

Protected Distribution Systems

Student Guide

February 2024

Center for Development of Security Excellence

Lesson 1: Course Introduction

Introduction

Course Overview

Welcome to the Protected Distribution Systems course. Protected Distribution Systems (PDSs) are used to protect unencrypted national security information (NSI) that is transmitted via wire line or optical fiber. PDSs are one solution to safeguarding classified information.

But who is responsible for a PDS, and what are the requirements for approving, installing, and inspecting a PDS? This course addresses the PDS requirements for all DOD Components.

Course Objectives

Here are the course objectives. Take a moment to review them.

- Describe a Protected Distribution System (PDS)
- Describe the PDS category selection process
- Identify the roles and responsibilities, standards, and procedures applicable during the complete PDS lifecycle

Lesson 2: Overview of the PDS

Introduction

Objectives

This lesson introduces:

- The Protected Distribution System (PDS)
- Categories and carrier types
- What affects PDS category selection

Here are the lesson objectives. Take a moment to review them.

- Describe the purpose of a PDS
- Describe the categories of PDS
- Describe the types of PDS
- Describe how the data type parameter, threat environment, and access area type affect the PDS category selection process

Policy Guidance

The Committee on National Security Systems Instruction (CNSSI) No. 7003 provides guidance and standards for Protected Distribution Systems. The guidance was issued under the authority of National Security Directive 42: National Policy for the Security of National Security Telecommunications and Information Systems. It supersedes the National Security Telecommunications and Information Systems Security Instruction (NSTISSI) 7003, Protected Distribution Systems, dated 13 December 1996.

You may access the CNSSI No. 7003 via the [Course Resources](#) page.

Purpose and Categories

Purpose

The purpose of a PDS is to protect unencrypted national security information (NSI) that is transmitted via wire line or optical fiber. Because the NSI is unencrypted, the PDS must provide safeguards to deter exploitation. The emphasis is on intrusion detection rather than prevention of penetration.

A PDS is intended primarily for use in low and medium threat locations, and is not recommended for use in high or critical threat locations. It is also NOT PERMITTED in uncontrolled access areas. For those areas, you must use an Authorizing Official (AO) approved encryption solution instead.

Categories

There are two categories of PDS.

Category 1 provides a reduced level of security and is used in more secure environments. There is a single type of carrier for a Category 1 PDS. It is called a simple carrier, and it is constructed of metal or polyvinyl chloride pipe—at least schedule-40 grade—or utilizes armored cable. This type of construction can be installed at reduced costs.

A Category 2 PDS provides more significant physical levels of security protection and has five types of carriers:

- A hardened carrier is constructed of a ferrous metal, such as ferrous electrical metallic tubing, ferrous pipe conduit, or ferrous rigid sheet metal ducting. It is normally used between controlled access areas (CAAs) in the same building.
- A buried carrier is used between CAAs located in different buildings.
- A suspended carrier can be used for short runs when it is not practical to bury the carrier between buildings.
- An alarmed carrier is used when it is not practical to perform required daily inspections.
- A continuously viewed carrier can be used within an area that is already under constant surveillance for physical security reasons.

Selecting a PDS Category

The guidance for selecting a Category 1 or Category 2 PDS is based on three factors.

The first is the classification or type of data (Confidential, Secret, Top Secret, and Sensitive Compartmented Information) that is being handled.

The second is the area through which the PDS is installed, whether low threat or medium threat. A PDS is NOT recommended for use in high or critical threat locations. Use of a PDS in high and critical threat locations must be approved by the AO prior to design. Note that the AO is responsible for determining the threat environment. The AO will consult with the Certified Tempest Technical Authority and counterintelligence authority responsible for providing counterintelligence risk assessment.

The third factor is the type of access area in which the PDS is installed, whether in a CAA with the highest restriction of unauthorized access or in a limited access area (LAA) where exploitation is considered unlikely. Recall that PDS usage is not permitted for an uncontrolled access area (UAA). Data passing through UAAs must be encrypted.

Access Areas

CNSSI No. 7003 specifically defines controlled access area, limited access area, and uncontrolled access area.

Term	Definition
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.
Limited Access Area (LAA)	The space surrounding a PDS within which PDS exploitation is not considered likely or where legal authority to identify and remove a potential exploitation exists.
Uncontrolled Access Area (UAA)	The area external or internal to a facility over which no personnel access controls are or can be exercised or any area not meeting the definition of Controlled Access Area (CAA) or LAA.

Table 1

Table 1 from CNSSI No. 7003 defines the category of PDS required for low threat environments. For example, when the access area is controlled, a Category 1 PDS is sufficient. However, when the access area is limited, a Category 2 PDS is required if the data is Secret or higher.

