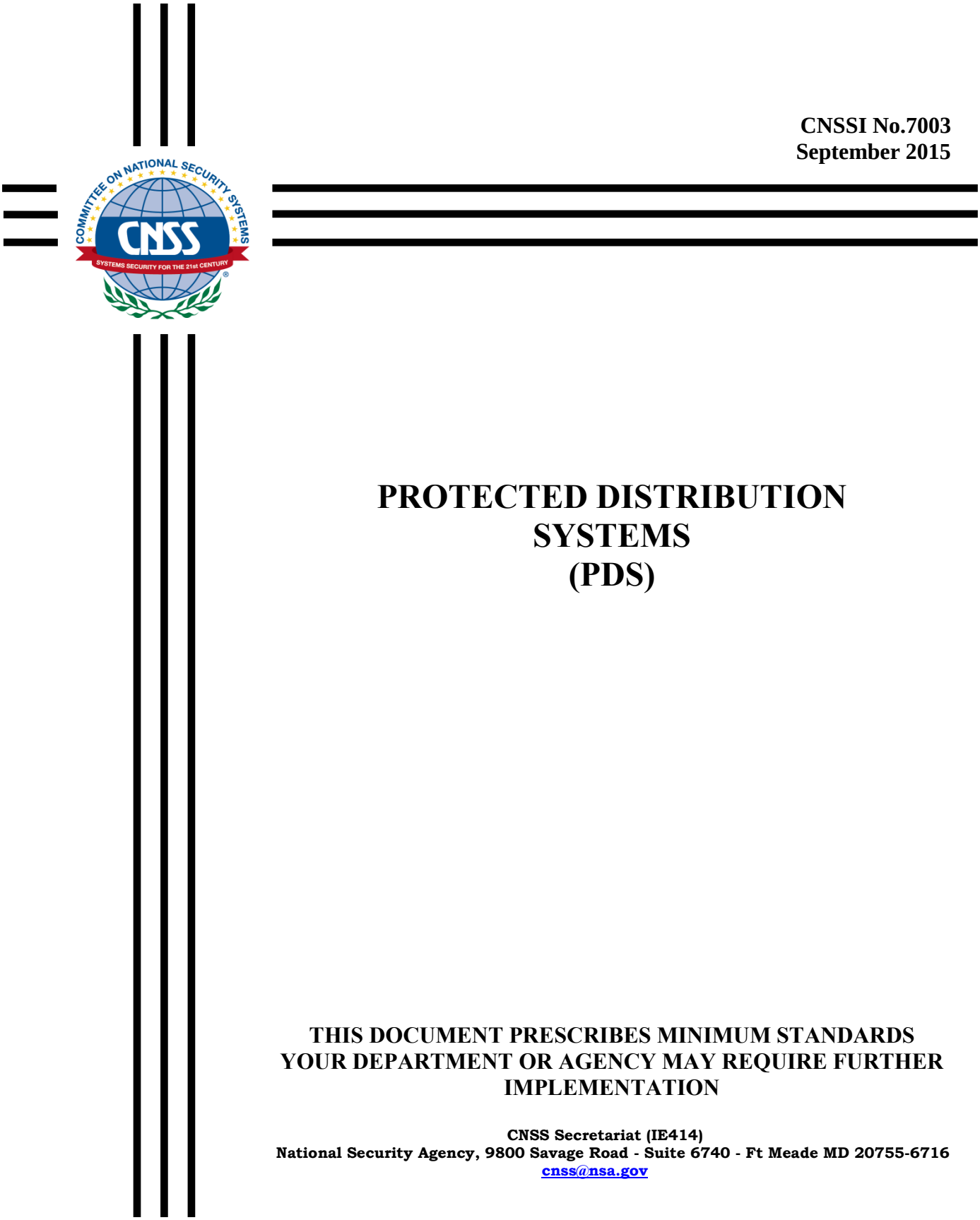

CNSSI No.7003
September 2015

PROTECTED DISTRIBUTION SYSTEMS (PDS)

THIS DOCUMENT PRESCRIBES MINIMUM STANDARDS
YOUR DEPARTMENT OR AGENCY MAY REQUIRE FURTHER IMPLEMENTATION

CNSS Secretariat (IE414)
National Security Agency, 9800 Savage Road - Suite 6740 - Ft Meade MD 20755-6716
cnss@nsa.gov

THIS PAGE INTENTIONALLY LEFT BLANK

NATIONAL MANAGER

FOREWORD

1. The Committee on National Security Systems (CNSS) issues this Instruction pursuant to its authority under *National Security Directive 42, National Policy for the Security of National Security Telecommunications and Information Systems.* This Instruction provides guidance and requirements for the approval and installation of wire line and optical fiber distribution systems used to protect unencrypted, National security information (NSI) through areas of lesser classification or control.

