

**PROTECTED DISTRIBUTION SYSTEM (PDS) DESIGN TEMPLATE
FOR CLASSIFIED PROCESSING ENVIRONMENTS**

**FOR
NAVY/MARINE CORPS INTRANET (NMCI)**

**Raytheon Document No: 58-03474-001
Revision –**



**Contract No.: N00024-00-D-6000
Data in accordance with: Contractor Format**

14 May 2003

Prepared by:
Raytheon
1501 72nd Street North
St. Petersburg, FL 33710



Approvals

	Name	Signature	Initial Date
Program Manager for IA	Frank Nackel		
Principal Engineer for IA	Cameron Gibson		
Requirements/Architecture for IA	Debra Palmer		
Software Quality Assurance for IA	Sharrie Takewell		
Content Lead	Bob Batie		

Document Revision History

This table need only be used when more than one version of the document is issued.

Revision	Issue Date	Author/Modifier	Section, Page(s), and Text Revised
–	05/15/2003	Bob Batie	Initial Release

Table of Contents

Para	Page
1 INTRODUCTION.....	1
2 PURPOSE	1
3 INTENDED AUDIENCE	1
4 BACKGROUND.....	2
4.1 Definitions	2
4.2 PDS Checklists.....	3
4.2.1 Completing the PDS Installation Checklist.....	3
4.2.2 Completing the PDS Physical Security Checklist.....	4
5 NMCI WAN TRANSPORT.....	5
6 PHYSICAL FACILITY INFRASTRUCTURE FOR CLASSIFIED PROCESSING	7
6.1 Restricted Access Area	7
6.1.1 Physical Security Requirements for an RAA	7
6.1.2 RAA with 2 to 25 Classified Seats.....	9
6.1.3 RAA with 25 to 50 Classified Seats.....	9
6.1.4 RAA with More than 50 Classified Seats	10
6.1.5 GSA-Approved Class 5 Security Containers	10
6.2 Controlled Access Areas.....	10
6.2.1 Physical Security Requirements for PDS within a CAA	10
6.2.2 CAA with Classified Seats.....	11
6.3 Secure Room/Open Secret Storage.....	12
6.3.1 Physical Security for Secure Room/Open Secret Storage.....	12
6.4 Utilizing Existing PDS.....	13
7 DESIGNING A PDS	14
7.1 Categories of PDS.....	14
7.1.1 Category I PDS	14
7.1.2 Category II PDS	14
7.1.3 Lock, Pull, and Junction Boxes for PDS	15
7.1.4 Shielded Cable Requirements	15
8 REFERENCES.....	16
9 ACRONYMS	16



List of Illustrations

Figure		Page
5-1	High-Level View of NMCI LAN	5
6.2.2-1	Conceptual Facility Layout with Various Classified Processing Areas	11

List of Tables

Table		Page
6.1.1-1	RAA Equipment Security	8
7-1	PDS Requirement for Low Threat Environments.....	14

List of Appendices

Appendix		Page
A	PDS Installation and Physical Security Checklists for Controlled Access Areas and Restricted Access Areas	A-1
B	PDS-Approved Hardware and Equipment Lists for Controlled Access Areas and Restricted Access Areas	B-1
C	PDS Approval Process for Controlled Access Areas and Restricted Access Areas.....	C-1

1 INTRODUCTION

The need to develop a Protected Distribution System (PDS) Template Design for Classified Processing Environments stems from the rapid pace that the Navy/Marine Corps Intranet (NMCI) is expected to install classified seats. Classified seats are those workstations and printers used to connect to the Secret Internet Protocol Routing Network (SIPRNet) and other classified networks required to provide safe and secure classified processing for the NMCI user community.

The types of facilities discussed herein are:

- Restricted Access Area (RAA) with 1 classified seat
- RAA with 2 to 25 classified seats
- RAA with 26 to 50 classified seats
- RAA with more than 50 classified seats
- Controlled Access Area (CAA) classified seats
- Limited Access Area (LAA)
- Secure Room
- Open Secret Storage

2 PURPOSE

The purpose of this document is to present a template that depicts the various types of classified processing environments to accommodate the rapid deployment of classified seats on NMCI. This template covers various seat types, numbers of seats in a single building, and what equipment, infrastructure, and configuration is required in order to certify the facility and system for classified processing.

This document assumes a TEMPEST Countermeasure Questionnaire (TRQ) has been completed and submitted for review, and there are no TEMPEST Countermeasures required. If the TRQ has not been done, it must be completed in accordance with Reference c of this document.

3 INTENDED AUDIENCE

This document is written for the Information Systems Security Engineer, Facility Security Officer, Site Transition Manager, Designated Approving Authority, Certification Agent, and Installer personnel who actually build out the infrastructure.

4 BACKGROUND

The need for clear directions when designing, installing, and approving classified infrastructure templates stems from confusion in developing and building out classified processing infrastructure. Past policy was not clear; facilities being built were being disapproved for classified processing. The Information Assurance (IA) Pub 5239-22 has been updated. The guiding document has been developed and is being promulgated throughout the Department of the Navy (DON) and U.S. Marine Corps to clear up misconceptions about the proper and secure design and installation of classified processing facilities.

4.1 Definitions

This section lists standard definitions associated with PDSs:

Approval Authority – The Department or Agency element having the authority to approve the installation and operation of the PDS. The Approval Authority is dependent upon the classification level and type of information carried by the PDS, as delineated in Section 5. The Approval Authority for NMCI is SPAWARSYSCEN Charleston.

Approved PDS Lock – A combination padlock conforming to Federal Specification FF-P-110. This lock is resistant to surreptitious manipulation, rather than resistant to physical penetration as in “high security” locks. The S&G model 8077 is an example of an approved PDS lock.

Controlled Access Area (CAA) – A physical area (e.g., building, room, etc.) that is under physical control and to which only personnel cleared to the level of the information being processed are authorized unrestricted access. All other personnel are either escorted by authorized personnel or under continuous surveillance. A CAA shall comply with the physical security requirements of Section 6. Within a CAA, a PDS is not required for classified information processed at or below the classification level to which access to the CAA is controlled. While unprotected cables may run within the CAA, they may not run outside the perimeter of the CAA. Safeguarding and storage of magnetic and hard copy media will be in accordance with SECNAVINST 5510.36.

Limited Access Area (LAA) – A physical area (e.g., a military base in the U.S.) that is under direct U.S. physical control and to which only authorized personnel are admitted. Access is not usually based on clearance level but rather on the presentation of an approved credential (e.g., picture badge with or without other technologies such as magnetic strip, bar code, etc.; visitor pass issued after verification of picture identification; etc.). Verification can be via guard inspection or electronic processing. Within the LAA, a PDS is always required. The PDS will not terminate within a LAA.

Restricted Access Area (RAA) – A physical area (e.g., building, room, etc.) to which only personnel cleared to the level of the information being processed are authorized unrestricted access, but does not meet all the physical security requirements of Section 6.

A PDS and an approved lockbox with an approved PDS lock are required in a RAA. The PDS will be extended within the RAA to a location in close proximity to the workstation and will be terminated in a lockbox that contains the connection for the network.

The workstation used on this type of connection should be a portable workstation that can be secured in an approved General Services Administration (GSA) container per SECNAVINST 5510.36 for the level of information being processed. An alternative would be to apply “tamper evident” tape to the chassis and cover of a desktop computer. The workstation will be connected to the network via this termination.

At the end of each day, the workstation will be disconnected and the lockbox secured with an approved PDS lock.

Printers and other devices associated with the network should be located in either a CAA or Secure Room location, or within a lockbox that is secured with an approved PDS lock.

All windows that might reasonably afford visual observation of classified activities within the facility shall be made opaque or equipped with curtains, blinds, or other coverings. The access doors to the RAA shall comply with the associated requirements of Section 6.

Safeguarding and storage of magnetic and hard copy media shall be in accordance with Chapter 10 of SECNAVINST 5510.36.

Secure Room (SR) – A physical area that meets the construction requirements per Exhibit 10A of SECNAVINST 5510.36 for open storage at the classification level of the information being processed. A PDS is not required for classified information processed at or below the authorized open storage level for the SR.

Special Category Information – The definition is classified and can be found in Reference c.

Uncontrolled Access Area (UAA) – A physical area (e.g., a military base in a foreign country) that is not under direct U.S. physical control and to which unauthorized personnel may gain access. Access to the area is not based upon the presentation of an approved credential. A PDS shall not be installed in a UAA. If other approved protective measures (e.g., use of an NSA Type 1 cryptographic device) cannot be implemented, a waiver may be requested from the Chief of Naval Operations (CNO N6142) via the SPAWARSYSCEN Charleston (Code 723) PDS technical review authority.