Table 1. Category of PDS required for Low Threat Environments

Type of Data	Type of Access Area			
	Limited	Confidential, Controlled	Secret, Controlled	Top Secret, Controlled
Confidential	1			
Secret	2	1		
Top Secret	2	1	1	
Sensitive Compartmented Information	2	1	1	1

Table 2

Table 2 defines the category of PDS required for medium threat environments.

Note that, with the increase in threat environment to medium, a Category 2 PDS is required for the Confidential Controlled access area when Top Secret or Sensitive Compartmented Information is handled.

Table 2. Category of PDS required for Medium Threat Environments

Type of Data	Type of Access Area			
	Limited	Confidential, Controlled	Secret, Controlled	Top Secret, Controlled
Confidential	1			
Secret	2	1		
Top Secret	2	2	1	
Sensitive Compartmented Information	2	2	1	1

Review Activities

Review Activity 1

What is the purpose and use of a Protected Distribution System (PDS)?

Select all that apply. Check your answer in the Answer Key at the end of this Student Guide.

- ☐ It is used to protect unencrypted National Security Information (NSI).
- ☐ The emphasis is on prevention of penetration.
- ☐ It is intended for use in high or critical threat locations.
- ☐ It is not permitted in uncontrolled access areas.

Review Activity 2

Which Type 2 carrier is used when it is not practical to perform required daily inspections?

Select the best response. Check your answer in the Answer Key at the end of this Student Guide.

- ☐ Hardened
- ☐ Suspended
- ☐ Alarmed
- ☐ Buried

Review Activity 3

Which category of Protected Distribution System (PDS) is appropriate for the following situations?

For each situation, select the best response. Check your answer in the Answer Key at the end of this Student Guide.

The carrier must pass through an uncontrolled access area.

- ☐ Category 1
- ☐ Category 2
- ☐ Neither

A buried PDS connects controlled access areas.

- ☐ Category 1
- ☐ Category 2
- ☐ Neither

A Top Secret PDS in a confidential controlled access area in a low threat environment

- ☐ Category 1
- ☐ Category 2
- ☐ Neither

A Top Secret PDS in a confidential controlled access area in a medium threat environment

- ☐ Category 1
- ☐ Category 2
- ☐ Neither

Lesson 3: Installation Guidance

Introduction

Welcome

Proper Protected Distribution System (PDS) installation is important to ensure the security of unencrypted National Security Information (NSI).

This lesson introduces

- General installation requirements
- Installation guidance for Category 1 and Category 2 carriers
- Installation requirements for pull boxes and other PDS connections
- The requirements for marking a PDS
- The roles and responsibilities for PDS installation, approval, operation, and inspection.

Sections VIII, IX, and X of CNSSI No. 7003 contain detailed installation guidance. You may access the CNSSI No. 7003 via the [Course Resources](#) page.

Objectives

Here are the lesson objectives. Take a moment to review them.

- Identify standards and procedures for PDS installation.
- Identify the roles of Authorizing Official (AO) and the PDS owner for the PDS.

General Installation Guidance

Origination and Termination

There are specific requirements regarding the origination and termination points for a PDS.

A PDS **must** originate in a controlled access area (CAA) that is controlled at the highest level of the data carried by the PDS. For example, if the PDS carries Secret data, the origination point must, at a minimum, be in an access area controlled at the level of Secret.

The PDS **should**, if possible, also terminate in a CAA that is controlled at the highest level of data carried by the PDS. However, if that is not possible, you must ensure that the PDS termination is secured with a lock box and a PDS lock.

PDS Lock

Ensure that all lock boxes use a PDS lock as defined in CNSSI No. 7003.

PDS Lock - A lock required to be resistant to surreptitious manipulation but not required to be resistant to physical penetration or interchangeable with a "high security" lock. A 3-position spin combination lock that meets the requirements of FF-L-2740, *Federal Specification Locks, Combination, Electromechanical*, may be used as an alternative.

Circuits and TEMPEST

Components of a single PDS may use circuits of more than one classification level. For example, one circuit might be Secret while another is Top Secret. However, those circuits must be separated to prevent unauthorized access by those who do not have the appropriate clearance. Access to all points with breakouts must be restricted to personnel cleared at the highest level of the classification carried in the breakout.

If it is necessary to install unclassified data cables within a PDS that is used for classified data lines, the PDS Owner must get prior review and approval from the Certified TEMPEST Technical Authority (CTTA). Furthermore, to protect classified data lines, a CTTA may implement additional TEMPEST countermeasures. Examples of additional countermeasures include: shielding wire or fiber optic lines; grounding metallic PDS; and isolating the PDS with non-conductive sleeves.

TEMPEST is a name referring to the investigation, study, and control of unintentional compromising emanations from telecommunications and automated information systems equipment (CNSSI-4009).

Carriers

General Requirements

Although all carriers have their own specific installation requirements, there are some general overarching guidelines that apply to both Category 1 and Category 2 carriers.

