

|||
NSTISS
NATIONAL
SECURITY
TELECOMMUNICATIONS
AND
INFORMATION
SYSTEMS
SECURITY

NSTISSI No.7003
13 December 1996

PROTECTIVE DISTRIBUTION SYSTEMS
(PDS)

**THIS DOCUMENT PROVIDES MINIMUM STANDARDS, FURTHER
IMPLEMENTATION MAY BE REQUIRED BY YOUR DEPARTMENT OR AGENCY**

NSTISS

NATIONAL MANAGER

NATIONAL SECURITY
TELECOMMUNICATIONS
AND INFORMATION
SYSTEMS
SECURITY

FORWARD

1. National Security Telecommunications and Information Systems Security Instruction (NSTISSI) No. 7003, Protective Distribution Systems (PDS), provides guidance for the protection of wireline and optical fiber PDS to transmit unencrypted classified National Security Information (NSI). This instruction is effective upon receipt, and supersedes NACSI No. 4009, Protected Distribution Systems, dated 30 December 19981 and Appendix K, NACSEM 5203, Guidelines for facility Design and RED/BLACK Installation, dated 30 June 1982. Please check with your agency for applicable implementing documents.

2. The major differences between this revision and the previous version are the identification of installation and physical security practices clarification of certain exempted applications from the approval process, the inclusion of government contractors in the scope of this publication, and the inclusion of detailed installation requirements.

3. Additional copies of this instruction may be obtained from:

NSTISSC SECRETARIAT
ATTN: V503 STE 6716
NATIONAL SECURITY AGENCY
FORT GEORGE G. MEADE, MD 20755-6716

SIGNED

KENNETH A. MINIHAN
Lieutenant General, USAF

PROTECTED DISTRIBUTION SYSTEMS (PDS)

SECTION

REFERENCES.....	I
PURPOSE.....	II
SCOPE III	
GENERAL.....	IV
SYSTEM APPROVAL.....	V

SECTION I - REFERENCES

1. The following references are applicable to the installation and use of PDS:
 - a. Department of State Composite Threat List, distributed periodically
 - b. NSTISSI No. 4009, National Information Systems Security (INFOSEC) Glossary, dated 5 June 1992
 - c. NSTISSI No. 7000, TEMPEST Countermeasures for Facilities, dated 29 November 1993
 - d. NSTISSI No. 7001, NONSTOP Countermeasures, dated 15 June 1994
 - e. NSTISSAM TEMPEST/2-95, RED/BLACK Installation Guidance, dated 12 December 1995

SECTION II - PURPOSE

2. This instruction stipulates approval authority, standards, and guidance for the design, installation, and maintenance of Protected Distribution Systems (PDS). This instruction incorporates a philosophy of “risk management” in lieu of the “risk avoidance” philosophy employed in the previous document. Absent specific facts, unique to each facility, suggesting greater or lesser risks, these standards shall be applied. However, sensible risk management practice dictates each facility must be evaluated on its own risks and vulnerabilities based on factors such as location, physical security, environment, access controls, personnel security requirements, etc. The overall security afforded by PDS is the result of a layered approach incorporating various protection techniques. The emphasis is placed on “detection” of attempted penetration in lieu of “prevention” of penetration. Criteria called out are based on threat or risk analysis relative to the location of the PDS. This generally results in reduced requirements and cost savings during installation and maintenance of PDS. The decision as to what extent the guidance provided in ANNEX B is followed ultimately rests with the department or agency Approval Authority.

SECTION III -SCOPE

3. This instruction applies to U.S. Government departments and agencies and their contractors and vendors who use, or are contemplating the use of a PDS to protect the transmission of unencrypted classified National Security information (NSI). This instruction describes the requirements for PDS installed within the U.S. (including its territories and possessions) and within LOW and MEDIUM threat locations outside of the United States as described by reference a. The threat within the U.S. is low. The use of PDS within a HIGH or CRITICAL threat location (per reference a) is not recommended. If PDS are used in these locations, protection techniques are determined on a case-by-case basis by the Approval Authority (see ANNEX A).