2. This Instruction supersedes National Security Telecommunications and Information Systems Security Instruction (NSTISSI) 7003, *Protected Distribution Systems*, dated 13 December 1996.

3. Additional copies of this Instruction may be obtained from the CNSS Secretariat or the Committee on National Security Systems website: www.cnss.gov.

FOR THE NATIONAL MANAGER:

/s/
CURTIS W. DUKES

TABLE OF CONTENTS

SECTION **PAGE**

ANNEX

PROTECTED DISTRIBUTION SYSTEMS (PDS)

SECTION I - PURPOSE

1. This Instruction stipulates guidance and standards for the design, installation, and maintenance of PDS. This Instruction incorporates a philosophy of "risk management" in lieu of a "risk avoidance". Absent specific facts unique to each facility suggesting greater or lesser risks, these standards shall be applied. This PDS guidance must be followed subject to discretion of the department or agency Authorizing Official (AO) who may act on facts unique to each facility suggesting greater or lesser risks. The overall security afforded by a PDS is the result of a layered approach incorporating various protection techniques. Emphasis is placed on "detection" of attempted penetration in lieu of "prevention" of penetration. Criteria outlined in this Instruction are based on threat or risk analysis relative to the location of the PDS. This generally results in reduced requirements and potential cost savings during installation and maintenance of PDS. The decision as to what extent the guidance provided in SECTIONS VIII thru X is followed ultimately rests with the department or agency AO. The PDS approval request identified in SECTION V, and outlined in ANNEX A, will describe the specifics of the PDS, including unique facts regarding the facility, installation details, and inspection methods and schedule. The AO must sign a formal written acceptance of risk for any deviations.

SECTION II - AUTHORITY

2. The authority to issue this Instruction derives from NSD-42, which outlines the roles and responsibilities for securing national security systems consistent with applicable law, Executive Order 12333, *United States Intelligence Activities*, as amended, and other Presidential directives.

3. Nothing in this Instruction will alter or supersede the authorities of the Director of National Intelligence (DNI). Information in the following sections and tables which relates to Sensitive Compartmented Information (SCI) is advisory to the DNI.

SECTION III - SCOPE

4. This Instruction applies to U.S. Government (USG) departments, agencies and their contractors and vendors who use PDS to protect the transmission of unencrypted NSI. This Instruction provides guidance for PDS installed within *low* and *medium* threat locations worldwide as determined by the AO in consultation with the cognizant Certified TEMPEST Technical Authority (CTTA**)** and Counterintelligence Authority responsible for providing counterintelligence (CI) risk assessment. The use of PDS within a *high* or *critical* threat location is not recommended. If PDS are used in these locations, protection techniques must be determined on a case-by-case basis by the AO in consultation with the cognizant CTTA and Counterintelligence Authority responsible for providing a CI risk assessment. The cognizant CTTA will provide the AO the TEMPEST requirements for the PDS based on the technical threat as determined by the CTTA.

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

SECTION IV - POLICY

6. PDS are used to protect all unencrypted NSI through areas of lesser classification or control. Inasmuch as the NSI is unencrypted, the PDS must provide adequate electrical, electromagnetic, and physical safeguards to deter exploitation. Careful consideration should be given to using encryption or establishing a Controlled Access Area (CAA) in lieu of a PDS. To minimize cost overruns, the threat environment, value of data being lost, risks, cost and operational impact of maintaining the security of the system should be assessed prior to PDS acquisition and installation.

7. The use of PDS within an Uncontrolled Access Area (UAA) is not permitted and National Manager approved encryption solutions must be employed.

8. Encryption solutions for secure multi-site connectivity which have been approved by the National Manager for National Security Systems (NSS) are the preferred methods for protecting NSI.

9. PDS must be installed in accordance with the guidance provided in SECTIONS VIII thru X and is subject to deviation at the discretion of the department or agency AO.

