



Communications and Information

PROTECTED DISTRIBUTION SYSTEMS

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

This instruction prescribes the approval and construction requirements for a protected distribution system (PDS) and implements National Security Telecommunications and Information Systems Security Instruction (NSTISSI) 7003, *Protected Distribution Systems*. Use of extracts is encouraged. Direct questions and comments on the contents of this instruction through appropriate command channels to Headquarters, Air Force Communications Agency, Information Protection Division (HQ AFCA/SYS), 203 W. Losey Street, Room 2040, Scott AFB IL 62225-5234. Refer recommended changes and conflicts between this and other publications, using AF Form 847, **Recommendation for Change of Publication**, to HQ AFCA, Systems Security Applications Branch (HQ AFCA/SYSA), 203 W. Losey Street, Room 2040, Scott AFB IL 62225-5234.

SUMMARY OF REVISIONS

This revision aligns the instruction with AFRD 33-2, *Information Protection*, and implements NSTISSI 7003. It makes changes in PDS protection requirements and the approval process for PDSs.

	Paragraph
Introduction .....	1
PDS Defined.....	2
PDS Selection Considerations.....	3
PDS Operation.....	4
PDS Justification .....	5
PDS Plan .....	6
PDS Plan Validation.....	7
PDS Construction .....	8
PDS Certification .....	9
PDS Approval .....	10
PDS Recertification .....	11
PDS Deactivation .....	12

	Page
<b>Attachments</b>	
1. Glossary of References, Acronyms, Abbreviations, and Terms.....	7
2. PDS Approval Flowchart .....	8
3. PDS Construction Criterions .....	9
4. Technical Inspections.....	13

**1. Introduction.** AFSSI 4100 (C), *Communications Security Program (U)*, requires the use of National Security Agency (NSA)-endorsed communications security (COMSEC) products and services to secure classified telecommunications by all Air Force activities and their contractors. Information systems or networks that process classified national security information in more than one controlled access area and require the transfer of that information between controlled access areas must use a secure means of transference; courier or secure telecommunications. If secure telecommunications is chosen, include a secure telecommunications requirement (COMSEC) in the system security policy. In order of preference, the COMSEC requirement is met by: NSA-endorsed COMSEC systems (encryption), NSA-endorsed intrusion detection optical communications system

(IDOCs), or PDS. AFSSI 4100 also requires the use of NSA-endorsed COMSEC products, techniques, and protected services to protect unclassified, sensitive telecommunications involving Air Force activities and their contractors. When a PDS is chosen to protect unclassified, sensitive information, follow the standards in this instruction for CONFIDENTIAL information.

1.1. Although it is the last alternative for consideration, you may use a PDS to transmit unencrypted, clear-text, classified national security information provided the PDS is protected with adequate electrical, electromagnetic, and physical safeguards as identified in this instruction. In establishing the standards for PDS construction and use, national managers incorporated the philosophy of risk management rather than risk avoidance. As such, the standards specified in this instruction are the minimum protection standards based on national guidance. The assumption of any additional risk to lessen the minimum specified standards is not an option. Organizations wishing to discuss this policy may forward their specific concerns through command channels to HQ AFCA/SYS. Develop the certified technical solution using the process of AFI 33-103, *Requirements Development and Processing*, to justify a PDS. Use of any PDS not meeting the standards of this instruction is prohibited.

1.2. Do not use a PDS within a high threat environment as defined by NSTISSI 7000 (C), *TEMPEST Countermeasures for Facilities* (U), Annex A (S), *TEMPEST Threat to Facilities* (U). MAJCOM Information Protection (IP) offices are on automatic distribution for this document.

**2. PDS Defined.** A PDS is a physically protected wire line (data line) between subscribers who electronically share classified and unclassified national security information. Those subscribers that share classified national security information reside in controlled access areas and the PDS protects information passed between them through an area of lesser control. The controlled access area processing the classified information can be a desk, cubicle, set of cubicles, room, group of rooms, wing, floor, building, or buildings. Establishing or defining the controlled access area boundary is important because a PDS is installed between controlled access areas; not within a controlled access area. In short, a PDS is the wire line carrying classified information and includes the distribution system comprised of either a hardened or simple distribution system that provides the acceptable degree of physical security to the wire line. A wire line carrying classified information within the controlled access area is a RED wire line or RED signal line.