4.2 PDS Checklists

The PDS checklists are included in Appendix A of this document. These checklists are designed to assist personnel in describing the physical attributes of the facility(ies) being considered as locations for classified processing systems. They are an important part of the PDS design package and provide consistent data for clearly describing the security features of the physical facility.

The site personnel should use these checklists when completing the site survey for NMCI classified processing systems being scheduled for installation at their location. Completion of these checklists may be a shared responsibility between the DON and Information Strike Force (ISF) personnel. The checklists should be forwarded to the reviewing and approving authority Spawar Systems Center Charleston SC (SSC CH), as well as the site design personnel to ensure that accurate physical build out can be accomplished.

4.2.1 Completing the PDS Installation Checklist

This is a very simple form to complete. There are two columns that contain categories of descriptive information about the PDS to be installed or the PDS that has been installed. The very first row is labeled “Building / room (s)”. In the first blank cell of the first blank column, enter the building or room number. Then complete the column by checking the appropriate characteristic of the PDS. The additional columns are used for other rooms or buildings to describe the PDS installation associated with that space.



4.2.2 Completing the PDS Physical Security Checklist

This form is organized similar to the PDS Installation Checklist. The first three cells describe the building/room and whether it is designated as a CAA, RAA, or Secure Room. Enter the information in these cells and complete the column by checking the appropriate box. The additional columns are used for additional spaces. Most of the sections require one checkmark. However, the “Doors” section may require extra checkmarks, depending on if the hinges are external or they are double doors.

5 NMCI WAN TRANSPORT

A top-level view of a classified Transport Boundary (cTB) encrypts classified network traffic before it reaches the outer switch of the unclassified Transport Boundary (TB). The unclassified Transport Boundary then transports the encrypted traffic to the Very high performance Backbone Network Services (vBNS+) and/or Community of Interest Network Services (COINS) and the Network Operations Center (NOC). From the NOC, classified traffic can be routed to and from the SIPRNet. Figure 5-1 shows a normal architecture to and through the classified Transport Boundary.

The assumption here is the area between building A and Building B is an LAA/RAA. This area would be fenced in with an 8ft. high fence topped with concertina wire. The PDS here would either be Buried or Suspended carrier following all the requirement for each type of PDS.

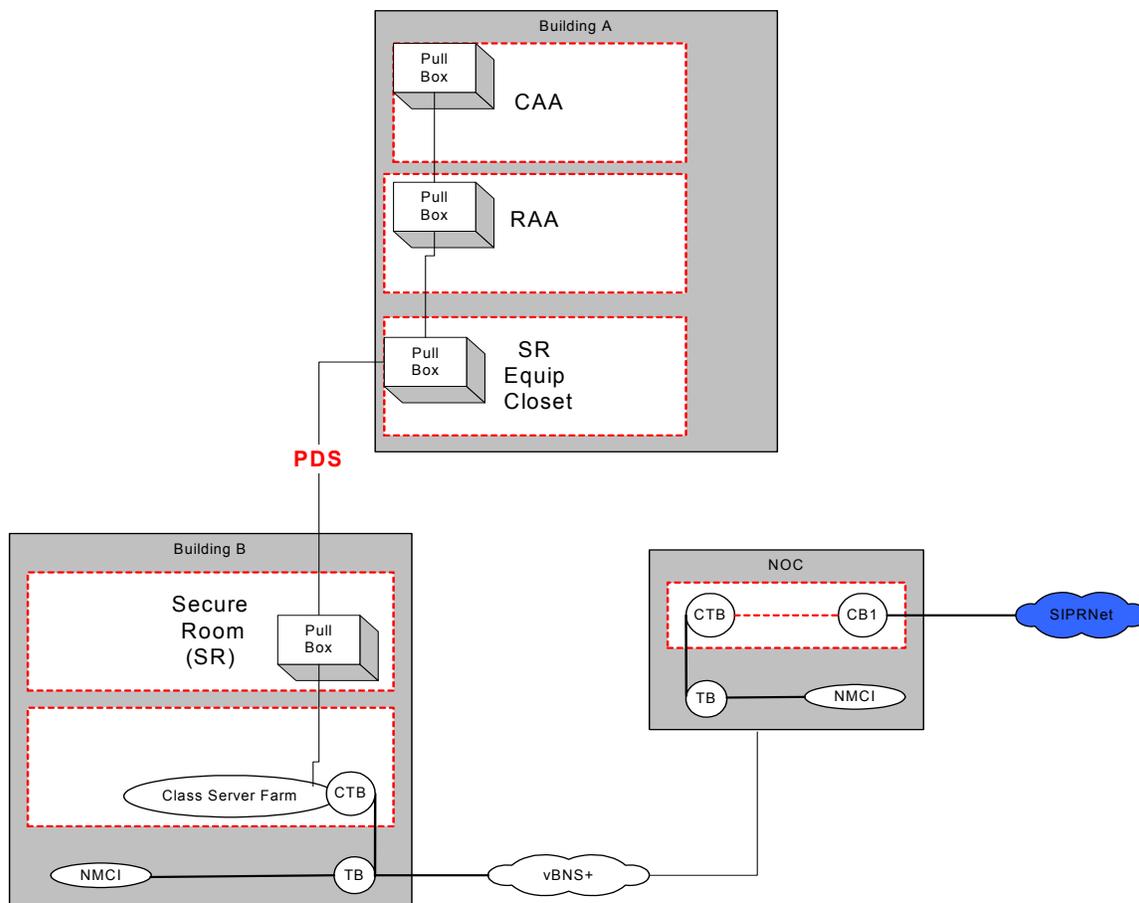


Figure 5-1. High-Level View of NMCI WAN

Traffic from the classified seats travels the PDS to the classified server farm or classified Transport Boundary. The classified server farm contains Antivirus, Intruder Alert (ITA), Windows 2000 policy managers, as well as vulnerability and threat analysis sensors. All of these manage the IA components installed on the client and application servers. The components used for the classified server farm are listed in Appendix B.



The PDS that runs between the buildings A and B may be suspended or buried. See paragraph 7.1.2 of this document or Refer to IA Pub 5239-22, paragraph 6.3.2 for detailed guidance.

6 PHYSICAL FACILITY INFRASTRUCTURE FOR CLASSIFIED PROCESSING

6.1 Restricted Access Area

A physical area (e.g., building, room, etc.) to which only personnel cleared to the level of the information being processed are authorized unrestricted access, but does not meet all the physical security requirements of a CAA.

6.1.1 Physical Security Requirements for an RAA

Physical security for an RAA only applies to the doors. The doors must be constructed of substantial wood or metal. The door shall have a high security dead bolt lock with a 1-inch throw and a cylinder that meets UL437 Standard; or a built-in GSA-approved combination lock meeting Fed Spec FF-L-2740. The hinge pins of out swing doors shall be peened, brazed, or spot-welded to prevent removal. When double doors are used, an astragal will be installed on the active leaf of the door. PDS that terminates in a RAA is controlled at the level of the National Security Information (NSI) (classified information) carried by the PDS. Each RAA must be equipped with a GSA-approved security container for storage of hard drives, cable, and other classified material. All windows must have an opaque covering, curtains, or blinds to prevent inadvertent viewing from outside the RAA.

The PDS infrastructure consists of all hardware required to protect cables carrying NSI. For an RAA, a Category II PDS must be installed. This includes approved lock/junction/pull boxes, conduit, couplers, and ducting. A lockbox (preferably with internal hinges) is used to protect the PDS termination. Lockboxes used for termination within the RAA should be at least 6 x 6 x 4 inches deep and have a door with internal hinges. The hasp must be permanently fixed to the box. If hinges are external, the hinge pin must be welded. Tap screws may be used internally to mount the terminal block. No other openings are authorized for this box. The lock for the lockbox must be an approved PDS lock. The lockbox may terminate up to four connections within the box as long as it is within 12 feet of the classified workstations and/or printer located in the same room. The PDS should be marked at intervals of 10 feet or less with any color paint or tape except red.

PDS installed between floors in multi-story buildings should be installed in the following manner. The section that goes through the false ceiling must be inspectable. The ceiling tile can be removed, or replaced with a clear tile if allowable by the local Fire code. If neither of those are options, then an inspection path (tube) should be built around the riser.

Conduit within this facility must be at least 3/4-inch Electro Metallic Tubing (EMT) or galvanized threaded pipe (more expensive) but should be large enough to accommodate cables being ran in the facility. All couplers for conduit lockboxes must be sealed all around with metal epoxy. Conduit must be ran below any false ceiling to facilitate unobstructed visual inspection. The PDS may not be ran within walls, modular furniture raceways, and/or any place where it is not viewable in accordance with IA Pub 5239-22.

Classified processing equipment within the RAA must have physical security controls to detect, protect, and hinder exploitation.