4. The contents of this instruction should be made available to personnel involved in the planning, acquisition, installation, approval, and operation of communications systems (that process classified NSI) and PDS.

SECTION IV - GENERAL

5. PDS are used to transmit unencrypted classified NSI through an area of lesser classification or control. Inasmuch as the classified NSI is unencrypted, the PDS must provide adequate electrical, electromagnetic, and physical safeguards to deter exploitation. Since PDS can be penetrated, given the opportunity and adequate time, a philosophy of detection of attempted penetration is employed in this document. Careful consideration is given to the application before PDS is selected in preference to another INFOSEC system. There may be economic, technical, or operational factors making PDS necessary in comparison to other INFOSEC systems. Although proper design and installation of PDS are important, continued physical security integrity after installation is critical. The cost and operational impact of maintaining the security of the system should be assessed prior to acquisition and installation, since such costs can easily exceed the installation cost.

6. Incidents of tampering, penetration, or unauthorized interception must be reported immediately to the PDS Approving Authority for assessment, and local security authority for review and initiation of an investigation. Subject to law enforcement procedures, which take precedence, the PDS should not be used until the incident is assessed and its security status determined. If this is not practical, users of all PDS should be notified of the possible breach in security, and the use of the PDS should be limited to the greatest extent possible.

SECTION V - SYSTEM APPROVAL

7. The PDS should be installed in compliance with ANNEX B. For any given facility, physical and technical security safeguards for the PDS normally should not exceed the safeguards afforded to the physical space originating and processing the data carried by the PDS. However, protection controls pertinent to classification, geographical location, and types of areas through which the PDS are installed shall be evaluated and requirements applied by the Approval Authority on a case-by-case basis. The Approval Authority shall ensure the PDS are inspected prior to initial operation.

8. The heads of U.S. Government departments and agencies, or their designees, are authorized approval and recertification authority for the operation and modification of PDS. The Approval Authority for the contractor-operated PDS shall be the cognizant security office.

9. PDS approval is obtained from the Approval Authority prior to system installation, use, or modification. Prior to formal approval, the proposed PDS should be technically reviewed by the Approving Authority's technical representative to verify compliance with ANNEX B and, if appropriate, a Certified TEMPEST Technical Authority (CTTA) to determine the need for TEMPEST countermeasures in accordance with reference c. and d.

10. Requests for approval for PDS shall include the information required by ANNEX C. Requests for approval of a modification to existing PDS or for re-approval of PDS which have failed rectification may include only the items pertaining to the modification/recertification failure.

11. Temporary test configurations do not require formal approval if they: do not exceed one month duration; are confined within U.S. Government installations; and do not process higher than SECRET information. However, they must be approved by the responsible Designated Approval Authority (DAA).

12. Proposed PDS within the U.S. which do not process higher than CONFIDENTIAL information shall be approved by the responsible DAA. Technical review is required only when the proposed PDS are installed in existing PDS approved at a higher classification level.

13. Mobile systems employing inter-shelter cabling need not be re-approved for each relocation if the relocation provides security comparable to that of the original approval. Otherwise, new approval must be obtained.

14. Deactivation of approved PDS must be reported to the PDS Approving Authority.

Encls:

1. ANNEX A - DEFINITIONS
2. ANNEX B - INSTALLATION GUIDANCE
3. ANNEX C - APPROVAL REQUEST

ANNEX A

DEFINITIONS

Certain definitions contained in reference b. apply to this instruction. Some additional definitions are included to define terms not included in reference (b).