**3. PDS Selection Considerations.** The requiring agency, in concert with the Command, Control, Communications, and Computer systems officer (CSO) and systems telecommunications engineering manager (STEM), must carefully consider using a PDS before selecting it in preference to other COMSEC solutions. Economic, technical, or operational factors may make a PDS necessary in comparison to other COMSEC solutions. However, a PDS is not a preferred method and is considered only as a last resort.

3.1. **Operation Considerations.** Operating a PDS requires continued physical security integrity after construction. The cost and operational impact of maintaining the security of the system can easily exceed the construction costs. Consider using a PDS only after the requiring agency agrees to afford it the required degree of protection 24 hours a day, 7 days a week.

3.2. **Classification Level Considerations.** When reviewing communications needs, consider future requirements in regard to the classification level of the information to be transmitted, the requisite physical controls needed, and the geographical location of the PDS site. Typically it is easier and less costly to include the capability for future requirements than to retrofit an installed system for such updates.

3.3. **Physical Security Considerations.** The operating agency must protect the PDS such that only persons who are cleared for the highest classification and category of information transmitted over the system may have unrestricted access to the system. Escort all personnel who do not have the appropriate security clearance, but require occasional, temporary access to the PDS terminal equipment and interconnecting lines (for example, safety and fire inspectors) to prevent a compromise of the information or the security integrity of the PDS. Maintain the physical security integrity of the PDS on a continual basis, regardless of whether the PDS is or is not in operation.

**4. PDS Operation.** When protecting the transmission of information with a PDS, the requiring agency must specify the office responsible for:

4.1. Controlling the PDS. This office must ensure personnel in controlled access areas are aware that they are responsible to assist in the close supervision of the visible components of the PDS. Investigate all reports of suspicious activity immediately.

4.2. Maintaining the record of events. Maintain a record of all PDS events such as alarms (if used), patrols (if used), inspections, employee reports, and so forth. The local security supervisor, as identified by the DAA, reviews the record monthly.

4.3. Reporting incidents of tampering, penetration, or unauthorized interception.

4.4. Receiving reports of incidents of tampering, penetration, or unauthorized interception. Ensure a local office is identified to receive reports of tampering, penetration, or unauthorized interception of information transmitted over a PDS. This office will immediately report physical incidents of tampering, penetration, or unauthorized interception to the approval authority for assessment, to the local security authority for review and initiation of an investigation, and as a physical security COMSEC

incident following the procedures established for physical security incidents in AFI 33-212, *Reporting COMSEC Incidents*. Do not use the PDS until the incident is assessed by the approval authority and its security status is determined.

4.5. Investigating alarms, tampering, penetration, or unauthorized interception.

**5. PDS Justification.** Justify a PDS using the certified technical solution process of AFI 33-103 and meet the requirements of this instruction before approving construction or use. The requiring agency, CSO, and STEM must justify using a PDS instead of an approved COMSEC system, Intrusion Detection Optical Communications System (IDOCs), or courier before submitting the certified technical solution for approval.

5.1. Justify the PDS by:

5.1.1. Showing that courier is not timely, practical, or feasible, and,

5.1.2. Using a capability or cost basis.

5.2. If the justification is based on capability, the CSO must show:

5.2.1. There is no COMSEC system or IDOCs with the capability to handle the data to be passed over the PDS.

5.2.2. A capable system exists but there is not enough equipment available to support this requirement.

5.3. IDOCs provides the capability to secure communications over optical fiber lines without the use of encryption or a PDS. The National Security Agency Information Systems Security Products and Services Catalog provides additional information on IDOCs.