10. The AO must ensure PDS are inspected in accordance with SECTION XI and certified prior to initial operation.

11. A standard operating procedure (SOP) to ensure proper installation, maintenance, operation and inspection of the PDS must be developed by the PDS owner approved by the AO and approved by the cognizant security authority. The SOP must be submitted as a part of the PDS approval documentation.

12. For PDS currently installed within an UAA, a plan to achieve compliance to this Instruction must be in place to the AO within 12 months from the date of signature of this Instruction. Compliance to this Instruction must be achieved and validated by the AO within 36 months from the date of signature of this Instruction. PDS compliance is to be verified through the network authorization process.

13. The AO may delineate alternative security measures for the use of PDS within agency or department specific platforms, such as ships, aircraft, or mobile platforms. Alternate security methods may be used when the platforms cannot be treated equivalently to facilities due to any of the following: (1) Cost prohibitive; (2) Unusable due to weight, size, or other physical restrictions; (3) Security mitigations conditions exist across the platforms.

SECTION V - RESPONSIBILITIES

14. The AO is responsible for approval, certification, and recertification of PDS. The AO is also responsible for approving the reactivation of a PDS. PDS approval requests should undergo a technical review and be approved prior to procurement of materials. PDS must be recertified when modified or when the threat level or security posture changes. PDS approval documentation and all updates should be kept for the lifetime of the physical structure of the PDS.

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

16. 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.

17. Mobile platforms employing inter-shelter cabling need not be re-approved when relocated if the cognizant security authority determines that relocation provides security comparable to that of the original approval. Otherwise, new approval must be obtained.

18. Deactivation of an approved PDS must be reported to the AO by the PDS owner within 30 days.

19. When a CI risk assessment is being completed to assess the potential risk of exploitation, factors to be considered in the risk assessment must include, at a minimum:

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.

SECTION VI - DEFINITIONS

20. The following definitions apply to this Instruction. All other terms used in this issuance are defined in CNSSI No. 4009, *National Information Assurance (IA) Glossary*.

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.
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-2740B, *Federal Specification Locks, Combination, Electromechanical*, may be used as an alternative. A tamper indicative padlock with a wire loop seal may also be used.
Tamper Evident Seal	A serialized mechanical seal used to secure an access panel from unintended entry. The tamper evident seal is resistant to physical removal without showing signs of tampering and provides visual evidence of the panel's integrity. Guidance on the effective use and information on how to obtain tamper evident seals and tamper indicative padlocks is available from the National Security Agency (NSA) Information Assurance Directorate.
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.
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.

SECTION VII – REFERENCES

21. References are provided as Annex B. Future updates to referenced documents shall be considered applicable to this policy.

SECTION VIII - GENERAL PDS INSTALLATION GUIDANCE

22. The PDS must originate and terminate in a CAA that meets the physical security requirements for the type and classification of the data carried by the PDS. When the termination area cannot be controlled to the level of the data carried by the PDS (e.g., in a multi-use conference room), the PDS termination must be secured with a lock box. The lock box must meet the same requirements as a pull box for the PDS carrier type. Terminal equipment must be safeguarded to prevent tampering.

23. In order to use PDS to transport NSI, adequate installation procedures must be used to ensure the PDS does not compromise NSI. The guidance varies based upon the classification/type of data handled and the type of area through which the PDS is installed. There are two basic types of PDS: Category 1 and Category 2. Table 1 defines the category of PDS required for an installation within a *low* threat environment. Table 2 defines the category of PDS required for an installation within a *medium* threat environment.

a. A Category 1 PDS provides a reduced level of physical security protection due to the higher level of control for the surrounding area. A Category 1 PDS can therefore generally be installed using a simple carrier at a reduced cost.

b. A Category 2 PDS provides more significant physical security protection. To implement a Category 2 PDS, the PDS may be installed in one of five types of carriers. The carrier type selection is based upon the physical conditions of the area the PDS traverses, the location of the PDS terminations, and the cost of implementation. The cost of implementing the PDS includes not only the cost of the initial installation, but also the recurring costs of inspection and maintenance. The installer and user should carefully consider all of the potential costs associated with the PDS during the design process.

c. The Category 1 or 2 carrier should be installed in plain view to meet the inspection requirements of SECTION XI. The PDS should not be installed above a false ceiling, below a false floor, or inside a wall unless it is clear that all portions within the wall, above the ceiling or below the floor are inspectable by means identified in the PDS approval request. If the PDS cannot be installed in plain view, or is rendered un-inspectable, then the PDS must be an alarmed carrier.

