Committee on National Security Systems

NATIONAL

INFORMATION ASSURANCE (IA)

INSTRUCTION

FOR

COMPUTERIZED TELEPHONE

SYSTEMS

NATIONAL MANAGER

FOREWORD

1. The Committee on National Security Systems Instruction (CNSSI) No. 5002, "National Information Assurance (IA) Instruction for Computerized Telephone Systems," contains guidance for planning, installing, maintaining, and managing a computerized telephone system (CTS), while enabling an organization to achieve on-hook audio security of computerized telephones located in discussion areas (e.g., sensitive compartmented information facility(SCIF)) that need to be isolated from wires and media that extend beyond the perimeter of these areas. Implementation of this instruction does not preclude the application of more stringent requirements and may not satisfy the requirements of other security programs such as TEMPEST, COMSEC (Communications Security), or OPSEC (Operational Security).

2. This instruction is strictly intended for computerized telephone systems (CTS); use of Voice over Internet Protocol (VoIP) or hybrid systems based on IP or IP-related technologies must adhere to CNSS Instruction No. 5000, "Guidelines for Voice over Internet Protocol (VoIP) Computer Telephony," April 2007.

3. The National Telephone Security (NTS) Working Group (WG) is the primary technical and policy resource in the United States (U.S.) Intelligence Community (IC) for all aspects of the Technical Surveillance Countermeasures (TSCM) Program involving telephone systems located in areas where sensitive government information is discussed.

4. CNSS Instruction No. 5002 is effective on the date of signature.

5. Copies of this instruction may be obtained by contacting the Secretariat as noted below or via the website www.cnss.gov.

6. U.S. Government contractors and vendors shall contact their appropriate government agency or Contracting Officer Representative regarding distribution of this document.

FOR THE NATIONAL MANAGER

/s/
DEBORA A. PLUNKETT

NATIONAL INFORMATION ASSURANCE (IA) INSTRUCTION FOR COMPUTERIZED TELEPHONE SYSTEMS

SECTION I – PURPOSE

1.   This instruction sets forth the requirements for planning, installing, maintaining, and managing a computerized telephone system (CTS)[1], while enabling an organization to achieve on-hook audio security of computerized telephones located in a sensitive compartmented information facility (SCIF) or in areas where sensitive information is discussed. Any CTS conforming to this instruction shall ensure all protected on-hook telephones are completely isolated from all transmission media and wires that are physically unprotected.

SECTION II – SCOPE

2.   The provisions of this instruction apply to telephone systems that rely on the CTS installation to isolate sensitive discussion areas from transmission media that extend beyond the perimeter of a facility's physically protected space (PPS). This instruction shall be referenced and included in U.S. Government-sponsored procurement specifications for all CTS installations intended to be CNSSI 5002 compliant.

3.   This instruction is strictly intended for CTS; use of Voice over Internet Protocol (VoIP) or hybrid systems based on IP or IP-related technologies must adhere to Reference l, CNSS Instruction No. 5000, "Guidelines for Voice over Internet Protocol (VoIP) Computer Telephony," April 2007.

SECTION III –APPLICABILITY

4.   This instruction applies only to telephone systems in which the CTS hardware, system wiring, and stations requiring isolation are located within a PPS. The CTS cannot ensure isolation between uncontrolled, incoming lines and stations located outside the PPS. If on-hook audio security is required, telephones outside the PPS must be either type-accepted under Telephone Security Group (TSG) Standard 3 or 4, references h and i,

---

[1] A computerized telephone system or CTS does not include guidance for Internet Protocol (IP) or IP-related technologies.

or must be protected by an approved isolator or disconnect device in conformance with CNSSI No. 5006, reference k.

SECTION IV – REFERENCES

5. References are listed in ANNEX A.

SECTION V – DEFINITIONS

6. Definitions in CNSSI No. 4009, Reference e, apply to this policy; additional policy-specific terms are defined in ANNEX B.