5.4. If the justification is based on cost, the requiring agency must show that using a PDS is less costly than using an approved COMSEC system or IDOCs. When this justification is used, compare and show the total life-cycle cost of COMSEC equipment or IDOCs to the total life-cycle cost of the proposed PDS. As a minimum, the PDS plan must show the following:

5.4.1. PDS construction costs.

5.4.2. Annual operation and maintenance costs.

5.4.3. Annual physical security costs.

**6. PDS Plan.** The requiring agency prepares a PDS plan prior to constructing a PDS. Make two copies. Organize the information in the order listed below.

**NOTE:** Some required information may cause the plan to be classified.

**6.1. User Identification.** Identify:

6.1.1. The name and location of the requiring agency. This will normally be the office of record for the PDS. The office of record will maintain and file the PDS package as a part of the certification and accreditation file.

6.1.2. The name and office symbol of the DAA.

6.1.3. The controlled access areas connected by the PDS.

6.1.4. All uncontrolled access areas and limited controlled areas on the PDS route.

**6.2. PDS Operation Requirements.** Identify the:

6.2.1. Controlling office for the PDS (paragraph 4.1).

6.2.2. Office and method to record events relative to the PDS (paragraph 4.2).

6.2.3. Office and method to report incidents of tampering, penetration, or unauthorized interception (paragraph 4.3).

6.2.4. Office to receive reports of tampering, penetration, or unauthorized interception (paragraph 4.4).

6.2.5. Office to monitor and investigate alarms, incidents of tampering, penetration, or unauthorized interception and to comply with AFI 33-212.

**6.3. Physical Security Requirements.** Identify the:

6.3.1. Highest classification level and category of information carried by the PDS.

6.3.2. Minimum security clearance level of individuals who will have unrestricted access to any portion of the PDS.

6.3.3. Construction requirements from attachment 3, Table A3.1; list in the order outlined in attachment 3.

6.3.4. Type of distribution system chosen.

6.3.4.1. If an alarmed carrier PDS was chosen, identify the office to monitor the PDS alarm,

6.3.4.1.1. The required responses to alarm conditions (this information, when applied to a specific PDS, is classified).

6.3.4.1.2. The office that will respond to PDS alarms.

6.3.4.1.3. The required minimum interval for alarm circuit verification as determined by the cognizant security authority (this information, when applied to a specific PDS, is classified).

6.3.4.2. If the continually-viewed PDS was chosen, identify the office to provide the monitoring service.

6.3.5. Required minimum interval for lines route inspections from Table A3.2 (this information, when applied to a specific PDS, is classified).

6.3.6. Office that will make the lines route inspections.

6.3.7. Required minimum interval to make the technical inspections from Table A3.3 (this information, when applied to a specific PDS, is classified).

6.3.8. Office that will make the technical inspections or ensure inspection completion. Technical inspection requirements are defined in attachment 4.

6.4. **Wire Line Requirements.** Identify the type of data line from attachment 3, paragraph A3.3. The requirement is to contain any emanations of the *intended* unencrypted signal within the PDS. Use shielded metallic wire cable, shielded metallic wire lines, or fiber optics.

**NOTE:** Do not confuse the requirements to contain emanations of the *intended* unencrypted signal with the Emission Security (EMSEC) countermeasures. EMSEC countermeasures are applied to contain the *unintended* compromising emanations within the inspectable space as identified by the wing IP office.

6.4.1. Shielded Wire Lines. Use shielded wire lines meeting the requirements identified in the shielded cables attachment of AFSSM 7011, *The Emission Security Countermeasures Review*.

6.4.2. Coaxial Cables. The shield of a coaxial cable is used as a signal return path. Because of this, it cannot be used as a shield to satisfy this requirement. Use a second shield insulated from any metallic carrier portion of the PDS and insulated from the coaxial return path. A second alternative is to use triaxial cable.

6.4.3. Fiber Optic Cables. It is not necessary to shield fiber optic cables. However, you may not use fiber optic cables which contain metallic conductors or metallic strength members.

6.5. **Physical Construction Requirements.** Identify the organization proposed to install the PDS. Describe the PDS physical properties. Include in this section:

6.5.1. Diagrams showing the proposed route and all involved controlled access areas, limited controlled areas, and uncontrolled access areas.