Workstations must have removable hard drives and tamper evident tape attached to the cover and chassis to detect tampering. During hours of non-operation, the hard drive is removed and stored in a security container. These drives should also have an associated workstation identification attached to the drive to ensure the appropriate user retrieves the drive for his workstation. If the workstation is portable and does not have the tamper evident tape or removable hard drive, it must be stored in a GSA-approved security container when the facility is left unattended. A Thin Client terminal may also be used in this environment but must adhere to the installation criteria and have tamper evident tape installed in the same manner as discussed earlier in this paragraph.

The networked printer located within a RAA should be small enough to fit inside the drawer of a classified security container when not in use. This should probably be a small footprint deskjet (i.e. LexMark or HP DeskJet) style printer. The printer cable must be stored when not in use. A connection should be provided to the printer within one of the lockboxes. If a laser printer is being used and it is too large for the security container, it must be installed in a security cabinet at all times or be located in a CAA. The printer types below are from the NMCI catalog under Contractor Line Item Number (CLIN) 23.

Within a RAA, such as a Commander’s office or single user location, a parallel or serial printers should be used. Parallel or serial printers need no additional protection, because they are connected to and controlled by the classified processing workstation that provides the protection. Any of the printers listed in the CLIN list may be installed in this configuration without any further security considerations.

Cables used to connect the workstation to the PDS must also be stored in a security container when not in use.

Communications security (COMSEC) equipment (e.g. Type 1 encryption devices) may not be installed within a RAA unless it is housed within a GSA-approved Class 5 security container such as the Information Processing Systems (IPS) Cabinet specifically designed for housing COMSEC or electronic equipment.

[Approved printer containers that house large footprint printers located within RAAs are TBD. Once the container is located and approved, it will be added to Appendix B.](#)

Table 6.1.1-1 shows how equipment within a RAA should be secured, installed, configured, and/or maintained. All equipment should be marked/labeled with the highest classification of the information stored or processed on the system/equipment.

Table 6.1.1-1. RAA Equipment Security

	Tamper Tape	Security Container	Approved Lockbox	Comments
Workstation	X			At all times
Thin Client	X			Diskless
Laptops		X		When not in use
Router/Switch			X	At all times
Removable Media		X		When not in use
Removable Classified Hard Drive		X		When not in use
Cables		X	X <u>1</u> /	When not in use

	Tamper Tape	Security Container	Approved Lockbox	Comments
Printers (small)		X	X	One or the other when not in use
Laser Printers			X	If too large for safe
COMSEC		X		IPL cabinet at all times

Note 1/ If space is available within the lockbox, the cable(s) may be stored inside.

6.1.2 RAA with 2 to 25 Classified Seats

The physical security, PDS infrastructure, cabling, and classified processing equipment for an RAA must meet the requirements as stated in paragraph 6.1.1 of this document and IA Pub 5239-22.

For RAAs where the seat count is between 2 and 25 seats, lockboxes may terminate up to 4 classified seat connections within each box as long as it is within 12 feet of the classified workstations located in the same room. There should be no more than one box per seat and/or printer. The minimum number of lockboxes should be 1 and the maximum number of boxes no more than 26 (depending on the number of printers). It is recommended that approximately eight boxes be installed in this situation.

If the workstation is portable or does not have the tamper evident tape or removable hard drive, it must be stored in a GSA-approved security container when the facility is left unattended. It is recommended that one to two security containers should be available for a facility of this size.

Routers, hubs, or other classified processing equipment housed within the RAA must be installed in a lockbox and must meet the same standards as discussed in paragraph 6.1.1 above. These devices, if left unattended, are subject to tamper and exploitation if not adequately protected. Using tamper resistant tape only prevents the device from being opened and does not prevent an unauthorized user from plugging directly into the device.

6.1.3 RAA with 25 to 50 Classified Seats

The physical security, PDS infrastructure, cabling, and classified processing equipment for an RAA must be installed to meet the requirements as stated in paragraph 6.1.1 of this document and IA Pub 5239-22. Each RAA must be equipped with at least two 4-drawer GSA-approved security containers for storage of hard drives, cables, and other classified material. All windows must have an opaque covering, curtains, or blinds to prevent inadvertent viewing from outside the RAA.

For a facility with 25 to 50 classified seats, there should be no more than 1 lockbox per seat and 1 box per printer. The minimum number of boxes should be equal to the number seats divided by four plus additional boxes to account for printers. The maximum number of boxes should be no more than 50 used as termination points within this RAA. It is recommended that approximately 20 boxes be installed.

Conduit used to construct the category II PDS within this facility must be large enough to accommodate the number of cables being run in the facility. Major raceways within the facility may be as large as 4 inches in diameter (large enough to accommodate the number of cables being installed with pull boxes) where smaller size conduits are attached that provide secure access to the termination lockbox. All couplers for conduit lockboxes must be sealed all around with metal epoxy in the same manner as discussed in paragraph 6.1.1.

Workstations and printers must have removable hard drives and tamper evident tape attached to the cover and chassis. During hours of non-operation, the hard drive is removed and stored in the security

container. If the workstation is portable or does not have the tamper evident tape or removable hard drive, it must be stored in a GSA-approved security container when the facility is left unattended.

6.1.4 RAA with More than 50 Classified Seats

When more than 50 classified seats are being installed, careful cost analysis should be conducted (by the design engineer) to determine the cost effectiveness of installation within the RAA or making physical security upgrades to meet the standards of a CAA. If it is determined that the cost to maintain the RAA is more feasible, follow the guidance set forth in paragraph 6.1.1 of this document. (Be sure to remember the rule of thumb that the number of terminations per box may be up to four.) Multiple floors within the same building should be included in this assessment, if classified seats are part of the installation plan.

6.1.5 GSA-Approved Class 5 Security Containers

The GSA-approved Class 5 security containers (Hamilton) are used to store classified processing devices such as hard drives, small footprint printers, COMSEC material, and other classified material within an RAA or Secure Room where COMSEC devices are used. When used in an RAA, the size of the container required is dependent on the seat count. For locations with fewer than 10 seats, it is recommended that the 2-drawer container be supplied. If the seat count is expected to increase over time, the designer may consider providing the 4-drawer container to ensure adequate space. Where the seat count is greater than 10, the 4-drawer container is recommended. The container should have adequate space to store approximately 10 classified hard drives per drawer. The National Stock Number and dimensions are listed in Appendix B.

6.2 Controlled Access Areas

A physical area (e.g., building, room, etc.) that is under physical control and to which only personnel cleared to the level of the information being processed are authorized unrestricted access. All other personnel are either escorted by authorized personnel or under continuous surveillance (as identified in NAVSO Pub 5239-22).

6.2.1 Physical Security Requirements for PDS within a CAA

A PDS may originate and terminate in a CAA controlled at the level of the National Security Information (NSI) carried by the PDS. The physical security for a CAA is defined in the updated NAVSO Pub 5239-22. The physical security requirements are significant and are similar to a Secure Room but without a GSA lock and Intrusion Detection System (IDS). The PDS Approval Authority certifies a CAA. The Physical Security Manager/ Officer should identify applicable rooms as a CAA, RAA, etc. The local DAA may certify a CAA in which a PDS is not required. The PDS Inspector will validate all applicable rooms and CAAs, if not previously certified by the local DAA during review/inspection. The CAA must meet all physical security requirements of the updated IA Pub 5239-22, dated Jan 2003. The CAA certification must be provided in the site-specific System Security Authorization Agreement (SSAA) for the associated network portion. The objective is to deter unauthorized personnel from gaining access to the PDS, including attached workstations, and to ensure unauthorized access is discovered.

Figure 6.2.1-1 shows a conceptual floor plan where PDS runs from a secure equipment closet traversing an RAA and LAA and terminating within an RAA and CAA. A Category II (hardened) PDS is used to traverse these areas. RAA corridor (No. 6) shows a junction box installed to comply with the PDS policies. Note that within the Secure Room and into the adjoining CAA, no PDS is needed; however, industry best practices should be followed. To other locations where the PDS must traverse the RAA and LAA corridors to terminate within Secure Room No. 2, no PDS is required within Secure Room No. 2.

As the PDS extends into RAA No. 1, a PDS is required to the desktop and printer. Where the PDS leaves the secure equipment room and traverses RAA corridor No. 6, it stops as it enters CAA No 7 and no PDS is required within this area.