The PDS Owner should install the carrier in plain view, because inspection of the carrier is integral to ensuring the data is not compromised. Installing the carrier above a false ceiling, below a false floor, or inside a wall makes inspection difficult. However, if the PDS Owner can arrange to make those areas inspectable, the PDS approval request must identify that information. When the PDS Owner cannot install the PDS in plain view nor make it inspectable, the PDS must be an alarmed carrier.

Category 1

For a Category 1 PDS, use a simplified carrier to install cables. The carrier must be constructed of either metal or polyvinyl chloride (PVC) pipe of at least a schedule-40 grade.

Otherwise, use an armored cable. For armored carriers, the jacket must be constructed of a flexible metallic material such as copper, aluminum, or steel. Some armored cables are not constructed of a solid continuous material, such as those that use interlocking spiral segments. In this case, the metallic material must have an overall, continuous plastic sheath.

Category 2

Recall that there are five types of Category 2 carriers: hardened, buried, suspended, alarmed, and continuously viewed.

Hardened

When installing a hardened carrier, be aware of: the requirements for construction materials; the requirements on how and where to mount the carrier; and the requirements that apply when a carrier needs to pass through a void.

Construction Materials:

- Hardened carriers must be constructed of a ferrous material, namely, ferrous, electrical metallic tubing (EMT), ferrous pipe conduit, or ferrous rigid sheet metal ducting.
- Do not use flexible conduits or armored cables as a hardened carrier.

Mounting:

- To facilitate unobstructed visual inspections, allow for a clearance of at least one inch from walls, floors, ceilings, other conduits, or any object that would interfere with visual inspection.
- You may flush mount the carrier to a surface only if the surface consists of at least four inches of reinforced concrete or the equivalent.

Traversing a Void:

- If the carrier traverses a void, such as a hollow wall, ceiling, or floor, the carrier must traverse through the center of an inspection port that has a diameter greater than the carrier size plus 10 centimeters (4 inches).
- If the void is greater than 15 centimeters (6 inches) thick, the inspection port diameter must increase to the size of the carrier plus 20 centimeters (8 inches).
- Inspection ports where the PDS starts and terminates in the CAA are not typically required, but the AO will make that determination.

- Construction requirements based on Fire Codes take precedence over PDS construction requirements, but should be documented in the PDS plan.

As a final note, if the carrier connects two controlled access areas by passing through an uncontrolled access area (UAA), data in the carrier passing through the UAA must be encrypted.

Buried

Installing a buried carrier has its own set of requirements for: construction materials, permissible locations, how deep to bury it, and how to secure access to the buried carrier.

Construction Material:

- The carrier must be constructed of electrical metallic tubing (EMT), rigid pipe, polyvinyl chloride (PVC), or a similar type of plastic electrical conduit.

Location:

- Before you bury the carrier, be sure the property is owned or leased by the U.S. Government or the U.S. contractor that controls the PDS.

Depth:

- How deep you have to bury the carrier depends on the threat designation for the specific location.
- For low threat locations, bury the carrier one meter below the surface. A lesser depth may be used within a low threat area with prior approval if the carrier is encased within the center of mass of approximately 20 centimeters (8 inches) of concrete.
- If you run into a blocked passage, or you can't dig one meter down because of soil conditions, you may use a lesser depth. However, if you use a lesser depth, you must ensure that the carrier is encased in the center of eight inches of concrete.
- For medium threat locations, you must bury the carrier one meter deep AND ensure it is encased within the center of 8 inches of concrete or within an approved concrete and steel container.

Securing Access:

- To secure access to buried carriers, use a PDS lock or alarm for manholes and any other access points.

Suspended

You may use a suspended carrier for short runs when it is not practical to bury the PDS. Hang it directly between buildings and be sure it is elevated at least five meters above the ground.

Before you install it, be sure the property over which it is suspended is owned or leased by the U.S. Government or by a U.S. Government contractor or vendor that controls the PDS.

Terminate the suspended carrier in a controlled access area on each end, or have it immediately enter a hardened PDS at the building boundary.

To facilitate unimpeded inspection, ensure the carrier is clear of any obstruction and that the area where it is suspended is illuminated at night.

Alarmed

Recall that alarmed carriers are used when it is not practical to perform daily inspections.

The carrier itself should be protected by an alarm system that detects attempted penetration of the carrier. Alternatively, the space surrounding the entire carrier may be covered by an area or volumetric alarm system that is approved by the cognizant, physical-security authorities.

The alarm system must be capable of prompt detection of penetration, and the office where the alarm is annunciated must be manned 24/7. Security forces must be able to respond within 15 minutes. The alarm system must transmit a line fault message to the annunciator panel if the system fails. The alarm must also provide protection from tampering and be able to register malfunctions.