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. 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

24. The PDS should be marked to make it easily identifiable to the inspector. The markings should be placed at sufficient intervals to facilitate inspections, however, intervals shall not exceed 3 meters. The markings may consist of tape, paint, cable tags, or any other suitable method that does not obscure or impair inspection. However, the PDS should not be labeled as a PDS, or labeled with text that would indicate that it carries NSI. The markings should not be red, since this color is often used to identify fire sprinkler systems, fire alarm wires, and NSI. The PDS may not be painted unless using a distribution system that has a factory painted coating.

25. If pull boxes are used during PDS installation, the following conditions must be met:

- Covers must be secured to the pull boxes by welding or epoxy after installation.
    - If welded, at least one weld must be applied on each side of the box and cover.
    - If epoxy is used, it must be applied between all mating surfaces continuously around the cover. Painted surfaces must be treated to form a mechanically strong epoxy bond.
- Boxes with pre-punched knockouts will not be used under any circumstances.
- If the pull box will be accessed after installation, then the pull box cover must be secured with an approved PDS lock or tamper evident seal. Multiple locking devices or seal may be required for larger pull-boxes.
- Hinge-pins for pull-box covers must be non-removable. The hinge must be hidden or mechanically blocked to prevent removal.
- Hasps used to secure the cover must be permanently and securely attached to the box (e.g., tack welded).

- For *low* threat areas, pull boxes must be constructed of a ferrous metal with a minimum thickness of 16 gauge.
- For a *medium* threat area, pull boxes must be constructed of a ferrous metal with a minimum thickness of 14 gauge and must have a cover that can be locked. However, the material need not be thicker than the PDS carrier or the thickness needed for box rigidity.

26. The PDS will minimize the use of conduit joints, pull boxes, and other types of connections. All connections must be permanently sealed completely around all surfaces (e.g., welding epoxy, or fusion). When the connection consists of more than one seam (e.g., a compression couple), then all seams must be sealed. The seal must provide a mechanical bond between the components of the carrier and must be visible for inspection. Epoxy seals will use a thick, opaque material. Couplers that are secured with a "set screw" must not be used.

27. Circuits must be separated to prevent unauthorized access by those without the appropriate clearance, and to inhibit inappropriate circuit cross connection.

a. As a cost reduction, circuits of more than one classification level may use components of a single PDS. However, unclassified data cables must not be installed within a PDS used for classified data lines without prior approval and review by all user organization's CTTAs. Consult the cognizant CTTA for CNSS Advisory Memorandum (CNSSAM) *TEMPEST/1-13, RED/BLACK Installation Guidance* requirements.

b. Access to all points with breakouts must be restricted to personnel cleared at the highest level of the breakout. Access points containing multi-level classified circuits, and do not have breakouts of higher level circuits, can be serviced by lower level cleared personnel if escorted by personnel cleared for the highest level circuit.

c. All termination boxes should be located within a CAA at the highest level of data being interfaced at the box, or must be secured with a lock box and PDS lock.

28. Based on a technical evaluation of the PDS design, a CTTA may implement additional TEMPEST countermeasures to protect the classified data lines. The countermeasures may include shielding wire lines, fiber optic lines, grounding metallic PDS, and/or isolating the PDS with non-conductive sleeves.

SECTION IX - CATEGORY 1 PDS INSTALLATION GUIDANCE

29. Category 1 PDS provides a reduced level of physical security protection and must be installed in accordance with the following:

a. Data cables must be installed in a simplified carrier. The carrier must be constructed of metal or polyvinyl chloride (PVC) pipe of at least a schedule-40 grade, or armored cable. If armored cable is used, the armor jacket for the cable must be constructed of a flexible metallic material, such as copper, aluminum or steel. If the armored cable is not constructed of a solid, continuous material (i.e., the armor uses interlocking spiral segments), then the metallic material must have an overall, continuous plastic sheath.

b. All connections and access points must be secured and controlled by personnel cleared to the highest level of data handled by the PDS.