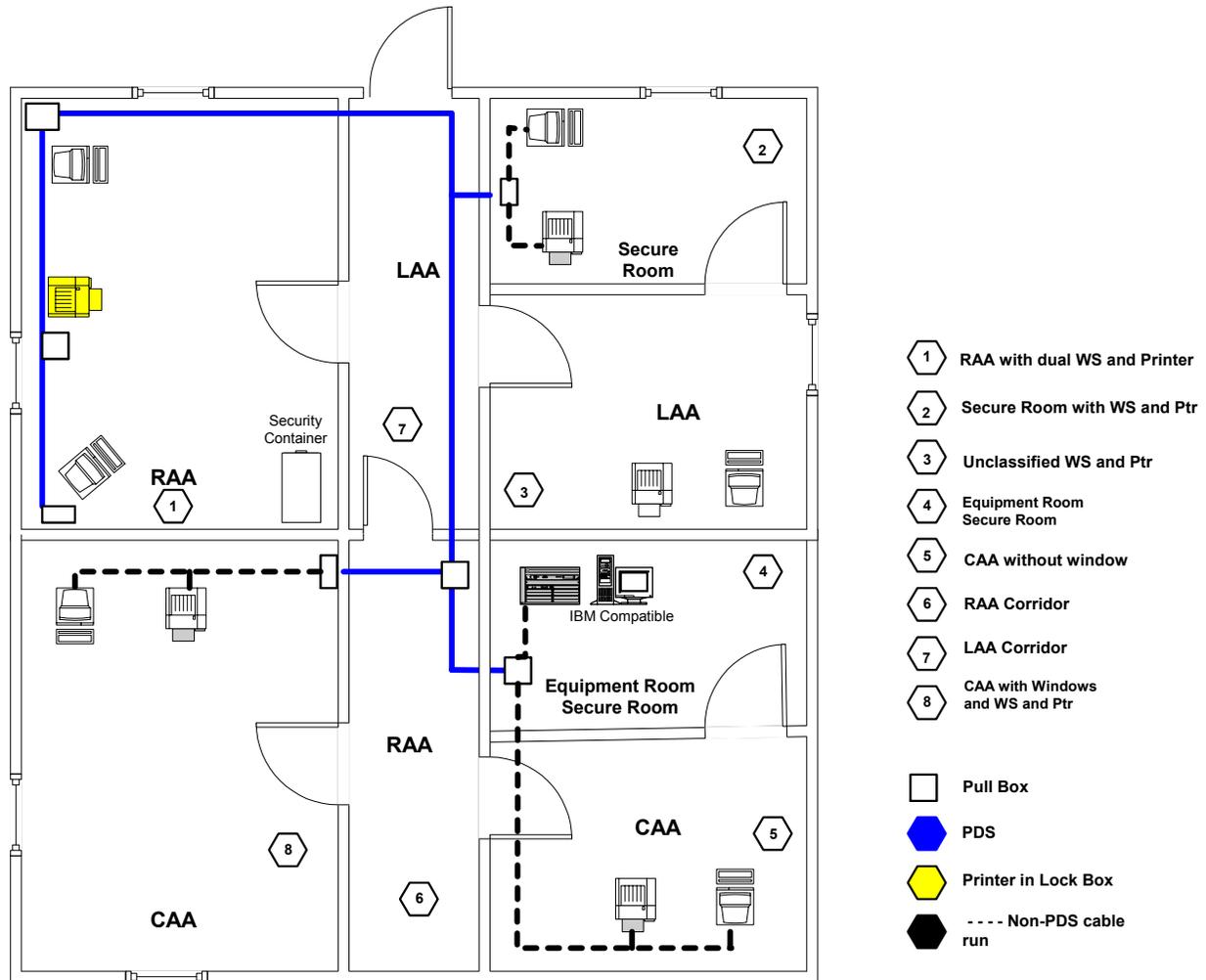


Figure 6.2.2-1. Conceptual Facility Layout with Various Classified Processing Areas

6.2.2 CAA with Classified Seats

In all cases where there is an approved CAA, no PDS is required as long as the level of the information being processed is equal to (or less than) the certification of the CAA. Installation in this area should follow good engineering installation practices for secure networks. This includes cable trays, ducts, drops, and termination boxes. The capacity to handle classified seats in any number should be a design consideration including classified seats from 1 to N.

6.3 Secure Room/Open Secret Storage

Within the Secure Room, no PDS is needed; however, industry best practices identified in the Electronic Industries Association/Telecommunications Industry Association (EIA/TIA) should be followed. The physical security for a Secure Room is defined in SECNAVINST 5510.36. A Secure Room is certified by the Physical Security Manager for the facility. A Secure Room requires a significant level of physical security as discussed in paragraph 5.3.1 for an open secret storage facility. A Secure Room is most often used for COMSEC equipment and may consist of a Class 5 security container or secure cabinet housed within a CAA.

Examples of the most common Secure Rooms are:

- Information Assurance Centers (IACs),
- Server Farms,
- Classified communications closets, and
- Other facilities that meet the physical security requirements.

6.3.1 Physical Security for Secure Room/Open Secret Storage

Secure Room/Open Secret storage is authorized in locations that meet the physical security requirements identified in 5510.36, section 10A. Walls, floors, and the roof shall be of permanent construction materials, true floor to ceiling. Doors shall be made of substantial wood or metal, usually 1-4/3-inch solid core or 18 gauge metal cladding. Doors will have a high security UL437 dead bolt lock (combination X0 7/8/9), and a swipe badge or cipher lock used for control access.

Windows will be made opaque to prevent visual observation. Windows that are less than 18 feet off the ground shall be constructed or covered with materials that indicate forced entry. Openings that are man-passable shall be hardened in accordance with MIL-HDBK-1013/1b or shall not exceed 96 square inches.

The location housing the open storage area is subject to continuous protection by cleared guard or duty personnel inspecting the area once every 4 hours; or an IDS with a response time within 30 minutes of alarm annunciation.

Equipment installed in this area need not be afforded any additional physical protection (i.e., security containers, safes, lockboxes, secure cabinets, or PDSs). The PDS Approval Authority will reevaluate any existing PDS. The correction must be completed within one year of the interim approval date. Good installation and industry best practices should be used when installing systems or equipment within these facilities.

6.4 Utilizing Existing PDS

Existing PDS may be used if it is certified to the standards set forth in IA Pub 5239.22 and its use has been approved by the owner of the PDS. Any additions, extensions, or modifications to an existing approved PDS shall require that new sections of the PDS be submitted for approval. The submission shall reference the approval letter for the existing approved PDS, and the Approval Authority will determine if a re-inspection of the approved section will be required.

The process for using existing PDS requires the local site provide a PDS certification document. If no certification document exists or if the PDS has never been approved, the PDS may be granted an interim approval provided the PDS is documented and a Plan of Action and Milestones (POA&M) developed by the site with scheduled milestones for completion and compliance with the PDS Guide Book, IA Pub 5239.22. The POA&M corrected action must be completed within 1 year of its initial cutover and utilization date.

7 DESIGNING A PDS

When designing a PDS, the following steps should be taken:

1. Determine the classification levels of the NSI.
2. Determine the type of areas the PDS will originate, traverse, and terminate (i.e., Secure Room, CAA, RAA, or LAA).
3. Verify the PDS originates in a Secure Room or CAA.
4. Verify the PDS terminates in a Secure Room, CAA, or RAA.
 - (a) If the PDS terminates in an RAA, lockboxes must be used.
5. Verify the PDS traverses an LAA or better.

Determine the classification levels of the NSI planned or being processed on the system. Determine the threat level for the facility/base where the system will be located. Use Table 7-1 to determine the type of PDS required; i.e., Category I uses a simplified carrier or Category II, which provides a more significant level of protection. Note that Category II is the most common type of PDS installed.

Table 7-1. PDS Requirement for Low Threat Environments

Type of Data	Type of Area				
	LAA	RAA	Confidential CAA	Secret CAA	Top Secret CAA
Confidential	II	I			
Secret	II	II	I		
Top Secret	II	II	I	I	
Special Category	II	II	I	I	I

7.1 Categories of PDS

There are two categories of PDS as described below.

7.1.1 Category I PDS

Category I PDS replaces the “Simplified” PDS. It is used in areas with higher access controls. The carrier may be constructed from PVC or similar type plastic conduit.

Approved Armored cable may be used for easier installation. Joints must be permanently sealed (epoxy).