Continuously Viewed

For a continuously viewed carrier, ensure the area where the carrier is installed is under observation 24/7, including when the area is not operational. Security personnel must investigate the area of attempted penetration within 15 minutes of discovery.

Pull Boxes and Other Connections

Pull Boxes

Connections for carriers are necessary for the PDS; however, it is important to minimize the use of pull boxes, conduit joints, and other types of connections.

Do NOT use pull boxes with pre-punched knockouts.

Construction materials for pull boxes depend on the threat area. If you are in a low threat area, use a ferrous metal with a minimum thickness of 16 gauge. If you are in a medium threat area, use a ferrous metal with a minimum thickness of 14 gauge. Note that 14 gauge metal is thicker than 16 gauge metal.

If the pull box does not require opening after installation:

- Secure the cover to the box by welding it or applying epoxy.
- If you weld it, there must be at least one weld on each side of the box and cover.
- If you use epoxy, apply it between all mating surfaces continuously around the cover.

The requirements for pull boxes that need to be accessed after installation are as follows.

- The hinge pins for pull box covers should be either internal or non-removable.
- If you use a hasp to secure the cover, permanently and securely attach the hasp to the box.
- Secure the cover with an approved PDS lock or tamper evident seal.

Other Connections

For connections other than pull boxes, permanently seal the connections around all surfaces either by welding, epoxy, or fusion. Seal all seams if there is more than one seam in the connection. The seal must provide a mechanical bond between the components of the carrier and must be visible for inspection.

For epoxy seals, use a thick opaque material.

Do NOT use couplers that are secured with a set screw.

For hardened carriers, connections such as elbows, couplings, and nipples must be of the same material as the carrier.

Markings

Markings

Clearly mark the PDS to make it easily identifiable to the inspector. You may use tape, paint, cable tags, or any other suitable method. Place the markings at 3 meter intervals or less. However, do not indicate on the label that this is a PDS or that it carries National Security Information (NSI).

Also, do not paint a PDS in its entirety. This is to prevent someone from tampering with the PDS and masking the tampered PDS with paint. If there are environmental concerns

regarding the integrity of the PDS due to accelerated corrosion, PDS can be purchased with factory painted coating. This option should be used instead of the PDS Owner applying paint as that would require a waiver by the Authorizing Official (AO).

In addition, do not use red markings, as red is typically used to identify fire sprinkler systems. For example, white tape may be used to mark the PDS.

Responsibilities and the Approval Process

Responsibilities

Now let's discuss the roles and responsibilities for PDS installation, approval, operation, and inspection.

The basic responsibilities for the PDS are shared by the Authorizing Official (AO) and the PDS Owner.

The AO is responsible for PDS approval, certification, and recertification. The AO also must approve reactivation of a PDS. Note that the PDS has its own approval. The assessment and authorization for the PDS can either be separate from or combined with the Assessment and Authorization (A&A) for systems and networks. Each AO may define the specific approval process to be utilized.

The PDS owner is responsible for the installation and maintenance of the PDS.

Next, look at how these responsibilities play out in the PDS approval process.

The Approval Process

All PDS requests must go through an approval process.

The PDS owner originates the request. Counterintelligence (CI) personnel are responsible for conducting a CI risk assessment to assess the potential risk of exploitation. The PDS approval request describes the specifics of the PDS, including unique facts regarding the facility, installation details, inspection methods, and schedule. The PDS owner must develop a Standard Operating Procedure (SOP) to ensure proper installation, maintenance, operation, and inspection of the PDS and submit the SOP as part of the approval documentation.

The request undergoes technical review and must be approved by the AO BEFORE the procurement of materials.

The PDS owner is then responsible for installing the PDS. Note that during construction, temporary configurations used to test the operation of data lines, or the network, do not require technical review. The AO must validate that the PDS configuration meets the Temporary Configuration criteria. Use of a validated temporary configuration must be approved by the responsible AO.

When installation is complete, the AO must ensure the PDS installation, and any associated documentation, is assessed for compliance to CNSSI No. 7003 prior to initial operation.

The PDS owner is responsible for the operation, maintenance, and inspection of the PDS.

CI Risk Assessment

CNSSI No. 7003 lists these factors to consider at a minimum in the CI risk assessment.

NOTE: The information in the box below will not be on the test but is included here as additional information that may provide useful background and insight.

- a. Foreign or domestic location.
- b. Use of U.S. citizens for 24/7 access control.
- c. Use of U.S. procured, installed, and monitored intrusion detection devices.
- d. Presence of uncleared personnel or foreign nationals in, on, or nearby the controlled facility/compound.
- e. Existence of any co-located, unaffiliated tenants in the facility.
- f. Proximity of the PDS to other infrastructure requiring maintenance.
- g. Any use or dependency on contracted security for intrusion detection/reporting/response.
- h. Stand-off distance from the PDS to the perimeter of the controlled area.
- i. Proximity of the PDS to uncontrolled buildings and structures beyond the perimeter and the nationality of tenants of those buildings.
- j. Known human intelligence (HUMINT) and technical threat (capabilities, intentions, and activities) of the host nation.
- k. Known history of foreign host and foreign intelligence security services (FISS) capabilities and activities to exploit PDS, fiber optics, and communications closets.

