DEPARTMENT OF THE NAVY

NAVSO P-5239-22
OCTOBER 1997

PROTECTED DISTRIBUTION SYSTEM (PDS) GUIDEBOOK

MODULE 22

INFORMATION SYSTEMS SECURITY (INFOSEC) PROGRAM GUIDELINES

NAVSO P-5239-22
OCTOBER 1997

Distribution: Submit requests for placement on distribution (including supporting justification), or amendment to the existing distribution, to:

Commanding Officer
Space and Naval Warfare Systems Center Charleston
Code 723
P.O. Box 190022
North Charleston, SC 29419-9022

Commercial 1-800-304-4636
E-Mail: subscribe@infosec.navy.mil

Electronic versions of this document may be downloaded via anonymous ftp from infosec.navy.mil or http://infosec.navy.mil/info.html.

FOREWORD

Naval INFOSEC Publication (NAVSO Pub) 5239 “Information Systems Security (INFOSEC) Program Guidelines” is issued by the Chief of Naval Operations (N643). It consists of a series of modules providing procedural, technical, administrative and/or supplemental guidance for all information systems, whether business or tactical, used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission or receipt of data. Each module will focus on a distinct program element and describe a standard methodology for planning, implementing and executing that element of the INFOSEC program within the Department of the Navy (DON).

This module, "Protected Distribution System (PDS) Guidebook", provides the Information Systems Security Managers (ISSMs) and Information Systems Security Officers (ISSOs) with guidance and procedures to be used when designing and installing PDSs.

This module supersedes Section VI of Enclosure (4) “PDS Approval Requests” and Attachment (A) to Enclosure (5) “PDS Installation Criteria” of OPNAVINST C5510.93E, dated 22 February 1988.

THIS PAGE INTENTIONALLY BLANK

TABLE OF CONTENTS

PROTECTED DISTRIBUTION SYSTEM GUIDEBOOK

1. **REFERENCES.** The following references are applicable to the installation and use of PDS:

a. NSTISSI No.7003, Protected Distribution Systems (PDS), of 13 Dec 96.

b. Department of Defense Foreign Clearance Guide, distribution periodically [1]

c. DoD Dir C5200.19, dated 16 May 96

d. NSTISSAM TEMPEST/2-95, RED/BLACK Installation Guidelines, dated 12 Dec 96 [2]

2. **PURPOSE.** This guidebook implements reference (a) and stipulates approval authority, standards, and guidance for the design, installation, and maintenance of a Protected Distribution System (PDS). This guidebook 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 a PDS.

3. **SCOPE.**

a. This guidebook applies to Department of the Navy activities which use, or are contemplating the use of a PDS to protect the transmission of unencrypted classified National Security Information (NSI). This guidebook describes the requirements for a PDS installed within the U.S. (including its territories and possessions) and within LOW and MEDIUM threat locations outside the United States as described by reference (b). The threat within the U.S. is LOW. The use of a PDS within a HIGH or CRITICAL threat location (per reference (b)) is not recommended. If a PDS is used in these location, protection techniques are determined on a case-by-case basis by the cognizant Approval Authority.

b. 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.

---

[1] Available through the local Naval Criminal and Investigative Service Field Office.
[2] Available from SPAWARSYSCEN Charleston SC Code J723

c. Definitions specifically applicable to this guidebook are contained in Appendix A.

4. GENERAL.

a. PDS are used to transmit unencrypted classified NSI through an area of lesser classification or control. In as much 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 are 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 costs.

b. Incidents of tampering, penetration, or unauthorized interception must be reported immediately to the PDS Approval Authority for assessment, and the local Security Manger 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.

5. SYSTEM APPROVAL.

a. The PDS for shore facilities should be installed in compliance with Appendix 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 or 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.

b. The PDS for ships should be installed in accordance with Section B.6 of Appendix B. In accordance with Appendix B, PDS are not required aboard submarines since physical access is controlled at the Secret level.

c. 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 Approval Authority's technical representative to verify compliance with Appendix B and, if appropriate, a Certified TEMPEST Technical Authority (CTTA) to determine the need for TEMPEST countermeasures in accordance with reference (c).

d. Requests for approval of PDS shall include the information required by Appendix 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/rectification failure.

e. Temporary test configurations do not require formal approval if they do no exceed one month duration; are confined within U.S. Government installation; and do not process higher than SECRET information. However, they must be approved by the responsible Designated Approval Authority (DAA).

f. 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.

g. 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 a new approval must be obtained.

h. Deactivation of approved PDS must be reported to the PDS Approval Authority.