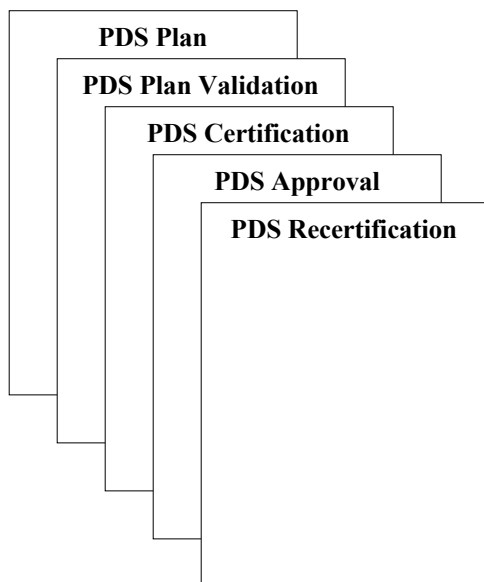
6.5.2. Diagrams identifying other wiring, lines, and electrical equipment located along the proposed route.

6.5.3. A listing of materials proposed for use to construct the PDS.

6.5.4. Any other meaningful information.

**7. PDS Plan Validation.** The requiring activity submits the PDS plan (2 copies) to the wing IP office for validation. The wing IP office reviews the request for adequate justification and obvious errors such as requiring unnecessary redundancy in protection or any major omissions. The wing IP office validates the PDS plan ensuring all requirements of this instruction are met and attaches the validation to the PDS plan as shown in Figure 1. The wing IP office files one copy. When proposing a modification to an existing PDS, include only the items pertaining to the modification when requesting approval.

**Figure 1. The PDS Package.**



**8. PDS Construction.** Construct the PDS according to the validated plan. Do not use a PDS to protect classified traffic until certification and approval is achieved.

**9. PDS Certification.** After construction is complete, resubmit the PDS package consisting of the PDS plan and validation documentation to the wing IP office for certification.

9.1. The wing IP office certifies:

9.1.1. Compliance with the construction plan.

9.1.2. The PDS passed a lines route inspection by the lines route inspector.

9.1.3. The PDS passed a technical inspection by the technical inspector.

9.1.4. The controlling office is identified.

9.1.5. The incident reporting and investigating system is in effect.

9.1.6. If used, alarm circuit verification procedures are established.

9.1.7. If used, continuous viewing procedures are established.

9.1.8. The certification authority must ensure all discrepancies are corrected before forwarding to the approval authority.

9.2. The wing IP office attaches the certification to both copies (original and wing IP office file copy) of the PDS package as shown in Figure 1. Keep the wing IP office file copy and return the original to the requiring agency.

## **10. PDS Approval.**

10.1. **Approving the PDS.** The requiring agency submits the complete PDS package consisting of the PDS plan, the validation documentation with the validating authority signature, and PDS certification documentation with the certifying authority signature to the DAA. The DAA approves operation of the PDS as part of the system certification and accreditation. The PDS package is independent of, but essential to, the system certification and accreditation. Attach the approval to the PDS package as shown in Figure 1. Forward a copy of the approval to the wing IP office who attaches the approval to their file copy.

10.2. **Approval Authorities.** Except as noted below, the Designated Approval Authority (DAA) approves the PDS as a part of the certification and accreditation process for the network or information system the PDS is supporting. AFPD 33-2 requires that all systems be certified and accredited prior to operation; AFSSI 5024, Volume I, *The Certification and Accreditation (C&A) Process*, details the process that will be used to certify and accredit AF Systems. Complete the requirements of this AFSSI before obtaining approval to operate. Attachment 2 contains a PDS approval flow chart.

10.2.1. **Temporary Systems.** The developmental or systems DAA may approve temporary configurations without processing a formal approval package if the PDS:

10.2.1.1. Is in place no more than one month, and

10.2.1.2. Is confined within U.S. Government installations, and

10.2.1.3. Does not process higher than SECRET information.

10.3. **Contractor Facilities.** The head of the government contracting department or agency is the approval authority for a contractor owned and operated PDS.