SECTION VI – SYSTEM REQUIREMENTS

7. The requirements set forth, herein, are critical to organizations in the planning, installing, maintaining, and managing of the CTS that rely on the Private Branch Exchange (PBX) installation to isolate sensitive discussion areas from wires and media that extend beyond the perimeter of the facility's physically protected space. CNSSI 5002 cannot be partially implemented. If a CTS installation cannot meet the requirements established by CNSSI 5002, then another approved protection method must be used in areas where on-hook audio security is required. A CNSS Instruction No. 5002 CTS installation will consist of the following minimum system requirements (derived from references a through d and f through n):

A. **MINIMUM SYSTEM REQUIREMENTS**

(1) **Physical Security Requirements:** 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. The PPS containing the CTS must have the same level of protection as the highest level of PPS containing the stations it services.

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

b. All program media, including Federal Information Processing Standards (FIPS) compliant removable media, (e.g., CD, Flash Memory, Thumb Drive, DVD, Tape…) must be under positive physical security and possess a write-protection mechanism to prevent unauthorized alterations. All hardware storing sensitive information will be disposed of securely when no longer in use.

c. Up-to-date master and backup copies of the operating program must be maintained for confirmation and/or reloading. 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. Additionally, an organization may desire to maintain an up-to-date hard copy (print out) of the operating program.

d. Conduit and associated fittings between non-contiguous PPS shall prevent direct contact with the wiring. Any attempt to compromise the integrity of the conduit shall be readily identifiable.

(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 physically access, inspect, and electronically test all transmission paths leaving the PPS for the presence of audio or data transmissions.

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

i. The External Frame No. 1 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.

ii. The External Frame No. 2 must terminate all the wiring leaving the PPS. The termination point of incoming central office trunks, referred to as a demarcation point, normally incorporates Universal Service Order Codes RJ21 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 External Frame No. 2.

iii. 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 service inside the PPS require wiring connections outside the PPS then this wiring will terminate at the External Service Frame and be cross connected to the second external frame.

iv. Cross connects between the External Frames No. 1 and No. 2 will be by separate single pair wires. No extra cross

connects will be permitted beyond the minimum number required to provide the needed service.

    v. External frames will be physically separated by at least 6 inches from each other and by 12 inches from 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 exclusively used to terminate all connections from the CTS to PPS equipment and stations. There must not be any cross connects between internal and external frames (note figure page 6). A waiver must be in writing, posted, and maintained in the wireroom, since the PPS may be a SCIF, any waiver affecting a SCIF will affect its reciprocal use.

d. Cables from internal and external frames must not be terminated in the same card rack. No two (2) card racks may share common cabling to the wiring frames. Any waiver requires documentation and approval by the departments or agencies designated security authority or equivalent.

e. Subscriber stations of the CTS and trunk lines must be wired only to CTS port circuits. The signal isolation between non-communicating port circuits must exceed 70 decibels. 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. If telephones inside/outside of the PPS share the same directory, then the telephone inside the PPS must have voice privacy enabled.

g. The system must be capable of generating a complete memory listing of the program, for comparison with the master program, where removable programming media are not used, and when CTS programming is stored electronically inside CTS.

(3) **Operational Characteristics**: Some CTS have operational features that are inconsistent with good audio security practices. These features can cause the CTS to execute electronic functions that are expressly prohibited. These prohibited functions can compromise the isolation that must be provided by the CTS. When an operational feature of the CTS uses a prohibited function, the feature must be positively disabled in hardware. The following paragraphs define required and prohibited characteristics of the CTS:

PHYSICALLY PROTECTED SPACE (PPS)
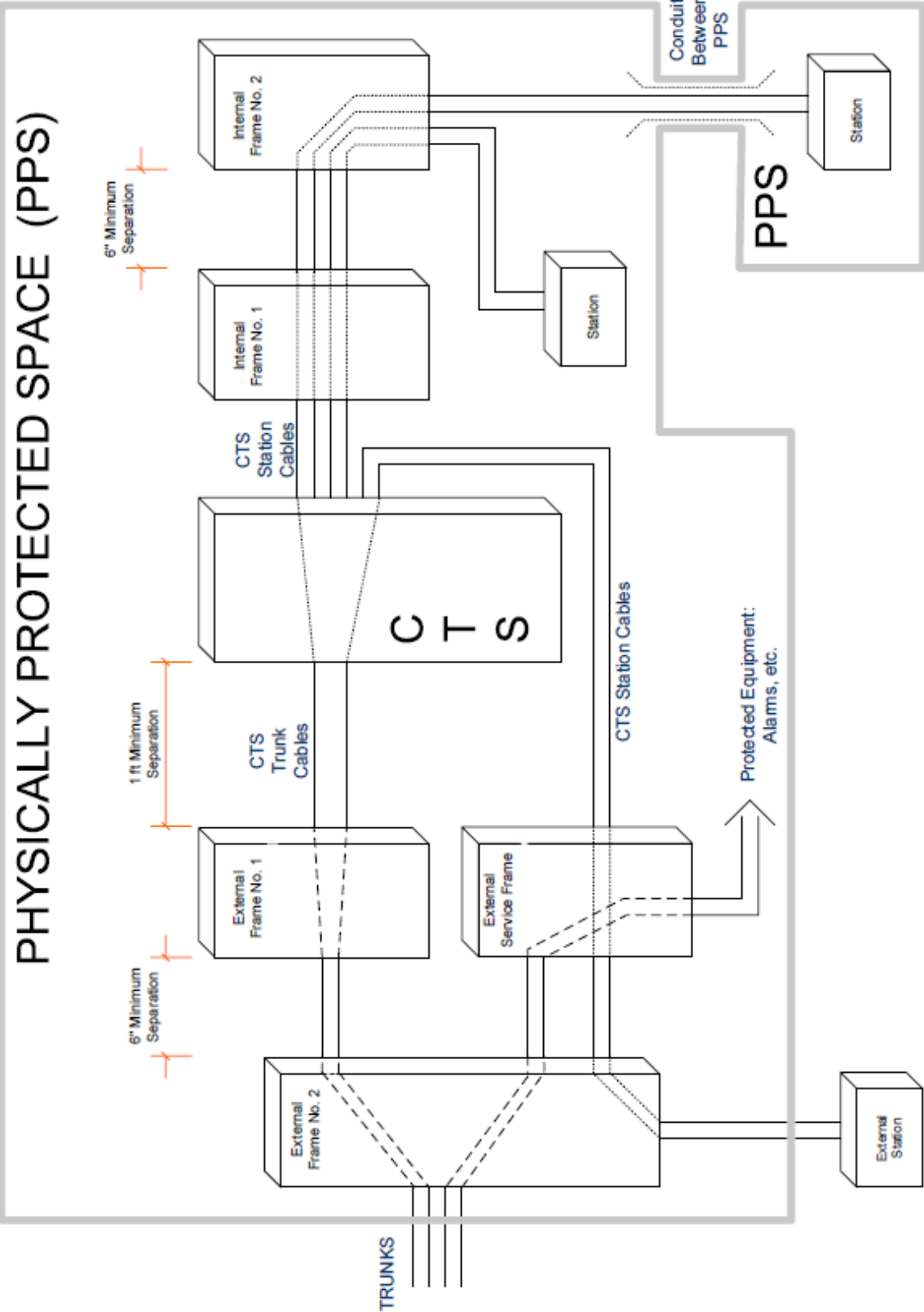
a. The off-hook condition of a subscriber station must be initiated by the user at the station. However, the CTS can place the station on-hook.

    i. The CTS can never possess the capability, nor can its software be programmed to place a station in an off-hook state. Neither the operator of the CTS nor an individual with access to CTS software can use the CTS or CTS software to take a station off-hook. The CTS cannot hold a station off-hook when the user places the station on-hook.

    ii. 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 activity in the system. However, 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, nor can the on hook condition be canceled by the CTS or by user with access to the station mounting cord wiring.

    iii. 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; however, there is no prohibition against supporting action by the CTS.

    iv. A station may not be used if any internal microphone element can be electrically connected to, or caused to transmit audio to, the mounting cord when it is on hook.

    v. A station may not be used if the CTS software can change the instrument to an off-hook condition. Authorized stations include analog instruments, instruments with push-to-talk handsets or any instrument that precludes external control of internal microphones or the on-hook condition. Caution: Internal microphones and the on-hook condition of these instruments have the ability to be controlled by CTS software.