SECTION X - CATEGORY 2 PDS INSTALLATION GUIDANCE

30. A Category 2 PDS provides significant physical security protection and can be implemented by using one of the following carriers: hardened, buried, suspended, alarmed, or continuously viewed.

a. *Hardened* carriers are normally used between CAAs that are located within the same building. The data cables must be installed in a carrier. The carrier must be constructed of ferrous, electrical metallic tubing (EMT); ferrous pipe conduit; or ferrous rigid sheet metal ducting. Flexible conduit and armored cables must not be used as a hardened carrier. The carrier must not open to expose data cables (e.g., removable covers), except at approved pull boxes and termination boxes. The carrier must utilize elbows, couplings, nipples, and connectors of the same materials. All joints and connections must be sealed as described in paragraphs 21 and 22. The carrier must be installed to provide an unobstructed view during visual inspections and must provide at least 2.5 centimeters (1 inch) of clearance from walls, floors, ceilings, ducts, cables, other conduits, or any material that may obstruct visual inspections. If a wall, floor, or ceiling surface is at least 10 centimeters (4 inches) of reinforced concrete or equivalent, the carrier may be flush-mounted to the surface instead of leaving a 2.5-centimeter gap. If the carrier traverses a void (e.g., a hollow wall, ceiling, 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). If installation of an inspection ports results in compliance issues with other security standards, the solution must be addressed in PDS approval request. If a carrier is used between two CAAs that are separated by floors considered UAA, the data in the carrier going through the UAA must be encrypted (e.g., CAA on the 1st and 4th floor and the 2nd and 3rd floor considered UAA).

b. *Buried* carriers are normally used between CAAs that are located in different buildings. The data cables must be installed in a carrier. The carrier must be constructed of conduit consisting of EMT, rigid pipe, PVC, or a similar type of plastic electrical conduit. All connections must be permanently sealed completely around all mating surfaces,(e.g., welding, epoxy, fusion, or PVC glue). The carrier must be buried a minimum of 1 meter (39 inches) below the surface and on property owned or leased by the USG or by the U.S. contractor or vendor that controls the PDS. If the carrier cannot be buried to a 1-meter depth due to soil conditions or blocked passage, 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.

1) If the buried carrier is installed in a *medium* threat location, then the carrier must be buried a minimum of 1 meter below the surface and be encased within the center of mass of approximately 20 centimeters (8 inches) of concrete. A concrete and steel container of sufficient size (to preclude surreptitious penetration in a period less than two hours as confirmed by laboratory tests) may be used in lieu of the 20 centimeters (8 inches) of concrete.

2) The buried carrier should enter a building through the building's concrete slab or basement wall. All portions of the PDS above the 1 meter depth and not within a CAA (e.g., a PDS rising to a pull box on the side of a building) must meet the requirements of a Category 2 hardened carrier.

3) Manholes or any other access (e.g., hand hole) to the buried PDS must be secured with a PDS lock or an alarm. The PDS lock must be visible for daily inspection. If a PDS lock cannot be used due to the physical construction of the manhole, then a standard locking manhole cover and micro-switch alarm should be used.

c. *Suspended* carriers may be used for short runs when it is not practical to bury the PDS between buildings (e.g., between the 3rd floors of adjacent buildings). Suspended carriers between buildings are permissible if they terminate in a CAA on each end or immediately enter a hardened PDS at the building boundary. The suspended carrier must be hung directly between buildings. The suspended carrier must be elevated a minimum of 5 meters (16 feet 4 inches) and only used if the property traversed is owned or leased by the USG or by a USG contractor or vendor that controls the PDS. Suspended carriers must be installed to provide unimpeded inspection and be clear of any obstruction or device which encroaches upon the system to facilitate tampering. The area containing the suspended carrier must be illuminated at night.

d. *Alarmed* carriers may be used when it is not practical to perform daily inspections (e.g., when the PDS must be installed in locations that are not easily accessible). An alarmed carrier must be protected by an alarm system that detects attempted penetration of the carrier. As an alternative, the space surrounding the entire carrier may be covered by an area or volumetric (e.g., infrared, motion detection) alarm system that is approved by the cognizant, physical-security authorities. The alarm system must be capable of prompt detection of any penetration and annunciate the alarm in an office manned 24 hours-a-day, 7 days-a-week. The office must be capable of notifying security forces that can respond within 15 minutes. The alarm must provide protection from tampering and be able to register malfunctions. The alarm system must also transmit a line fault message to the annunciator panel if the system fails. A visual inspection of the PDS in accordance with Table 3 is not required for an alarmed system. However, each alarm zone must be tested in accordance with Table 5. The SOP for the alarmed carrier must be implemented to;