- a. Approval Authority. Department or Agency having Approval Authority for the for the installation and operation of the PDS.
- b. Controlled Access Area (CAA). The complete building or facility area under direct physical control within which unauthorized persons are denied unrestricted access and are either escorted by authorized persons or are under continuous physical or electronic surveillance.
- c. Designated Approval Authority (DAA). Official with the authority to formally assume responsibility for approving an Information System or network at an acceptable level of risk. Responsible for issuing an accreditation statement recording the decision to accept all security risks and countermeasures.
- d. Limited Controlled Area (LCA). The space surrounding a PDS within which exploitation is not considered likely or legal authority to identify or remove a potential exploitation exists.
- e. Protective Distribution Systems. Wireline or fiber-optic distribution systems used to transmit unencrypted classified NSI through an area of lesser classification or control.
- f. Special Category Information. See reference c. Definition is classified.
- g. Uncontrolled Access Area (UAA). The area external or internal to a facility over which no personnel access controls are or can be exercised.

ANNEX B

PROTECTED DISTRIBUTION SYSTEMS (PDS) INSTALLATION GUIDANCE

1. General. This annex provides criteria for installing Protected Distribution Systems (PDS). In order to use PDS for classified NSI, adequate installation procedures must be used to ensure the PDS do not compromise information. The guidance required varies based upon classification or type of data handled and type of area through which the PDS are installed. PDS carrying SECRET (S), TOP SECRET (TS), or special category information data should be submitted for approval or reviewed to the Approval Authority. A criteria matrix is provided in Table B-1, see page B-4 of this document, as a cross reference to specific installation procedures contained in this annex.

a. Installation and Maintenance of PDS as follows:

(1) PDS terminal equipment should be installed in a CAA;

(2) Whenever possible, PDS lines should not be installed concealed (e.g., behind walls and above ceilings) from view of personnel responsible for conducting the required line route inspections and continuous surveillance;

(3) Employees in a CAA should be made aware that PDS exist and any suspicious activity should be reported;

(4) A record should be maintained in accordance with the directions from the Approval Authority relative to all PDS events, e.g., inspections, results of patrols, alarm events, or employee reports;

(5) Personnel not having the appropriate security clearance and special category access, but requiring occasional, temporary access to PDS interconnecting lines area (e.g., safety and fire inspectors) should be monitored continuously by appropriately cleared and access indoctrinated personnel preventing compromise of the processed information or the security integrity of the PDS;

(6) Those PDS subject to periodic visual inspections (Table B-2, see page B-5 of this document) and technical inspections (Table B-3, see page B-6 of this document), should be assessed for signs of penetration, tampering, and any other anomaly causing a deterioration of protection safeguards. The person(s) formally appointed to accomplish the visual inspection should be trained sufficiently to recognize physical changes in PDS including attempts at penetration and tampering. The person selected to accomplish the technical system inspection should be sufficiently trained to recognize changes in the technical aspects of PDS, e.g., by-pass circuitry, attachment or removal of devices or components, inappropriate or suspicious signal levels, and mechanical, TEMPEST, and RED/BLACK integrity of the PDS; and

(7) PDS in a tactical environment should be located within the limits of the installation and command post, or in an area directly under the commander's physical control.

2. Emanation Security. The objective is to ensure the PDS complies with the TEMPEST requirements as determined by the CTTA in accordance with reference c, through e.

3. Physical Security. The objective is to deter unauthorized personnel from gaining access to the PDS without such access being discovered. Table B-1, see page B-4 of this document, specifies guidance for different areas of control by classification level.

4. Protected Distribution Systems. There are two categories of PDS:

a. Hardened Distribution Systems. These are afforded significant physical security protection and can be implemented by the use of the following three carriers:

(1) Hardened Carrier. The following applies:

(a) The data cables must be installed in a carrier;

(b) The carrier should be constructed of electrical metallic tubing (EMT), ferrous conduit or pipe, or rigid-sheet steel ducting, utilizing elbows, couplings, nipples, and connectors of the same material;

(c) All connectors should be permanently sealed completely around all surface (e.g., welding (continuous or track), compression, epoxy, fusion, etc.). If pull boxes are used, the pull-box covers should be sealed to the pull boxes around the mating surfaces after installation or the pull box covers must not have removable hinge pins and must be secured with a General Services Administration (GSA) approved changeable combination padlock. Boxes with prepunched knockouts may not be used;