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. Any automated method of creating an off-hook condition is prohibited on subscriber equipment; to include, voice activated features and hands free answering.

c. Any unauthenticated feature allowing remote or trunk line access to CTS services must be disabled. CTS services should be accessible

only from subscriber stations or equipment.

    d. Remote diagnostic, maintenance, or programming functions are prohibited except as specified in paragraph 8.A.(4).d.iii.

(4) **Management of the CTS:** 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, administrative procedures governing the management of the CTS are provided below.

    a. Elements of these procedures include:

        i. Physical security

        ii. Personnel security

        iii. Management of system configuration, hardware, software, and layout

        iv. Appropriate technical security countermeasures

    b. Access to station equipment, CTS components, wiring, and distribution frames within the PPS must be limited to personnel with appropriate security clearances and uncleared maintenance and installation personnel, who are closely accompanied by cleared, technically competent escorts who will ensure the system's security integrity. During a CTS installation and after any major system change, a risk assessment should be performed in order to determine if additional countermeasures are needed.

    c. End-to-end encryption must be enabled to protect sensitive data in transit. Appropriate key management procedures must be implemented. End user processes should be in place to protect encryption cards when not in use.

    d. Unique user accounts will be in place and used for all system access. 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 paragraph 8.A.(4).e.iii.

    e. In emergency situations and when vital to operations, a remote maintenance procedure over an unsecured communications link may be provided by an uncleared RDS facility with the following restrictions:

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

ii. 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, is necessary for connection it must be completely disconnected when not in use.

iii. 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.

iv. One-time password and/or a two-factor authentication log-in/access method shall be used to ensure user account verification, a higher level of assurance, and reduce possible system compromise.

f. Specific personnel must be designated to ensure the security of the RDS services and are responsible for ensuring all of the below items for RDS operation:

i. Verify the immediate need for RDS.

ii. Telephone the RDS facility, verify that the support activities are available, and the facility is ready to transmit.

iii. Make the necessary connections between the RDS port ancillary equipment and outgoing trunks or lines.

iv. Dial the RDS facility to establish the RDS port connection and verify with the facility that the connection was established.

v. 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.

vi. If real-time monitoring is not available, or not in an immediately comprehensible form, the following procedure must be accomplished as soon as the RDS is terminated:

1. Reload the system from the safeguarded master program copy.

2. If the program medium is non-removable, read the complete memory listing and compare it to the safeguarded master copy. This may cause interruption of CTS service on some systems.

3. If the RDS service cannot be scheduled to make such interruption operationally and administratively acceptable, the system must permit real-time monitoring.

vii. When the RDS service is terminated; disconnect all connections needed for the RDS service.

g. System software or hardware will be changed by designated and properly cleared individuals with the appropriate administrative privileges, who will be permitted sole physical access to the programming stations. The System Audit Log will be enabled during installation or programs changes; audit logs will be stored as cited in paragraph 8.B.(1).g. The CTS will log critical system functions and activity which will be reviewed on a periodic basis. To control access, default system passwords will be changed and new passwords will be secured and controlled by personnel responsible for maintaining the CTS in accordance with the Intelligence Community Standard Number 500-16, "Password Management," 16 March 2011.

h. The integrity of all protective measures must be ensured by countermeasures inspections at least annually or after major system changes.

i. The operating program must be verified, at least annually, or in conjunction with routine inspections. If it is determined an unauthorized change has occurred and a reload of the operating program is required, then it must be reloaded from the protected master copy. A backup of the system should be performed to ensure the reloaded software logs will be retained to indicate the person performing the action and the date and time when the loading was accomplished.

j. Complete copies of all system documentation are to be kept with the CTS in the PPS. Documentation includes, but is not limited to, instructions; manuals; service practices; logs; system configuration records; and maintenance records.

k. Dial access or barrier codes are not adequate for denying unauthorized access to any CTS feature or control operation and are unacceptable for this purpose.

l. The manufacturer's default password(s) will be removed and replaced with password(s) meeting department or agency standards for network access.