- Verify its performance at intervals as shown in the PDS inspection schedule;
- Ensure the response by security personnel in the area of possible attempted penetration is within 15 minutes of discovery;
- Provide for inspection of the PDS to determine the cause of the alarm;
- Define action to be taken regarding the termination of transmission; and
- Initiate investigation of an actual intrusion attempt, etc.

e. *Continuously viewed* carriers are normally used when continuously viewed areas are already in place for physical security reasons. A continuously viewed carrier must be

under continuous observation, 24 hours-a-day, 7 days-a-week, including when non-operational. Such circuits may be grouped together, but they should be separated from all non-continuously viewed circuits ensuring an open field of view. The SOP must include the requirement to investigate any attempt to disturb the PDS. Appropriate security personnel should investigate the area of attempted penetration within 15 minutes of discovery.

f. Alternative carriers and other variances must be approved by the AO and the cognizant security authority based upon a technical review.

SECTION XI- PDS INSPECTION

31. As described in SECTION I, the PDS provides intrusion detection in lieu of intrusion prevention. Inspections are an integral part of the PDS. The frequency of the inspections is based upon the type and classification of the information carried, the control of the area surrounding the PDS, and the threat environment.

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

33. A log must be maintained of the PDS inspections. The log must contain the date of the inspection, the time of the inspection, the inspector's name, and the inspector's title. The log must be kept on record for a minimum of one year.

34. Two types of PDS inspections are required: visual inspections and technical inspections. Visual inspections are required for all PDS except for alarmed carriers and for continuously viewed carriers. In lieu of the daily inspection, the alarm system performance for alarmed carriers is verified at intervals provided in Table 5.

a. Visual inspections, if required, must be performed along the entire length of the PDS. The PDS carrier (e.g., conduit, buried path), connections, lock boxes, and terminal/pull boxes must be assessed for signs of penetration, tampering, and any other anomaly that could cause deterioration of protection safeguards. Locks and tamper evident seals must also be inspected. The PDS must be inspected from a distance that would allow the detection of an attempted intrusion. The inspection of a buried PDS must be extended out to 5 meters (16 feet 4 inches) on each side to the PDS carrier path. Adequate lighting must be provided to reveal any attempts at penetration.

1) The person(s) formally appointed to accomplish the visual inspection must be trained to recognize physical changes in PDS, including attempts at penetration and tampering.

2) The visual PDS inspection schedule is provided in Table 3 and is applicable 365 days a year. Visual inspections are not absolutely required for portions of PDS traversing a Secret or higher CAA but may be required by the AO.

Table 3. Visual Inspection Schedule

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

b. Technical inspections must be performed by visually and physically verifying the integrity of the PDS carrier (e.g., conduit, buried path). The connections lock boxes, and terminal/pull boxes must be assessed for signs of penetration, tampering, and any other anomaly causing a deterioration of protection safeguards. The mechanical security of the connections and covers must also be verified.

1) The person(s) formally appointed to accomplish the technical inspection must be trained to recognize both physical changes in the PDS, including attempts at penetration and tampering, and changes in the technical aspects of the PDS (e.g., by-pass circuitry; attachment or removal of devices or components; inappropriate or suspicious signal levels; mechanical; TEMPEST and RED/BLACK integrity of the PDS).

2) The technical inspection must be performed prior to approval and at random intervals thereafter. The technical PDS inspection schedule is provided in Table 4. At a minimum, the following procedures must be used to perform the inspections:

a) The initial inspection should document the path of the PDS, the locations for all pull boxes, and the 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. Subsequent inspections must verify the path of the PDS and the location of pull boxes and joints.

b) When test equipment is locally available and resident expertise allows, measure and record the electrical characteristics of the PDS lines to obtain a baseline electrical profile of the PDS. Accomplish the electrical characterization immediately upon completion of the PDS installation. Such measurements may consist of signal levels, voltage levels, time domain reflectometer (TDR) recorded readings, and any other electrical measurements that may be recorded and retained. Record and compare measurements taken at subsequent technical inspections to the previously recorded baseline measurements to identify possible tampering attempts.

c) The PDS must be inspected on all sides of the carrier and boxes. The use of hand-held mirrors may be required to view the top or back sides of the carrier. If practical, the carrier and sealed boxes should be loosened from walls to view the hidden surfaces.