7.1.2 Category II PDS

Category II PDS replaces the “Hardened” PDS; hardened is now a type of carrier for a Category II PDS. It is the most common category of PDS being installed. There are five types of Category II carriers:

- a. Hardened – The carrier must be constructed from metallic conduit, such as EMT Armored cable; flexible spiral wound conduit cannot be used. Joints must be sealed with epoxy
- b. Buried – The carrier must be buried at least 1 meter. If soil conditions do not allow a 1-meter depth, a shallower carrier may be encased in concrete. The thickness of concrete depends on depth. All joints must be sealed. This type carrier is not used for Base Level Information Infrastructure (BLII). Manholes and hand holes must be sealed (welded) or locked with PDS lock and be inspectable. The carrier should enter the building from underground. Carriers traversing crawlspaces require rigid steel pipe and/or other additional measures. If the carrier enters the side of the building, metal conduit or plastic conduit encased in concrete must be used. Refer to IA Pub 5239-22, paragraph 6.3.2 for detailed guidance.
- c. Suspended – Used between buildings in close proximity when a buried carrier is not possible or cost effective. The carrier must be at least 5 meters high with no poles. The ends of the carrier must terminate in Secure Room or CAA and the areas traversed must be owned/leased by U.S. entity. (Not used for new BLII installations.)
- d. Alarmed Carrier – This type of carrier is used when an IDS is already installed in the facility. The only type of Alarmed Carrier currently approved is a volumetric IDS, which is used for a PDS installed out of view, such as above false ceilings and below false floors. Areas surrounding entire length of PDS must be covered and an alarm test is required, but visual inspection is not. The downfall of this type of carrier is that it is subject to false alarms.
- e. Continuously Viewed – This carrier is used when an area is already monitored by a guard or a camera monitoring system is in place. The carrier must be in metal or plastic conduit and viewed 24/7.

7.1.3 Lock, Pull, and Junction Boxes for PDS

Appendix B contains a list of lock, pull, and junction boxes used with PDSs for egressing and traversing LAAs or RAAs, and terminating within RAAs and CAAs.

7.1.4 Shielded Cable Requirements

IAW the NSTISSAM TEMPEST2/95 w/Amendment 3 Feb 2000, under the recommendations A-F, para 3 states: RED processors meeting the requirements of NSTISSAM TEMPEST/1-92 (Levels II, III, or I) must use optical or shielded wire cables if specified as part of the manufacturer's installation specifications, or if specified for compliance with TEMPEST certification.

8 REFERENCES

- a. SECNAVINST 5510.36, Department of the Navy Information Security Program Regulation, 17 March 1999
- b. IA Pub 5239.22 PDS Guide Book, Draft update Jan 2003
- c. NSTISSAM TEMPEST/2-95 12 December 1995, with NSTISSAM TEMPEST/2-95A Amendment of 3 February 2000
- d. OPNAVINST C5510.93F/MCO C5510.19 Navy Marine Corps Implementation of National Policy on the Control of Compromising Emanations, January 2002

9 ACRONYMS

The following list of acronyms is used in this document.

BLII	Base Level Information Infrastructure
CAA	Controller Access Area
CLIN	Contract Line Item Number
CNO	Chief of Naval Operations
COMSEC	Communications Security
cTB	Classified Transport Boundary
CTTA	Certified TEMPEST Technical Authority
DAA	Designated Approving Authority
DON	Department of the Navy
EIA	Electronic Industries Association
EMI	Electromagnetic Interference
EMT	Electro Metallic Tubing
RFI	Radio Frequency Interference
GSA	General Services Administration
HDBK	Handbook
IA	Information Assurance
IAC	Information Assurance Center
IATO	Interim Approval to Operate
IDS	Intrusion Detection System
IPS	Information Processing System
ISF	Information Strike Force
ISSM	Information Systems Security Manager
ITA	Intruder Alert
LAA	Limited Access Area



MIL	Military
NMCI	Navy/Marine Corps Intranet
NOC	Network Operations Center
NSI	National Security Information
PDS	Protective Distribution System
POA&M	Plan of Action and Milestones
POC	Point of Contact
Ptr	Printer
RAA	Restricted Access Area
SIPRNet	Secret Internet Protocol Routing Network
SR	Secure Room
SSAA	System Security Authorization Agreement
TB	Transport Boundary
TBD	To Be Determined
TIA	Telecommunications Industry Association
TRQ	TEMPEST Countermeasure Questionnaire
UAA	Uncontrolled Access Area
vBNS+	very high performance Backbone Network Services
WS	Workstation



APPENDIX A. PDS Installation and Physical Security Checklists for Controlled Access Areas and Restricted Access Areas

A.1 COMPLETING THE PDS INSTALLATION CHECKLIST

This is a very simple form to complete. There are two columns that contain categories of descriptive information about the Protected Distribution System (PDS) to be installed or the PDS that has been installed. The very first row is labeled “Building / room (s)”. In the first blank cell of the first blank column, enter the building or room number. Then complete the column by checking the appropriate characteristic of the PDS. The additional columns are used for other rooms or buildings to describe the PDS installation associated with that space.

A.2 COMPLETING THE PDS PHYSICAL SECURITY CHECKLIST

This form is organized similar to the PDS Installation Checklist. The first three cells describe the building/room and whether it is designated as a Controlled Access Area (CAA), Restricted Access Area (RAA), or Secure Room. Enter the information in these cells and complete the column by checking the appropriate box. The additional columns are used for additional spaces.

All spaces involved in the PDS design should be documented in the checklist. This includes Limited Access Area (LAA), RAA, or hallways, as well as the termination room(s).



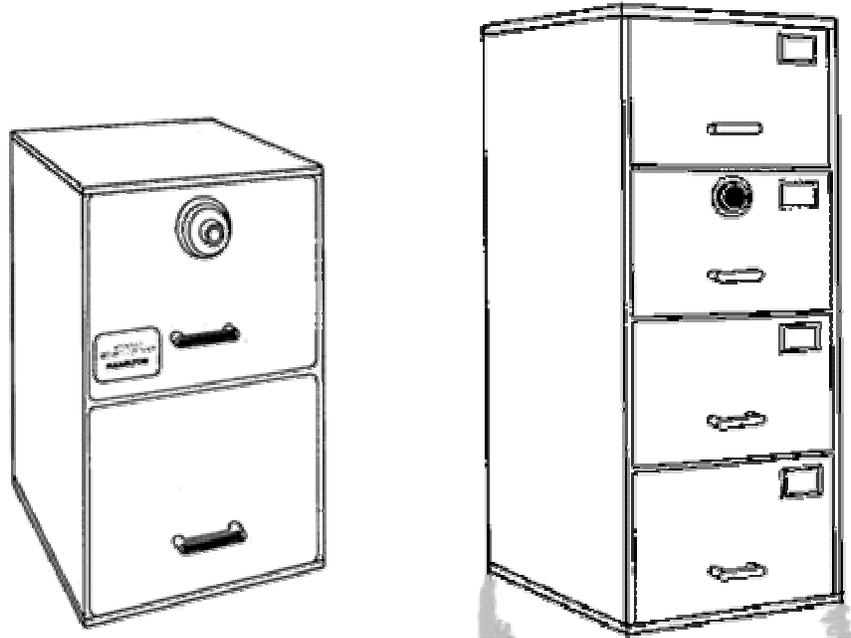
PDS Installation Checklist								
	Building / room (s)							
Carrier Type	Simplified (Cat 1)							
	Hardened							
	Buried							
	Alarmed							
	Suspended							
	Continuously viewed							
Origin	Secure Room							
	CAA							
	GSA Approved Safe							
Traverse	CAA							
	RAA							
	LAA							
	Other							
Terminate	Secure Room							
	CAA							
	RAA in lock box							
	Period Processing							
Pull Box	Continuous metal							
	Non-removable hinge							
	No knockouts							
	weld/countinous seal							
Lock Box	Meets pull box req.							
	Non-removable hinge							
	Permanent hasp							
	Approved PDS Lock							
Carrier	Below ceiling							
	In view / inspectable							
	Joints welded/epoxy							
RAA W/S	Mobile W/S in safe							
	Desktop with seal							
	Cable secured							
Printers	No Printer							
	In SR or CAA							
	Connected to WS							
	In lock box							
Check one or more items for Carrier Type, Origin, Traverse, Terminate and Printer Check all items for Carrier, Pull Box and Lock Box Check one item and Cable Secured for RAA Workstation								

PDS Physical Security Checklist								
	Building							
	Room							
	SR/CAA/RAA*							
Construction	True ceiling							
	Expanded Metal							
	Wire Mesh							
	IDS							
	Other							
Openings	No openings							
	Less than 96 sq in							
	Manbars							
	IDS							
Doors	Solid core							
	Metal/Metal Clad							
	Glass/solid							
	Non-removable hinge							
	Astragal active leaf							
Locks	UL437							
	X0-7/8/9							
	panic/crash bar							
Access	Swipe/proximity							
	Cipher lock							
	Locked when gone							
Viewing	No Windows							
	Blinds/Curtains							
	Locked/sealed							
	Not in view							
Windows	No Windows							
	Covered/Manbars							
	Sealed							
	Greater than 18 feet							
*RAA must meet door, lock, access and viewing requirements								



APPENDIX B. PDS-Approved Hardware and Equipment Lists for Controlled Access Areas and Restricted Access Areas

Figure B-1 shows General Services Administration (GSA)-approved security containers.