B. **ADDITIONAL SECURITY CONSIDERATIONS**

    (1) **Security Enhancements**. The following measures will assist organizations to maximize the overall security of the CTS and to achieve on-hook audio security. All unnecessary features will be disabled.

        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. A couple of examples include, line or trunk verification and executive override.

        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 or have all programming functions disabled.

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

        f. Capture and store call detail recording information off of the CTS to prevent access from unauthorized users.

        g. Capture and store system audit logs and audit trail off-line for review by authorized security personnel.

        h. Speed calling lists introduce OPSEC vulnerabilities and, thus, usage should be avoided.

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

        j. It is recommended that CNSS-approved instruments be used in classified discussion areas for added security and to further ensure on-hook audio protection.

SECTION VII – RESPONSIBILITIES

8. Heads of Federal Departments and Agencies shall:

    A. Develop, fund, implement, and manage programs necessary to ensure that the goals of this policy are achieved and that plans, programs, and CNSS issuances that implement this policy are fully supported.

    B. Incorporate the content of this policy into annual education, training, and/or awareness programs for individuals that plan, install, maintain, and manage the CTS.

C. Appoint a technically competent individual to document and approve, on their behalf, any deviation from this instruction. Deviations from the specified security measures mandated by this instruction should substitute compensating positive security measures to remedy the specific security deficiencies created by the omission(s).

Encl:
ANNEX A   References
ANNEX B   Definitions
ANNEX C   List of Acronyms

ANNEX A

REFERENCES

a. Code of Federal Regulations, Title 32 - National Defense, Volume 6, "Part 2004 – Directive on Safeguarding Classified National Security Information," Revised July 2003.

b. Director of Central Intelligence Directive (DCID) No. 6/2, "Technical Surveillance Countermeasures," March 1999.

c. Security Policy Board Issuance 6-97, "National Policy on Technical Surveillance Countermeasures," September 1997.

d. National Institute for Standards and Technology (NIST), Federal Information Processing Standards (FIPS) Publication 140-2, "Security Requirements for Cryptographic Modules," 25 May 2001.

e. CNSS Instruction No. 4009, "National Information Assurance (IA) Glossary," Revised May 2010.

f. Telephone Security Group (TSG) Standard 1, "Introduction to Telephone Security," March 1990.

g. Telephone Security Group (TSG) Standard 2, "TSG Guidelines for Computerized Telephone Systems," Revised September 1993.

h. Telephone Security Group (TSG) Standard 3, "Type-Acceptance Program for Telephones Used with the Conventional Central Office Interface," March 1990

i. Telephone Security Group (TSG) Standard 4, "Type-Acceptance Program for Electronic Telephones Used in Computerized Telephone Systems," March 1990

j. Telephone Security Group (TSG) Standard 5, "On-Hook Telephone Audio Security Performance Specifications," March 1990.

k. CNSS Instruction No. 5006, "National Instruction for Approved Telephone Equipment," September 2011.

l. CNSS Instructions No. 5000, "Guidelines for Voice over Internet Protocol (VoIP) Computer Telephony," April 2007

m. CNSS Instructions No. 5001, "Type Acceptance Program for Voice over Internet Protocol (VoIP) Telephones, December 2007.

        n.   Intelligence Community Standard Number 500-16, "Password Management," 16 March 2011.