Temporary Configuration

CNSSI No. 7003 specifically defines Temporary Configuration.

Temporary configurations are those which are in place for less than 30 calendar days and are confined within USG installations in areas that are not accessible to the general public, and do not process higher than Secret collateral information.

Modification, Deactivation, and Reactivation

Now consider the responsibilities for modifying, deactivating, or reactivating an approved PDS.

Before a PDS can be modified, the PDS owner must submit a request for modification to the AO and the AO must approve the modification. After the PDS is modified, it must be recertified by the AO. If a PDS needs to be deactivated, the PDS owner must notify the AO within 30 days of the deactivation. Before the PDS can be reactivated, the PDS owner must request reactivation from the AO and the AO must approve the reactivation.

Note that, both modification and reactivation may require an additional onsite assessment.

Review Activities

Review Activity 1

When possible, where should carriers for Category 1 and Category 2 Protected Distribution Systems (PDSs) be installed?

Select the best response. Check your answer in the Answer Key at the end of this Student Guide.

- ☐ Above false ceilings, below false floors, or inside walls
- ☐ In plain view
- ☐ Buried 1 foot or elevated 5 feet
- ☐ In darkened areas

Review Activity 2

Do the statements describe a carrier requirement for a Category 1 or Category 2 Protected Distribution System (PDS)?

For each item, select the best response. Check your answer in the Answer Key at the end of this Student Guide.

Carrier is constructed of metal or PVC pipe or armored cable.

- ☐ Category 1
- ☐ Category 2

Carrier is constructed of ferrous pipe conduit.

- ☐ Category 1
- ☐ Category 2

Carrier is buried 1 meter below property owned by the U.S. Government.

- ☐ Category 1
- ☐ Category 2

Carrier is protected by an alarm system.

- ☐ Category 1
- ☐ Category 2

Review Activity 3

Select True or False for each statement. Check your answer in the Answer Key at the end of this Student Guide.

The PDS should maximize the use of pull boxes, conduit joints, and other types of connections.

- ☐ True
- ☐ False

If a pull box will be accessed after installation, the cover must be secured with a PDS lock or tamper evident seal.

- ☐ True
- ☐ False

When epoxy is used to seal connections, a thick clear material must be used.

- ☐ True
- ☐ False

Review Activity 4

How should a Protected Distribution System (PDS) be marked to make it easily identifiable to the inspector?

Select all that apply. Check your answer in the Answer Key at the end of this Student Guide.

- ☐ Use paint, tape, or cable tags.
- ☐ Clearly indicate PDS on the label.
- ☐ Red is the preferred labeling color.
- ☐ Markings should be spaced 3 meters or less.

Review Activity 5

Who is responsible for these activities?

For each activity, select the best response. Check your answer in the Answer Key at the end of this Student Guide.

Ensure PDS is inspected and certified prior to initial operation

- ☐ PDS Owner
- ☐ Authorizing Official (AO)

Operation, maintenance, and inspection of PDS

- ☐ PDS Owner
- ☐ Authorizing Official (AO)

Installation of PDS

- ☐ PDS Owner
- ☐ Authorizing Official (AO)

Approving reactivation of a PDS

- ☐ PDS Owner
- ☐ Authorizing Official (AO)

Lesson 4: Inspection Guidance

Introduction

Welcome

Inspections are integral to protecting National Security Information (NSI) carried by the Protected Distribution system (PDS).

This lesson introduces requirements for visual inspections and technical inspections, as well as the requirements for alarm system verification.

CNSSI No. 7003 provides detailed guidance for PDS inspection in Section XI. You may access the CNSSI No. 7003 via the [Course Resources](#) page.

Objective

Here is the lesson objective. Take a moment to review.

- Describe requirements to perform PDS inspections (Visual Inspection Requirements, Technical Inspections Requirements, and Alarm System Inspection Requirements)

Inspections Overview

Introduction to Inspections

Because the PDS provides intrusion detection, rather than intrusion prevention, inspections are integral to protecting the National Security Information (NSI) carried by the PDS. The required frequency of inspections depends on the type of data carried and the threat environment. CNSSI No. 7003 requires that you log all inspections with the date and time of the inspection and the name and title of the inspector. Maintain the log for at least one year.

When an incident of tampering, penetration, or unauthorized interception occurs, the incident must be reported immediately to all organizations that use the PDS and to the local security authority. Until the incident can be assessed, and security status determined, the PDS should not be used. If this is not practical, users should limit use to the greatest extent possible.