Item	Vendor	Security Container Capacity	National Stock Number	Dimensions
1	Hamilton	2-Drawer	7110-00-082-6111	24-13/16" High 20-13/16" Wide 28-1/2" Deep
2	Hamilton	4-Drawer	7110-00-082-6112	48-13/16" High 20-13/16" Wide 28-1/2" Deep
3	DieBold	2-Drawer	7110-00-082-6111	24-13/16" High 20-13/16" Wide 28-1/2" Deep
4	DieBold	4-Drawer	7110-00-082-6112	48-13/16" High 20-13/16" Wide 28-1/2" Deep

Figure B-1. GSA-Approved Class 5 Classified Security Containers

B.1 PDS PULL/JUNCTION BOXES

Table B-1 contains the current list of approved junction/pull boxes for Protected Distribution System (PDS) installation. Other boxes will be added to this list as they are approved by the Certified TEMPEST Technical Authority (CTTA).

Table B-1. Junction/Pull Boxes for PDS installation

Description	Part Number	Vendor	Approved
Secure Enclosure 6'h x 6"w x 4"d	SP51-3427-01	McKinstry Metals	YES
Secure Surface Mount Box Enclosure (7.5' x 2.5" x 3.13")	SEC-WM-SM2-H1	Holcom	YES with epoxied hinge pin
Junction Box 7"(H) x 6"(W) x 4"(D).	SEC-WM-764-H1.	Holcom	YES with epoxied hinge pin

B.2 PRINTERS FOR CLASSIFIED PROCESSING

Table B-2 lists the printers from the NMCI Information Strike Force (ISF) Contract Line Item Number (CLIN) catalog. These printers are used to process classified information within Restricted Access Areas (RAAs) or Controlled Access Areas (CAAs). If these network printers are installed in a CAA, no additional protection is required. However, if the network printer is installed within an RAA, it must be installed within a security container or approved printer cabinet.

Table B-2. Printers for Classified Processing

Printer Type	Print Type	Make/Model	Authorized Location
Network Printer B/W Small Group	Laser Jet	HP 2100m	RAA Safe/Container or CAA
Network Printer, B/W Entry Workgroup	Laser	P-1210	RAA Safe/Container or CAA
Network Printer, Color, Small Group	Laser	HP 2500Cxi	RAA Container or CAA

Printers that are installed as a parallel or serial device need no additional security protections when installed in an RAA, because the connection is controlled by the workstation and does not provide a direct connection to the network.

B.3 PRINTER CABINETS FOR HOUSING CLASSIFIED PROCESSING PRINTERS

Printer cabinets are used in an RAA for printers that are too large to fit into standard security containers. Table B-4 lists the approved printer containers.

Table B-4. Approved Printer Cabinet

Printer Cabinet Type	Part Number	Print Type	Make/Model
TBD		Laser	HP 2500Cxi

B.4 TAMPER EVIDENT TAPE

The approved tamper evident tape to be applied by the installers of the classified processing systems is shown below. The tape should be purchased from one of the following vendors. First choice is Dickey Manufacturing Company. The price is competitive and their product has been recommended by the CTTA. The tape comes on rolls that are numbered and bar coded and leave a message either Open or VOID when tampered with. The tape comes in a variety of colors. I recommend Blue.

Vendor Information	Cost	Part/Stock Number	Quantity
Dickey Manufacturing Company 1315 East Main Street Saint Charles, Illinois 60174 630-584-2918, www.securityseals.com	per roll		
	\$25.00	TETS0001-1	100
	151.00	TETS0001-2	1000
	580.00	TETS0001-3	5000
Aircraft Security & Alert Systems 3863 Royal Lane Dallas, Texas 75229 219-956-9663, www.aircraftsecurityalert.com	Strip		
	\$1.25		each

B.5 GSA-APPROVED SECURITY CONTAINERS

Information Processing System (IPS) containers that conform to National Security Agency (NSA) National Policy NSTISSP #10, effective 21 July 1999

These containers provide for closed door, unmanned online operation of computers, network servers, and workstations that process classified information. These containers are provided in three different sizes:

1. Single door 30-39-24 unit and two double-door cabinets,
2. 54-39-24 unit, and
3. 54-45-24 unit.

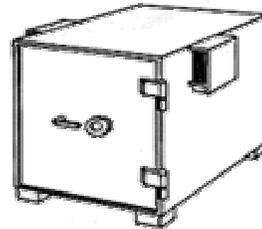
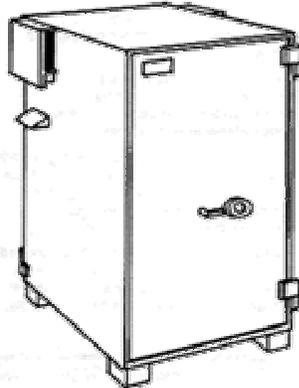
All of these cabinets provide for standard 24-inch rack mounting. Optional 19-inch rack mounting is available. Where environmental and/or temperature extremes are present or where electromagnetic interference/radio frequency interference (EMI/RFI) shielding is required, elective upgrades are available.

This new NSA policy states that, effective 31 December 1999, current communications security (COMSEC) containers may not be used to protect classified, online computer data files (e.g., disc packs or other online devices that process, store, or transmit classified information).

Figure B.5-1 shows a Hamilton Information Processing System (IPS) security container. This is one of the approved containers for installing crypto and other telecommunications equipment within an RAA.

**GSA Approved (IPS)
INFORMATION PROCESSING SYSTEM CONTAINERS**

GSA Approved IPS Containers are designed for the closed-door operation of your COMSEC- COMPUSEC- INFOSEC communications-computer equipment. These containers provide for the unmanned, on-line operation of computers, network servers and workstations that process classified information.



- All containers have standard rack mounts.
- Custom sizes and/or interiors are available to meet your specific equipment applications.
- Adjustable channels are affixed to interior side walls to facilitate installation of equipment.
- An optional fixed shell and/or a pull out shell can be provided for all IPS containers.

CLASS 5 PROTECTION
This is a U.S. Government CLASS 5 IPS Security Container which has been approved by the Government under Federal Specifications AA-F-363. It Affords the Following Protection:
20 man-hours against surreptitious entry
30 man-minutes against covert entry
15 man-minutes against forced entry

NEW LOCK SPECIFICATION
Amendment 1 of Federal Specification AA-F-363 requires that all locks used on GSA Approved Security Containers meet Federal Specification FF-L-2749.

This container is not intended for storage of classified documents.

Look for the Blue Label – Only GSA Approved IPS Containers are authorized for the protection of COMSEC and computer equipment processing classified information in unattended areas.

Item	Vendor	Security Container Capacity	National Stock Number	Dimensions
1	Hamilton	2 Drawer	7110-00-082-6111	24-13/16" High 20-13/16" Wide 28-1/2" Deep
2	Hamilton	4 Drawer	7110-00-082-6112	48-13/16" High 20-13/16" Wide 28-1/2" Deep
3	DieBold	2 Drawer	7110-00-920-9342	28 1/4" High 19 1/4" Wide 28" Deep
4	DieBold	4 Drawer	7110-00-920-9342	51 1/8" High 19 1/4" Wide 28" Deep
5	Trusted Systems	2 Drawer	TBD	24-13/16" High 20-13/16" Wide

Item	Vendor	Security Container Capacity	National Stock Number	Dimensions
				28-1/2" Deep
6	Trusted Systems	4 Drawer	TBD	48-13/16" High 20-13/16" Wide 28-1/2" Deep