6. **APPROVAL AUTHORITIES/TECHNICAL REVIEW AUTHORITY.** In accordance with reference (a) the following Approval Authorities are identified for DON PDS.

a. Space and Naval Warfare Systems Center Charleston SC (SPAWARSYSCEN) is the Approval Authority for DON SECRET and TOP SECRET GENSER PDS. In addition, SPAWARSYSCEN Charleston SC is the Technical Review Authority and engineering support agent for all DON PDS regardless of level of information processed. After review, SPAWARSYSCEN Charleston SC will forward technically acceptable Special Category PDS requests to the appropriate Approval Authority for action. Send all PDS requests for approval to: SPAWARSYSCEN Charleston Code 723, P. O. Box 190022 North Charleston, SC 29419-9022.

b. Commander, Naval Security Group Command (CNSG), in association with the National Security Agency (NSA), is the Approval Authority for DON Cryptologic PDS.

c. The Office of Naval Intelligence (ONI), in association with the Defense Intelligence Agency (DIA), is the Approval Authority for DON Special Compartmented Information (SCI) PDS.

DEFINITIONS

Certain definitions contained in NAVSO P-5239-02. apply to this instruction. Some additional definitions are included to supplement that guidebook.

a. **Approval Authority.** Department or Agency element having the authority to approve 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. **Protected Distribution System (PDS).** Wireline or fiber-optic distribution system used to transmit unencrypted classified NSI through an area of lesser classification or control.

f. **Special Category Information.** 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.

PROTECTED DISTRIBUTION SYSTEM (PDS) INSTALLATION GUIDANCE

1. General. This Appendix provides criteria for installing a Protected Distribution System (PDS). In order to use a PDS for classified NSI, adequate installation procedures must be in place to ensure the PDS does not compromise information. The guidance required varies based upon classification or type of data handled and type of area through which the PDS is installed. A PDS carrying SECRET (S), TOP SECRET (TS), or special category information data should be submitted for approval or review to NISE East Code 723. A criteria matrix is provided in Table B-1, as a cross reference to specific installation procedures contained in this Appendix. Installation and maintenance of PDS follows:

a. PDS terminal equipment should be installed in a CAA;

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

c. Employees in a CAA should be made aware that PDS exist and any suspicious activity should be reported;

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

e. Personnel not having the appropriate security clearance and/or 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 a compromise of the processed information or the security integrity of the PDS;

f. Those PDS subject to periodic visual inspections (Table B-2) and technical inspections (Table B-3) 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, mechanical, TEMPEST, and RED/BLACK integrity of the PDS); and

g. 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 a CTTA.

3. Physical Security. The objective is to deter unauthorized personnel from gaining access to the PDS without such access being discovered. Table B-1 specifies guidance for different areas of control by classification level. In addition, the areas within which the PDS terminates must provide adequate security to prevent undetected access to the PDS termination. From a risk management perspective, this can be met through use of the following physical security measures. The occupant(s) of the terminal area(s) should maintain an awareness of the physical condition of the area, so as to be able to detect any attempt at forced/covert entry. Additional physical security protection beyond what is listed here to provide classified open storage may be required to protect nonvolatile storage devices in the terminal equipment.

a. The door(s) to the area shall be solid core .

b. At the end of the working day, each door into the area shall be secured by either dead bolt lock, located within the terminal area, or through use of a high security key operated dead bolt lock (e.g., Schlage® model B700 or Medico Maxum®).

c. During working hours, the terminal area must be 1) occupied; 2) have access controlled through use of a cipher or Simplex® lock; or, 3) have the doors locked when unoccupied.

d. Windows reachable from the ground must be so constructed that any attempt to force entry will leave detectable and obvious markings. Windows above this level must be locked at the end of the work day.