There are two types of PDS inspections required: Technical and Visual. Technical inspections are required for all PDS, and visual inspections are required for most PDS. If the PDS is an alarmed carrier, the alarm system performance must be verified. The frequency in which the system performance must be verified depends on the type of information being transmitted.

Visual Inspections

Introduction to Visual Inspections

Visual inspections are required for most PDS except PDS transmitting Confidential data in a Low threat area, alarmed carriers, and continuously viewed carriers. The visual inspection must be performed by persons who are trained, in accordance with organizational policy, to recognize physical changes and attempts at penetration and tampering.

When performing a visual inspection, look at everything. Inspect all along the entire length of the conduit or buried carrier. Extend inspection at least five meters on each side of buried carriers. Inspect all carrier connections, boxes, locks, and seals. Don't forget to look through inspection ports when the PDS traverses a void.

Is anything amiss? Look for signs of penetration, tampering, or any other anomalies. Ensure you have adequate lighting, and inspect from a distance that allows you to detect any attempts at intrusion.

Table 3

Table 3 from CNSSI No. 7003 provides the visual inspection schedule. Visual inspections are random and daily, and the frequency depends on the highest classification of data carried and the threat area. For example, in medium threat areas, a visual inspection may be required once, twice, or four times daily depending on the highest classification of data carried.

Table 3. Visual Inspection Schedule

Highest Classification of Data Carried	Random Inspections <i>Per Day</i>	
	<i>Low Threat Area</i>	<i>Medium Threat Area</i>
Confidential	None	One
Secret	One	Two
Top Secret or Sensitive Compartmented Information	Two	Four

Technical Inspections

Introduction to Technical Inspections

The technical inspection must be performed by persons trained, in accordance with organizational policy, to recognize physical changes that indicate attempts at penetration and tampering, as well as changes in technical aspects such as bypass circuitry, attachment or removal of devices, and suspicious signal levels.

Technical inspectors:

- Visually and physically verify the integrity of the PDS carrier, whether conduit or buried path
- Inspect all connections, pull boxes, and terminal boxes
- Use hand-held mirrors, if needed, to inspect all sides of the carrier and boxes
- Open and inspect all pull boxes and terminal boxes that are not permanently sealed
- Verify lock combination numbers, lock serial numbers, and tamper-seal serial numbers
- Verify the mechanical security of connections and covers

Initial Technical Inspection

An initial technical inspection must be performed prior to approval of PDS operation.

After approval, technical inspections must be performed at random intervals at a frequency determined by data classification and threat environment.

The initial inspection documents the path of the PDS, the locations of all pull boxes, and locations for all conduit joints at intervals less than the length of conduit segments (typically 10 feet). The PDS may be documented using detailed “as-built” installation drawings or photographs.

At subsequent technical inspections, the inspector verifies the path of the PDS and the location of pull boxes and joints.

When test equipment is locally available and resident expertise allows, the initial inspection must also measure and record the electrical characteristics of the PDS lines to obtain a baseline electrical profile of the PDS.

Then, at subsequent technical inspections, the inspector makes a comparison to the baseline to identify possible tampering attempts.

Table 4

Table 4 from CNSSI No. 7003 provides the technical inspection schedule.

Inspections are random and annual, and the number of inspections per year depends on the highest classification of data carried and the threat environment. Low threat environments require one random annual inspection for all data classifications. For medium threat environments, a technical inspection must be performed once, twice, or four times annually depending on the highest classification of data carried.

Table 4. PDS Technical Inspection Schedule

Highest Classification of Data Carried	Random Inspections <i>Per Year</i>	
	Low Threat Environment	Medium Threat Environment
Confidential	One	One
Secret	One	Two
Top Secret or Sensitive Compartmented Information	One	Four

Alarm System Verification

Introduction to Alarmed Carriers Verification

When daily visual inspections of a PDS are not practical, an alarmed carrier must be used. Each separate alarm section or zone must be verified.

The Standard Operating Procedure (SOP) for each alarmed carrier must be implemented to do the following:

- Verify the performance for the alarmed carriers at the required scheduled intervals
- Ensure that the response by security personnel in the area of the possible attempted penetration is within 15 minutes of discovery
- Provide for inspection of the PDS to determine the cause of the alarm
- Define the action to be taken regarding termination of transmission
- Initiate an investigation of any attempt at intrusion.

Table 5

Table 5 from CNSSI No. 7003 provides the PDS Alarm Circuit Verification Schedule. Note that a PDS may have more than one alarmed carrier, and those carriers may carry different classifications of data. You must verify the performance for each alarmed carrier. Verify the performance monthly, weekly, or daily depending on the highest classification of data carried.

Table 5. PDS Alarm Circuit Verification Schedule

Highest Classification of Data Carried	Interval
Confidential	Monthly
Secret	Weekly
Top Secret or Sensitive Compartmented Information	Daily

Review Activities

Review Activity 1

For which of the following types of carriers are visual inspections usually required?