Figure B.5-1. Approved Information Processing System Container

B.6 SECURE ROOM CLASSIFIED TRANSPORT BOUNDARY EQUIPMENT

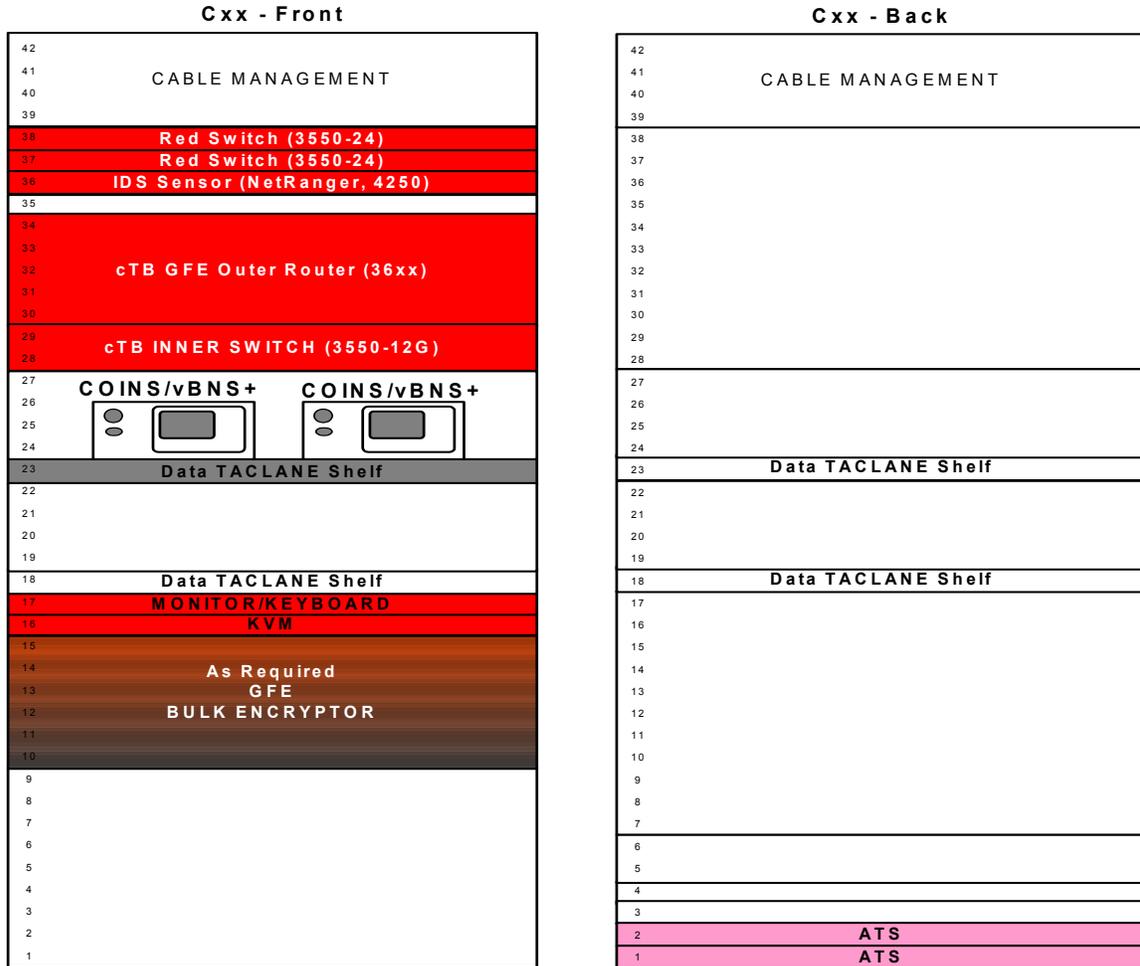
Table B.6-1 contains a list of equipment typically installed in a Secure Room or CAA closet where classified Transport Boundary equipment is located. This set of equipment may vary depending on the number of classified processing systems being connected to this set of equipment.

Table B.6-1. Secure Equipment Closet Classified Processing Components

Component	Vendor	Product	Type	Qty
Symantec ESM Manager W2K	Symantec	Manager	Hardware/Software Windows	1
Symantec Manager ITA	Symantec	Manager	Hardware/Software Windows	2
Symantec Manager Anti-Virus	Symantec	Manager	Hardware/Software Windows	1
Vulnerability Assessment Sensor	Symantec	Retriever	Hardware/Software Windows	1
Threat Analysis Sensor	Raytheon	SR	Hardware/Software Windows	1
Remote Dial-In Palladium Modem	KC	Optiva	Hardware	1
Type 1 Encryptor	GD	KG-175	Hardware	3

Figure B.6-1 shows the typical installation setup of a classified Transport Boundary with crypto.

cTB Crypto Cabinet



1 Cisco IDS 4250	2 Taclane KG-175
1 Cisco Catalyst 36xx	*FUTURE GFE Router
4 Cisco Catalyst 3550-24	*1 KG-xx
1 Cisco Catalyst 3550-12G	
125.6 Startup Amps, 35.6 Running Amps	
~7,500 BTUs, 20 AC Plugs	

Figure B.6-1. Typical Installation of a Classified Transport Boundary with Crypto



APPENDIX C. PDS Approval Process for Controlled Access Areas and Restricted Access Areas

C.1 PDS APPROVAL PROCESS

All Protected Distribution System (PDS) requests, regardless of classification level of the information to be protected, shall be submitted to SPAWARSYSCEN Charleston Code 723, P.O. Box 190022 North Charleston, SC 29419-9022 for technical review and approval. Before a PDS is authorized for the distribution of National Security Information (NSI), the PDS Approval Authority shall review and approve the PDS. If not approved, receiving PDS interim approval is a process (listed below) to achieve classified connectivity.

Previously existing/approved PDSs do not require reevaluations. Any additions, extensions, or modifications to an existing approved PDS shall require that the new sections of the PDS be submitted for approval. The submission shall reference the approval letter for the existing approved PDS, and the Approval Authority will determine if a re-inspection of the approved section will be required.

The Information Strike Force (ISF) team is responsible for the design and installation of new PDS. To prevent potential cost and time delays of an inadequate design, the PDS design should be coordinated early in the Navy/Marine Corps Intranet (NMCI) infrastructure build-out process and the PDS design shall be reviewed and approved by the Approval Authority before installation. If a PDS Approval Request is submitted after installation and found to be noncompliant, the PDS will not be approved until the identified deficiencies are corrected.

If the PDS design review indicates that deviations exist and the deviations are considered minor, an interim approval period of up to twelve months to correct the deviations and obtain full compliance can be approved. An Interim Approval to operate the PDS can be issued by the NMCI Designated Approving Authority (DAA) (i.e., COMNETWARCOM) pending full compliance. A Plan of Action and Milestones (POA&M) to correct the deviations is to be submitted by the site to the NMCI DAA within 30 days after the NMCI DAA grants Interim Approval. Development of the POA&M should be a coordinated effort between the site's point of contacts (POCs) (i.e., Government Information Systems Security Manager [ISSM], Physical Security Officer, and ISF Site Manager) and the PDS Inspector.

If discrepancies exist and Interim Approval for the PDS for the rollout of classified seats is requested, PMW 161 will provide a Technical Risk Assessment to the NMCI DAA who will make the determination to grant formal Interim Approval to Operate (IATO).

C.2 PDS APPROVAL PROCESS FLOWCHART

A flowchart of the approval process is provided in Figure C.2-1. The paragraphs that follow provide a general description of the process. The intent is to provide an overview of the design, installation, and approval processes of a PDS.