ANNEX B

DEFINITIONS

Terms used in this policy are defined in Reference e., with the exception of the following, although some additional terms are defined in References f and g.

a. 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 referred to as a Station Message Detail Recording (SMDR).

b. 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.

c. Common Control Cabinet: A cabinet that contains equipment supporting more than one sub-network of CTS. See also: Module.

d. Computerized Telephone System (CTS): 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.

e. 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 or (2) establishes a temporary metallic connection across the break only when the telephone is in the "in use" state.

f. External Frame: A wiring frame used to support wiring leaving the physically protected space (PPS).

g. External Service Frame: An intermediate frame used to terminate the CTS cabling for stations located outside the PPS and to terminate wiring associated with non-CTS services leaving the PPS.

h. 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 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.

i. 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.

j. Internal Frame: A wiring frame used to support wiring to CTS equipment and stations inside the physically protected space.

k. 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.

l. 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.

m. 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.

n. Module: The cabinet(s) that contain the complete switching equipment for a sub-network of the CTS. Some CTSs divide the internal telephone network into separate sub-networks organized around switching node points. Calls between sub-networks are carried by intermodule links or through a switching node hierarchy. Control of the sub-networks 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 sub-network is designated a common control cabinet and not a module cabinet.

o. Network Sub-Network: 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.

p. Off-Hook: A station or trunk is off-hook when it initiates or engages in communications with the CTS or with another station or trunk using a link established through the CTS.

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

r. Port Circuit: An input/output interface circuit in the CTS that connects the CTS to the communications link or a station or trunk.

s. 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.

t. Public Switched Telephone Network (PSTN): The ordinary dial-up telephone system.

u. Remote Access to CTS Services: A feature that permits incoming callers to access the CTS as if they were calling from a CTS station.

v. Remote Diagnostic Support (RDS): Off premises diagnostic, maintenance, and programming functions that are performed on the CTS via an external network trunk connection. No universal term is available for use throughout the telephone industry to designate this feature. Manufacturers refer to this feature by various descriptive names (e.g., RMATS and INADS are names unique to a particular systems).

w. Station Message Detail Recording (SMDR): Same as Call Detail Recording.

x. Station Mounting Cord: A flexible assembly of individually insulated electrical wires enclosed in a common insulating jacket and fitted with terminating connector that are used to provide the electrical connections between the main body of the telephone and the blocks or jacks that terminate the house cabling.

y. 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 CTS and is used to communicate with another station or trunk by means of a temporary connection switched by the CTS.

z. Trunk: Any connection from an external network to a communications port of the CTS that can be accessed by station equipment via the CTS switched network; examples of trunks are, central office access to the public switched network, private lines, tie lines to another CTS et cetra..

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

bb. Uncontrolled/Unprotected Line and/or Telecommunications Medium: A telecommunications medium such as a telephone wire-line that is not provided continuous positive physical protection against unauthorized or clandestine intercept of the information as it is being used to convey.

cc. Voice Terminal: A station or station set that carries voice telecommunication when in operational use.

ANNEX C

LIST OF ACRONYMS

ADP	Automated Data Processing
BCS	Business Communications Systems
CBX	Computerized Branch Exchange
CDR	Call Detail Recording
CPBX	Computerized Private Branch Exchange
CKTS	Computerized Key Telephone System
CTS	Computerized Telephone Systems
DCID	Directive of Central Intelligence Directive
EPABX	Electronic Private Automatic Branch Exchange
FIPS	Federal Information Processing Standards
HKS	Hybrid Key Systems
IA	Information Assurance
LAN	Local Area Network
NIST	National Institute for Standards and Technology
NSA	National Security Agency
NSI	National Security Information
NSS	National Security Systems
NTS	National Telephone Security
NTSWG	National Telephone Security Working Group
OCS	Office Communications Systems
PABX	Private Automatic Branch Exchange
PBX	Private Branch Exchange
PPS	Physically Protected Spaces
PSTN	Public Switched Telephone Network
RDS	Remote Diagnostic Support
SCIF	Sensitive Compartmented Information Facility
SMDR	Station Message Detail Recording
TSCM	Technical Surveillance Countermeasures
TSG	Telephone Security Group
VoIP	Voice over Internet Protocol