Select all that apply. Check your answer in the Answer Key at the end of this Student Guide.

- ☐ Alarmed carriers
- ☐ Buried carriers
- ☐ Continuously viewed carriers
- ☐ Suspended carriers

Review Activity 2

The required frequency for random daily visual inspections depends on which of the following?

Select all that apply. Check your answer in the Answer Key at the end of this Student Guide.

- ☐ How deep the carrier is buried
- ☐ The classification of data carried
- ☐ The threat area
- ☐ The number of pull boxes and connections

Review Activity 3

Which of the following are required for technical inspections?

Select all that apply. Check your answer in the Answer Key at the end of this Student Guide.

- ☐ Open and inspect inside pull boxes that are not permanently sealed
- ☐ Verify lock combination numbers, lock serial numbers, and tamper-seal serial numbers
- ☐ Verify the mechanical security of connections and covers
- ☐ Determine the cause of the alarm

Review Activity 4

How frequently must the performance of each alarmed carrier be verified?

Select the best response. Check your answer in the Answer Key at the end of this Student Guide.

- ☐ Once, twice, or four times annually depending on the threat environment
- ☐ Monthly, weekly, or daily depending on the classification of data carried
- ☐ Once before operation is approved, and at random intervals subsequently
- ☐ Once, twice, or four times daily depending on the classification of data and the threat environment

Lesson 5: Course Conclusion

Conclusion

Course Summary

In this course you learned about Protected Distribution Systems (PDSs) and who is responsible for them.

You learned about the requirements for:

- Approving the use of a PDS
- Installing a PDS
- Inspecting a PDS

The course addressed the PDS requirements for all DOD Components.

Objectives

Congratulations. You have completed the Protected Distribution Systems course.

You should now be able to perform all of the listed activities.

- Describe a Protected Distribution System (PDS)
- Describe the PDS category selection process
- Identify the roles and responsibilities, standards, and procedures applicable during the complete PDS lifecycle

To receive course credit, you must take the *Protected Distribution Systems* examination. Please use the Security Training, Education, and Professionalization Portal (STEPP) system from the Center for Development of Security Excellence to register for the online exam.

Appendix A: Answer Key

Lesson 2 Review Activities

Review Activity 1

What is the purpose and use of a Protected Distribution System (PDS)?

- ☒ It is used to protect unencrypted National Security Information (NSI). (*correct response*)
- ☐ The emphasis is on prevention of penetration.
- ☐ It is intended for use in high or critical threat locations.
- ☒ It is not permitted in uncontrolled access areas. (*correct response*)

Feedback: A PDS is used to protect unencrypted NSI with an emphasis on intrusion detection rather than prevention of penetration. It is intended for use in low and medium threat locations and is not permitted in uncontrolled access areas.

Review Activity 2

Which Type 2 carrier is used when it is not practical to perform required daily inspections?

- ☐ Hardened
- ☐ Suspended
- ☒ Alarmed (*correct response*)
- ☐ Buried

Feedback: An alarmed carrier is used when it is not practical to perform required daily inspections.

Review Activity 3

Which category of Protected Distribution System (PDS) is appropriate for the following situations?

The carrier must pass through an uncontrolled access area.

- ☐ Category 1
- ☐ Category 2
- ☒ Neither (*correct response*)

Feedback: Neither category may be used. A PDS may not be used for an uncontrolled access area (UAA). Data passing through UAAs must be encrypted.

A buried PDS connects controlled access areas.

- ☐ Category 1
- ☒ Category 2 (*correct response*)
- ☐ Neither

Feedback: A buried PDS is considered a Category 2 PDS.

A Top Secret PDS in a confidential controlled access area in a low threat environment

- ☒ Category 1 (*correct response*)
- ☐ Category 2
- ☐ Neither

Feedback: A Category 1 may be used in this situation.

A Top Secret PDS in a confidential controlled access area in a medium threat environment

- ☐ Category 1
- ☒ Category 2 (*correct response*)
- ☐ Neither

Feedback: A Category 2 is needed for this situation.

Lesson 3 Review Activities

Review Activity 1

When possible, where should carriers for Category 1 and Category 2 Protected Distribution Systems (PDSs) be installed?

- ☐ Above false ceilings, below false floors, or inside walls
- ☒ In plain view (*correct response*)
- ☐ Buried 1 foot or elevated 5 feet
- ☐ In darkened areas

Feedback: The carrier should be installed in plain view, as inspection of the carrier is integral to ensuring data is not compromised.

Review Activity 2

Do the statements describe a carrier requirement for a Category 1 or Category 2 Protected Distribution System (PDS)?

Carrier is constructed of metal or PVC pipe or armored cable.