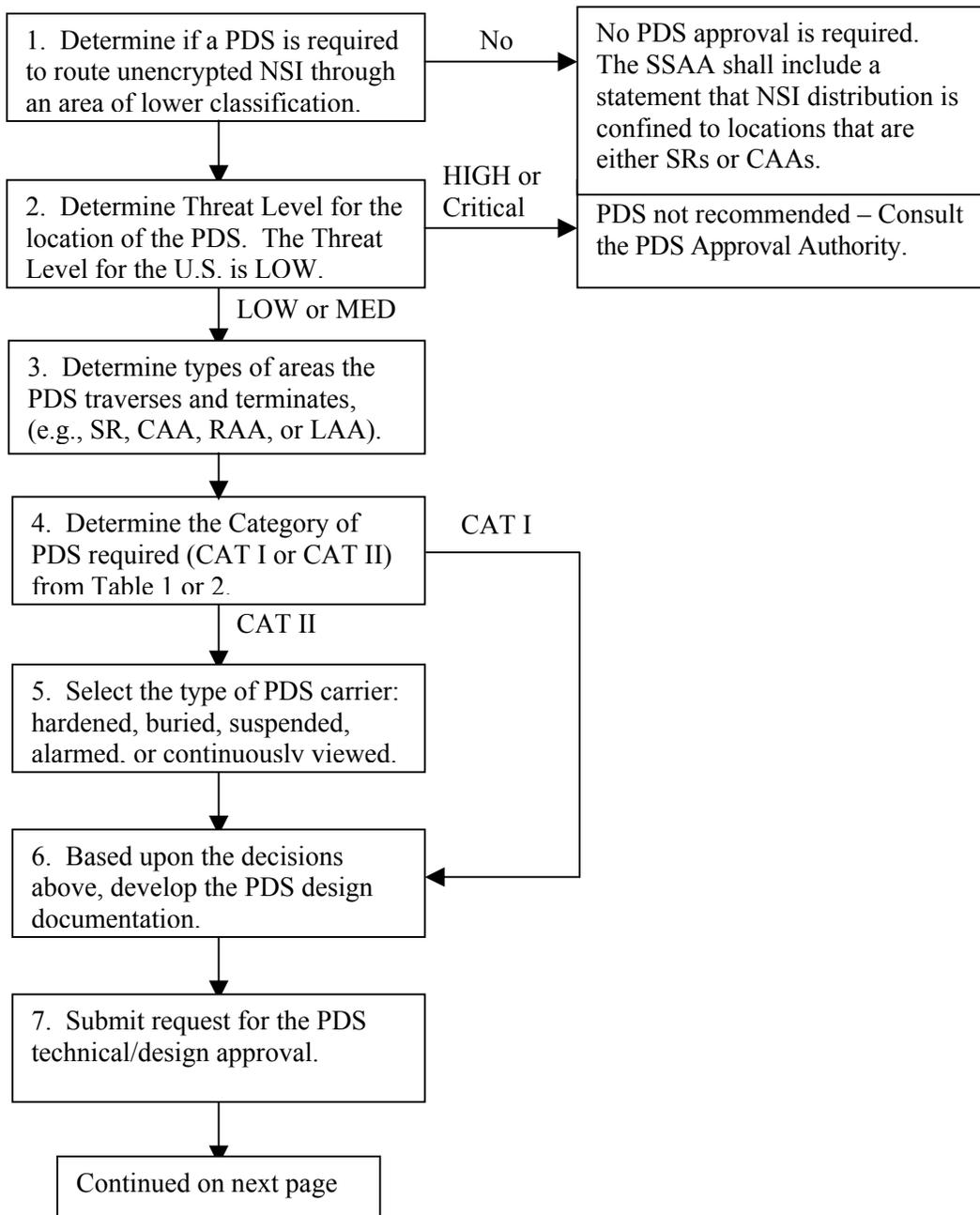


Figure C-2.1. PDS Approval Process Flowchart

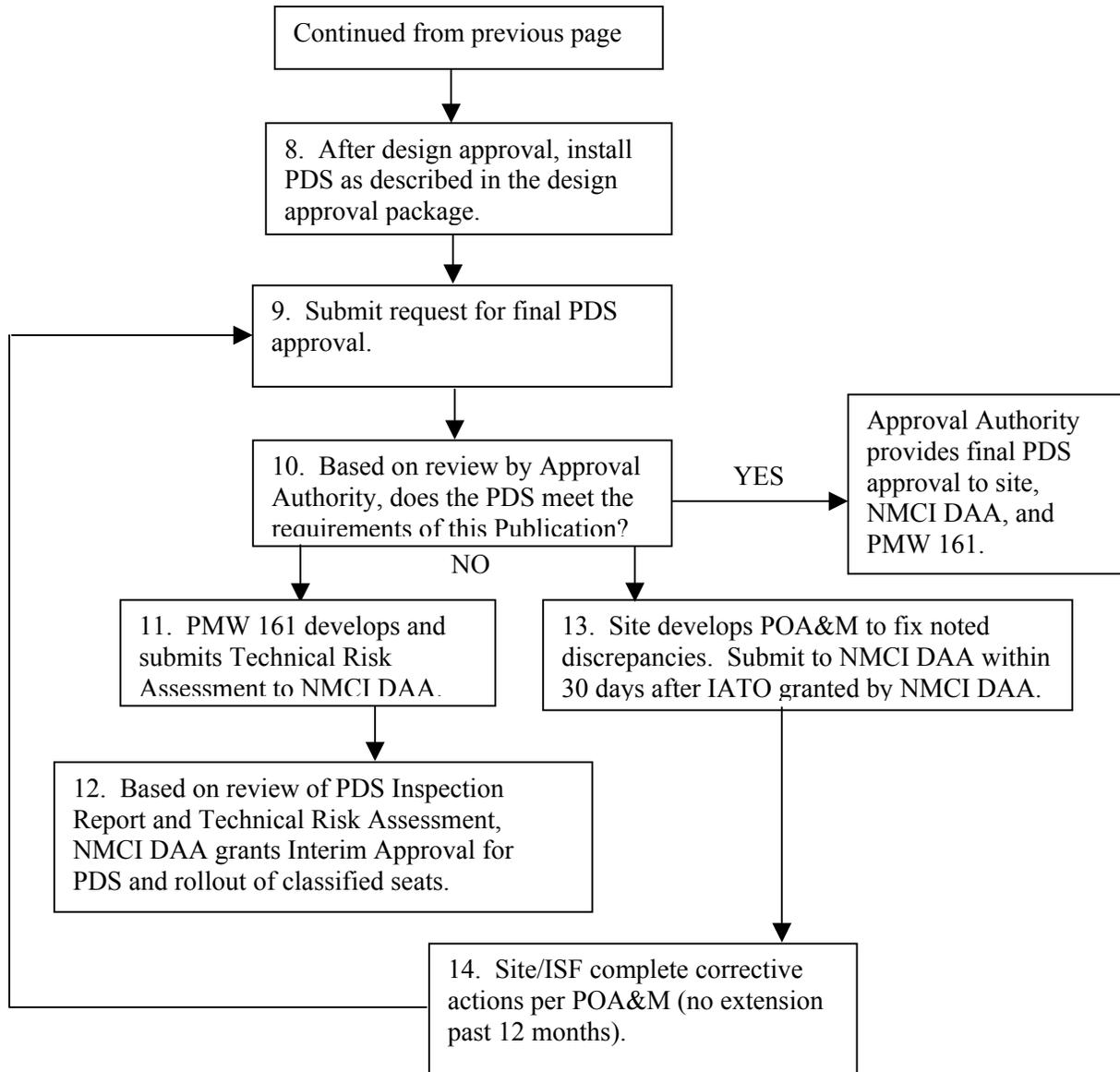


Figure C.2-1. PDS Approval Process Flowchart – Continued

C.2.1 Determine Types of Areas

In order to determine the category of the PDS required, the types of areas the PDS traverses must be identified. The PDS may traverse a Secure Room, Controlled Access Area (CAA), Restricted Access Area (RAA), or Limited Access Area (LAA). The PDS may not traverse an Uncontrolled Access Area (UAA). Also, the PDS must terminate in a Secure Room, CAA, or RAA. It is recommended that the site's Physical Security Officer identify the area designations.

C.2.2 Determine the Category

The category of PDS required for a PDS installed within the U.S. and its territories, or within a LOW threat environment overseas, is determined from OPNAV P-5239-22. The category of PDS required for a PDS installed within a MEDIUM threat environment outside the U.S. is determined from OPNAV P-5239-22.

C.2.3 Select the Type of PDS Carrier

If a Category II PDS is required, select a hardened, buried, suspended, alarmed, or continuously viewed carrier based on physical parameters of the area the PDS traverses, the location of PDS terminations, and cost of implementation.

C.2.4 Develop PDS Design Documentation

The design for the proposed PDS will now be developed (with reference to the PDS Design Template) based on the coordination between site government and ISF POCs and PDS Inspector, and the decisions made in the previous steps.

C.2.5 Submit Approval Request for Design Approval

The ISF submits a PDS Approval Request (PDS drawing package) for technical/design approval to the Approval/Technical Review Authority. The Approval Request shall be submitted before beginning installation to avoid potentially costly revisions and/or unnecessary installations.

C.2.6 Install PDS

After design approval, install the PDS as described in the approved design package. It is recommended that the site ISSM, Physical Security Manager, and PDS originator periodically inspect the installation to verify installation in accordance with the design. If design changes must be made during the installation phase, the Approval Authority should be contacted to ensure continued compliance.

C.2.7 Submit Request for Final Approval

After completion of the PDS, request a final approval. The approval request should reference the approved design and include verification by the site ISSM that the PDS was installed in accordance with the design. An inspection will be performed by an individual designated by the Approval Authority.

C.2.8 Final PDS Approval

If the PDS complies with the approved design and the requirements of Information Assurance (IA) Pub 5239-22, the PDS will be approved. If not, the Approval Authority, in coordination with the PMW 161 and NMCI DAA, will determine if the identified discrepancies must be corrected immediately or if Interim Approval is appropriate. If Interim Authority is decided, a POA&M will be developed to address the correction of identified discrepancies within a period not to exceed 12 months.

C.2.9 PDS IATO (i.e., Interim Approval)

Based on the PDS Inspection Report and a PMW 161 Technical Risk Assessment, PMW 161 will forward an IATO request for the PDS to the NMCI DAA for approval.

C.2.10 Develop and Submit POA&M

Development of the POA&M shall be coordinated between site government, ISF POCs, and PDS Inspector. They will provide a set of corrective actions to be taken so the identified discrepancies will be corrected and the PDS will meet all the stipulations of the IA Pub and approved design. The POA&M will be submitted to the NMCI DAA within 30 days after NMCI DAA granting PDS IATO. The identity of the individual responsible for monitoring the execution of the POA&M and providing periodic reports to both the Approval Authority and the DAA will be identified in the POA&M.

C.2.11 POA&M Actions Completed

When the requirements of the POA&M have been completed within the approved timeline, the steps in OPNAV P-5239-22, Sections 5.2.9 and 5.2.10, will be followed. The Site ISSM will verify in writing when discrepancies have been corrected.

If time remains in the 12-month period the DAA can determine if the POA&M will be revised to allow completion within the 12-month period. PDS IATOs will not be extended beyond the 12-month period that begins on the initial date of the IATO.

PDS Approval Request Form: See OPNAV Pub 5239.22.