relative ease or difficulty [for a small subscriber] to administer and maintain their own 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; 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 either 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 of 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 allowing incoming callers access to 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 b~ 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 the station equipment can access 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-ACCEPTANCE PROGRAM

The NTSWG Type-Acceptance program is a holdover from the TSG days. The program is

directed at manufacturers to promote USG acceptance of commercially developed systems, which are inherently safe and require few, if any, modifications for use in sensitive discussion facilities. Products that are Type-Accepted are placed on a qualified product's list and can be purchased for direct implementation. Manufacturers of Type-Acceptance products are bound by their individual assurance statements that products conform to this [NTWSG #2(a)] will continue to perform as design, and that changes to the basic product will be submitted to the NTSWG for review and re-certification (if required).

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. Another name for a telephone set.