(d) If the hardened carrier is buried, it should be a minimum of 1 meter below the surface and on the property owned or leased by the U.S. Government or the contractor having control of the PDS. Manholes should be secured with a GSA-approved changeable combination padlock. If GSA locks cannot be used, then a standard locking manhole cover and approved micro-switch alarms should be used. If the carrier is buried in an installation outside the U.S. in a MEDIUM threat location, it should be encased in approximately 20 cm (8 inches) of concrete or a concrete and steel container (of sufficient size to preclude surreptitious penetration in a period less than two hours as confirmed by laboratory tests). It may be appropriate for physical protection, not security, to encase PDS in concrete or bury the PDS with more depth than that required for security reasons; and

(e) Suspended systems between buildings should be elevated a minimum of 5 meters and only used if the property transverses is owned or leased by the U.S. Government or contractor having control of the PDS. PDS should be installed to provide unimpeded inspection and cleared of any obstruction or device which encroaches upon the system to facilitate tampering. The area containing PDS should be illuminated. The carrier should be inspected in accordance with the requirements of Table B-2, see page B-5 of this document.

(2) Alarmed Carrier. To use an Alarmed Carrier as a Hardened Distribution System, the carrier should be protected by an alarm system approved by the cognizant COMSEC and/or physical security authorities. A Standard Operating Procedure (SOP) approved by the base/facility security officer and commander, and the approval authority should be implemented to:

(a) Verify its performance at intervals as shown in Table B-4, see page B-6 of this document;

(b) Ensure response by security personnel in the area of possible attempted penetration, within 15 minutes of discovery;

(c) Provide for inspection of the PDS to determine the cause of the alarm;

(d) Define action to be taken regarding the termination of transmission;

(e) Initiate investigation of actual intrusion attempt, etc.

(3) Continuously viewed Carrier. To use this as a Hardened Distribution System, the carrier should be under continuous observation, 24 hours per day (including when operational). Such circuits may be grouped together, but should be separated from all non-continuously viewed circuits ensuring an open field of view. Standing orders should include the requirement to investigate any attempt to disturb the PDS. Appropriate security personnel should investigate the area of attempted penetration within 15 minutes of discovery. This type of hardened carrier should not be used for TS or special category information for non-U.S. UAA.

b. Simple Distribution Systems. These are afforded a reduced level of physical security protection as compared to a Hardened Distribution System. They use a Simple Carrier System (SCS) and the following means are acceptable:

(1) The data cables should be installed in a carrier;

(2)The carrier can be constructed of any material (e.g., wood, PVT, EMT, ferrous conduit). The joints and access points should be secured and be controlled by personnel cleared to the highest level of data handled by the PDS; and

(3)The carrier is to be inspected in accordance with the requirements of Table B-2 page B-5 of this document.

Table B-1 PDS Installation Matrix

(Applies to locations within a LOW Threat environment)

Type of Area

Type of Data	UAA	LCA	CONFIDENTIAL CAA	SECRET CAA	TOP SECRET CAA
CONFIDENTIAL	H	S			
SECRET	H	H	S		
TOP SECRET	H	H	S	S	
SPECIAL CATEGORY		H	H	S	S

(Applies to locations within a MEDIUM Threat Environment)

Type of Area

Type of Data	UAA	LCA	CONFIDENTIAL CAA	SECRET CAA	TOP SECRET CAA
CONFIDENTIAL	H	S			
SECRET	H	H	S		
TOP SECRET	H	H	H	S	
SPECIAL CATEGORY		H	H	H	S

NOTE: The PDS installation matrix in this table relates to use of specific installation procedures listed in paragraph B-3 of this ANNEX.