- ☒ Category 1 (*correct response*)
- ☐ Category 2

Feedback: A carrier for a Category 1 PDS must be constructed of metal PVC pipe of at least a schedule-40 grade or armored cable.

Carrier is constructed of ferrous pipe conduit.

- ☐ Category 1
- ☒ Category 2 (*correct response*)

Feedback: A Category 2 hardened carrier must be constructed of ferrous EMT, ferrous pipe conduit, or ferrous rigid sheet metal ducting.

Carrier is buried 1 meter below property owned by the U.S. Government.

- ☐ Category 1
- ☒ Category 2 (*correct response*)

Feedback: A buried cable is used for a Category 2 PDS.

Carrier is protected by an alarm system.

- ☐ Category 1
- ☒ Category 2 (*correct response*)

Feedback: An alarmed carrier is for a Category 2 PDS.

Review Activity 3

Select True or False for each statement.

The PDS should maximize the use of pull boxes, conduit joints, and other types of connections.

- ☐ True
- ☒ False (*correct response*)

Feedback: The PDS should MINIMIZE the use of pull boxes and other connections.

If a pull box will be accessed after installation, the cover must be secured with a PDS lock or tamper evident seal.

- ☒ True (*correct response*)
- ☐ False

Feedback: The statement is true. The cover must be secured with an approved PDS lock or tamper evident seal.

When epoxy is used to seal connections, a thick clear material must be used.

- ☐ True
- ☒ False (*correct response*)

Feedback: The epoxy must be a thick OPAQUE material so that it is clearly visible.

Review Activity 4

How should a Protected Distribution System (PDS) be marked to make it easily identifiable to the inspector?

- ☒ Use paint, tape, or cable tags. (*correct response*)
- ☐ Clearly indicate PDS on the label.
- ☐ Red is the preferred labeling color.
- ☒ Markings should be spaced 3 meters or less. (*correct response*)

Feedback: Tape, paint, or cable tags may be used and should be placed at 3 meter intervals or less. Never label the PDS as a PDS, and do not use red, as red is reserved for fire sprinkler systems. (Note that while marking a PDS with paint to be easily seen is acceptable, in most situations a PDS should NOT be painted in its entirety.)

Review Activity 5

Who is responsible for these activities?

Ensure PDS is inspected and certified prior to initial operation

- ☐ PDS Owner
- ☒ Authorizing Official (AO) (*correct response*)

Feedback: The AO must ensure the PDS is inspected and certified prior to initial operation.

Operation, maintenance, and inspection of PDS

- ☒ PDS Owner (*correct response*)
- ☐ Authorizing Official (AO)

Feedback: The PDS Owner is responsible for the operation, maintenance, and inspection of the PDS.

Installation of PDS

- ☒ PDS Owner (correct response)
- ☐ Authorizing Official (AO)

Feedback: The PDS Owner is responsible for the installation of the PDS.

Approving reactivation of a PDS

- ☐ PDS Owner
- ☒ Authorizing Official (AO) (correct response)

Feedback: Before a PDS can be reactivated, the AO must approve the reactivation.

Lesson 4: Review Activities

Review Activity 1

For which of the following types of carriers are visual inspections usually required?

- ☐ Alarmed carriers
- ☒ Buried carriers (correct response)
- ☐ Continuously viewed carriers
- ☒ Suspended carriers (correct response)

Feedback: Visual inspections are required for most PDS carriers except PDS transmitting Confidential data in a Low threat area, alarmed carriers, and continuously viewed carriers.

Review Activity 2

The required frequency for random daily visual inspections depends on which of the following?

- ☐ How deep the carrier is buried
- ☒ The classification of data carried (correct response)
- ☒ The threat area (correct response)
- ☐ The number of pull boxes and connections

Feedback: The frequency of random daily visual inspections depends on the highest classification of data carried and the threat area.

Review Activity 3

Which of the following are required for technical inspections?

- ☒ Open and inspect inside pull boxes that are not permanently sealed (*correct response*)
- ☒ Verify lock combination numbers, lock serial numbers, and tamper-seal serial numbers (*correct response*)
- ☒ Verify the mechanical security of connections and covers (*correct response*)
- ☐ Determine the cause of the alarm

Feedback: *Technical inspections involve opening and inspecting inside pull boxes, verifying lock combination numbers and serial numbers, and verifying the mechanical security of connections and covers.*

Review Activity 4

How frequently must the performance of each alarmed carrier be verified?

- ☐ Once, twice, or four times annually depending on the threat environment
- ☒ Monthly, weekly, or daily depending on the classification of data carried (*correct response*)
- ☐ Once before operation is approved, and at random intervals subsequently
- ☐ Once, twice, or four times daily depending on the classification of data and the threat environment

Feedback: *The performance for each alarmed carrier must be verified monthly, weekly, or daily depending on the highest classification of data carried.*