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

a. Hardened Distribution System. These are afforded significant physical security protection and can be implemented by 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 of pipe, or rigid-sheet ducting, utilizing elbows, couplings, nipples, and connectors of the same materials;

(c) All connections should be permanently sealed completely around all surfaces (e.g., welding (continuous or tack), 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 minimum of 1 meter below the surface and on 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 approve micro-switch alarms should be used. If the carrier is buried in a installation outside the U.S. in a MEDIUM threat location, it should 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 the PDS in concrete or bury the PDS with more depth than that required for security reasons; and,

(e) Suspended systems between building should be elevated a minimum of 5 meters and only used if the property traversed 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 clear 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.

(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;

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; and,

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 non-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 System. 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, PVC, EMT, ferrous conduit). The joints and access point should be secured and 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.

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, considered cost savings can be realized. In some cases, the savings will permits wider application services which otherwise could not be achieved, if separate PDS were required. Refer to references (c) and (d) 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.

6. Shipboard Installations. PDS installed on-board U.S. ships (except submarines) should comply with the following criteria.

a. Splicing of metallic wire or fiber optic cable runs carrying GENSER SECRET, TOP SECRET or any Special Category information external to areas accredited at that level of security shall be avoided. The cable shall not break out at any point along its entire run, except in an area accredited at that level of security. Routing of cables through normally locked spaces should be avoided.

b. Junction boxes required outside of secure spaces should be in an inspectable location and have the case tack welded shut or locked with a combination padlock conforming with FF-P-110, type DE, class 2.

c. If the junction box contains Special Category information, it shall be able to be inspected on all six sides of the box.

d. If a PDS terminates in an area which is not accredited to the level of security of the information (e.g., a stateroom), the PDS termination and associated terminal equipment should be afforded adequate Physical Security protection to preclude undetected access (normally not applicable above the GENSER SECRET level). This can normally be provided through the use of an appropriate security locking mechanism on the access door to the space. Additionally, safeguards may need to be taken to ensure that the information contained on the terminal storage media is provided the necessary protection when the area is unattended (e.g., use of removable hard disks which are secured in an appropriate lockable container).

TABLE B-1 PDS INSTALLATION MATRIX

Applies to location 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	S

Applies to location 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	S

LEGEND:

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

H - Hardened distribution system (paragraph 3.1)
S - Simplified distribution system (paragraph 3.2)

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

TABLE B-2 PDS INSPECTION MATRIX

PDS Visual Inspection Schedule for Location in a LOW Threat Environment (Number of Random Inspection Per Day)		
	Type of Area	
Highest Classification of Data Carried	UAA	LCA[1]
Confidential	one	none
Secret	one	one
Top Secret or Special Category	two	one

PDS Visual Inspection Schedule for Location in a MEDIUM Threat Environment (Number of Random Inspection Per Day)		
	Type of Area	
Highest Classification of Data Carried	UAA	LCA[1]
Confidential	two	one
Secret	four	two
Top Secret or Special Category	six	three

Note 1: Also Applies for Special Category, TS and Secret PDSs that traverse a Confidential CAA.

TABLE B-3 PDS Technical Inspection Schedule

Number of Random Inspections Per Year		
	Threat Environment	
Highest Classification of Data Carried	Low	Medium
Confidential	one	one
Secret	one	two
Top Secret or Special Category	one	four

TABLE B-4 PDS Alarm Circuit Verification Schedule

Highest Classification of Data Carried	Interval
Confidential	monthly
Secret	weekly
Top Secret or Special Category	daily

PROTECTED DISTRIBUTION SYSTEM (PDS) APPROVAL REQUEST

Requests for PDS approval shall be forwarded to NISE East, Code J723, Charleston SC, P.O Box 190022, North Charleston, SC 29419-9022. It shall include the following information in each listed category. Note that approval requests for shipboard PDS shall include only the information associated with categories 1, 2, 3, 4, 7b, 7c, , 8a and 8b.

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) an the electrical parameters (e.g., voltage and current levels);

4. Security Profile (Identify the highest classification of NSI 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 point 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 the 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 devises 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 system 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 System (PDS) (This section describes the security condition of PDS by provided 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.

8. Terminal Area Security (This section describes the security condition of the PDS terminal areas by providing the following information):

a. Identify how doors to the terminal areas associated with the PDS will be secured after working hours;

b. Indicate how doors to the terminal areas associated with the PDS will be controlled during working hours; and,

c. Describe any windows in the areas and how they are secured, identifying any which can be reached from the ground.