LEGEND:

- UAA - Uncontrolled Access Area
- LCA - Limited Controlled Area
- CAA - Controlled Access Area
- PDS - Protected Distribution System

B-5

INSTISSI NO. /005

B-0

INSTISSI NO. /005

5. Circuit Separation. The objective is to ensure PDS are not accessed by those without appropriate clearance and to inhibit inappropriate circuit cross connection.

a. General. Circuits of more than one classification level may use components of a single protected distribution system. Where the sharing of a single protected distribution system is feasible, considerable cost savings can be realized. In some cases, the savings will permit wider application of services which otherwise could not be achieved, if separate PDS were required. Refer to references c. and e. to determine if TEMPEST and/or RED/BLACK countermeasures are appropriate for PDS with shared circuits.

b. Access Points. Access to all points with breakouts should be restricted to personnel cleared at the highest level of the breakout. Access points containing multilevel classified circuits, but which do not have breakouts of higher level circuits, can be serviced by lower level cleared personnel, if escorted by personnel cleared for the highest level circuit.

c. Termination Boxes. All termination boxes should be located within a CAA at the highest level of data being interfaced by the box.

d. Additional Requirements. The CTTA may be contacted to ascertain whether RED/BLACK and/or TEMPEST measures are required.

ANNEX C

PROTECTED DISTRIBUTION SYSTEMS (PDS) APPROVAL REQUEST

Requests for PDS approval shall be forwarded to the department or agency Approval Authority. It shall include the following information in each listed category:

1. Installation Site (Identify the organization where the PDS will be installed and a point-of-contact's name and phone number);
2. Installation Activity (Identify the organization responsible for the installation of the PDS, and a point-of-contact's name and phone number);
3. System Information (Provide a description of the components directly connecting to the PDS, and a summary of the type of cable used in the PDS (e.g., fiber optics, shielded twisted pair, coaxial cable) and the electrical parameters (e.g., voltage and current levels);
4. Security Profile (Identify the highest classification of NIS processed on the PDS (if special category information, identify the specific categories or compartments processed); and provide a percentage breakdown of the type of NSI processed on the PDS);
5. Facility Security (This section provides information concerning the security conditions of the facility where the PDS will be located by providing the following):
 - a. Indicate on a map of the residential and commercial area, the facility's approximate location;
 - b. Indicate a fenced facility's fence location on the map and describe the type of fencing construction (also, indicate if a perimeter Intrusion Detection System (IDS) is installed);
 - c. Indicate the automobile, pedestrian, and amphibious access points on the map;
 - d. Are guards posted at these access points, and what hours are the access points open;
 - e. Is a personnel badge recognition system used; are access lists maintained; and is an escort required for uncleared personnel;
 - f. Is a registration control system used for vehicles, employees, visitors, and tradesmen;
6. Building Security (This section requests information on security conditions of the building(s) within which the PDS will be installed as follows):
 - a. Provide a floor plan of the building(s), describe the exterior and interior construction, and identify whether or not the building's perimeter has an IDS installed;
 - b. Indicate on the floor plan the access points to the building(s) (all windows accessible from the ground, fire escapes, etc. should be identified and any implemented window tamper protection devices should be described);
 - c. Are guards posted at the building access points, what hours are the access points open, and are cipher/simplex locks used for administrative access control to the building;
 - d. Indicate what type of doors and locks secure the access points;
 - e. Is a personnel badge recognition systems in use and are access lists maintained;
 - f. Indicate the clearance level of personnel entering the building , and if a clearance is required for unescorted access to the building;
 - g. Specify how the movement and operation of custodial, maintenance, and vending personnel is controlled, and if this requires an escort or continuous surveillance for uncleared personnel;

7. Protected Distribution Systems (PDS) (This section describes the security condition of PDS by providing the following information);
- a. Provide classification level of the area controlled, and indicate if uncleared personnel are monitored?
 - b. Indicate on a map or floor plan the location and routing of the proposed PDS. Describe its construction;
 - c. Describe the inspection procedures for detection of tampering; and
 - d. Will the PDS be alarmed, if so, describe in detail.