Caution should be used when removing the carrier and sealed boxes from the wall as the process may damage the integrity of the PDS.

d) Locks and tamper evident seals must be inspected by verifying the lock combination numbers, the lock serial numbers, and the tamper-seal serial numbers.

e) Pull boxes must be opened and inspected from the inside.

Table 4. PDS Technical Inspection Schedule

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

35. The alarm system performance for alarmed carriers is verified at intervals provided in Table 5. The alarm system must be verified for each separate section or "zone" The alarm will be verified in accordance with the SOP for the alarm, as described in paragraph 26.d.

Table 5. PDS Alarm Circuit Verification Schedule

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

Enclosures:
ANNEXES A-B

ANNEX A

SAMPLE PROTECTED DISTRIBUTION SYSTEMS (PDS) APPROVAL REQUEST

Requests for PDS approval must be forwarded to the department or agency AO. It will include the following information in each listed category.

1. *Installation Site* identifies the organization where the PDS must be installed, and a point-of-contact's name and phone number.

2. *Installation Activity* identifies the organization responsible for the installation of the PDS, and a point-of-contact's name and phone number.

3. *System Information* provide a description of the components directly connecting to the PDS, and a summary of the type of cable used in the PDS (e.g., fiber optics, shielded twisted pair, coaxial cable) and the electrical parameters (e.g., voltage and current levels).

4. *Security Profile* identifies the highest classification of NSI traversing the PDS (if Sensitive Compartmented Information, identify the specific categories or compartments processed); and provide a percentage breakdown of the type of NSI processed on the PDS.

5. *Facility Security* provides information concerning the security conditions of the facility where the PDS must be located, as follows:

- The facility's approximate location on a map relative to residential and commercial areas.
- A fenced facility's fence location on the map, a description of the type of fencing constructed, and identification of any perimeter intrusion detection system (IDS) installed.
- Automobile, pedestrian, and amphibious access points on the map.
- Access point hours of operation and guard assignment, if any.
- An explanation of personnel badge recognition systems in use, access lists maintained, and escort requirements for uncleared personnel.
- An explanation of a registration control system used for vehicles, employees, visitors, and tradesmen, if any.
- An explanation of the facility guard force to include citizenship, association (contract, direct hire, USG), and clearances.

6. *Building Security* provides information on the security conditions of the buildings(s) within which the PDS must be installed, as follows:

- A floor plan of the building(s), a description of the exterior and interior construction, and identification any perimeter IDS installed.

- Access points indicated on the floor plan of the building(s) (all windows accessible from the ground, fire escapes, etc., should be identified and any implemented window tamper protection devises should be described);
- Access point hours-of-operation, guard assignment, and access control use for administrative access control to the building.
- Door and lock types securing the access points.
- An explanation of personnel badge recognition systems in use and access lists maintained.
- Clearance level and escort requirements for personnel entering the building.
- An explanation of the control of the movement and operation of custodial, maintenance, and vending personnel, and any escort or continuous surveillance requirements for uncleared personnel.

7. *Protected Distribution Systems* provides the security condition of the distribution system, as follows:

- The classification level of the area controlled and indication of whether uncleared personnel are monitored.
- The location and routing of the proposed PDS on a map and/or floor plan. Describe its construction.
- Inspection procedures for detection of tampering.
- A detailed description of the PDS alarm, if applicable.

Classify site-specific PDS information in accordance with department/agency guidance.

ANNEX B

REFERENCES

The following references are applicable to the installation and use of PDS:

a. National Security Directive 42, National Policy for the security of National Security Telecommunications and Information Systems, 5 July 1990

b. Executive Order 12333, United States Intelligence Activities, December 4, 1981 (As Amended by Executive Orders 13284 (2003), 13355 (2004) and 13470 (2008))

c. CNSSI No. 4009 *Committee on National Security Systems (CNSS) Glossary*, 6 April 2015

d. FF-L-2740B, Federal Specification Locks, Combination, Electromechanical, 15 June 2011

e. Information Security Oversight Office, 32 CFR Parts 2001, *Classified National Security Information*, 28 June 2010

f. Information Security Oversight Office, 32 CFR Part 2004, *National Industrial Security Program Directive No. 1*, 10 April 2006

g. CNSSAM TEMPEST/1-13, *RED/BLACK Installation Guidance*, 17 January 2014

h. *National Security Agency Information Assurance Technical Capabilities Report*, May 2013.

i. CNSSP No. 22, *Policy on Information Assurance Risk Management for National Security Systems*, January 2012