10.4. **Tactical Systems.** A PDS used in a tactical system employing inter-shelter cabling is approved by the developmental or systems program office. Once approved, tactical systems do not require re-approval upon relocation providing the previously approved configuration is not changed; such as, the line lengths, cable types, connections, connectors, and so forth. A change in the physical placement of components is not a change in configuration.

## **11. PDS Recertification.**

11.1. The wing IP office recertifies a PDS as part of the system recertification and reaccreditation:

11.1.1. Annually, if installed outside the United States.

11.1.2. Every 3 years, if installed within the United States.

11.2. Recertify the PDS after verifying the following:

11.2.1. Lines route inspections—the PDS meets requirements and previous inspections were completed on schedule.

11.2.2. Technical inspections—the PDS was within limits and the inspections were completed on schedule.

11.2.3. Alarm circuit (if used) verification—previous alarm circuit tests were successful and completed on schedule.

11.2.4. PDS events record—evidence that this record is current and includes all significant events.

11.3. Attach the recertification to each copy (the office of record and the wing IP office) of the PDS package as shown in Figure 1.

11.4. A PDS that does not meet the above requirements may not be recertified.

11.4.1. The wing IP office notifies the DAA immediately when a PDS is not recertified.

11.4.2. The requiring agency corrects deficiencies discovered during recertification within 30 days and requests recertification.

11.4.3. A PDS that fails recertification can not be used until recertified.

**12. PDS Deactivation.** The operating agency reports deactivation of an approved PDS to the DAA and wing IP office within 5 days of deactivation. Destroy all files pertaining to the deactivated PDS after one year.

GEORGE F. FIEDLER, Lt Col, USAF  
Chief, Networks Division

**GLOSSARY OF REFERENCES, ACRONYMS, ABBREVIATIONS, AND TERMS****References**

NSTISSI 7003, *Protected Distribution Systems*  
 NSTISSI 7000 (C), *TEMPEST Countermeasures for Facilities (U)*, Annex A (S), *TEMPEST Threat to Facilities (U)*  
 AFI 31-101V1, *The Air Force Physical Security Program*  
 AFD 33-2, *Information Protection*  
 AFI 33-103, *Requirements Development and Processing*  
 AFI 33-203, *The Air Force Emission Security Program*  
 AFI 33-212, *Reporting COMSEC Incidents*  
 AFSSI 4100 (C), *Communications Security Program (U)*  
 AFSSI 5024, Volume I, *The Certification and Accreditation (C&A) Process*  
 AFSSM 7011, *The Emission Security Countermeasures Review*

**Acronyms and Abbreviations**

AFI	Air Force Instruction
AFPD	Air Force Policy Directive
AFSSI	Air Force Systems Security Instruction
AFSSM	Air Force Systems Security Memorandum
CAA	Controlled Access Area
COMSEC	Communications Security
CSO	Command, Control, Communications, and Computer Systems Officer
CTTA	Certified TEMPEST Technical Authority
EMSEC	Emission Security
emt	Electrical Metallic Tubing
GSA	Government Services Administration
IDOCS	Intrusion Detection Optical Communications System
IP	Information Protection
LCA	Limited Controlled Area
MAJCOM	Major Command
NSA	National Security Agency
NSTISSI	National Security Telecommunications and Information Systems Security Instruction
PVC	Polyvinyl Chloride
SCI	Sensitive Compartmented Information
SSO	Special Security Office
STEM	Systems Telecommunications Engineering Manager
UAA	Uncontrolled Access Area

**Terms**

**Access Control.** Process of limiting access to the resources of an automated information system (AIS) only to authorized users, programs, processes, or other systems.

**Controlled Access Area.** 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 Controlled Area.** The space surrounding a protected distribution system within which exploitation is not considered likely or legal authority to identify or remove a potential exploitation exists.

**Protected Distribution System.** A wire line or fiber optics distribution system with adequate electrical, electromagnetic, and physical safeguards to permit its use for the transmission of unencrypted classified information.

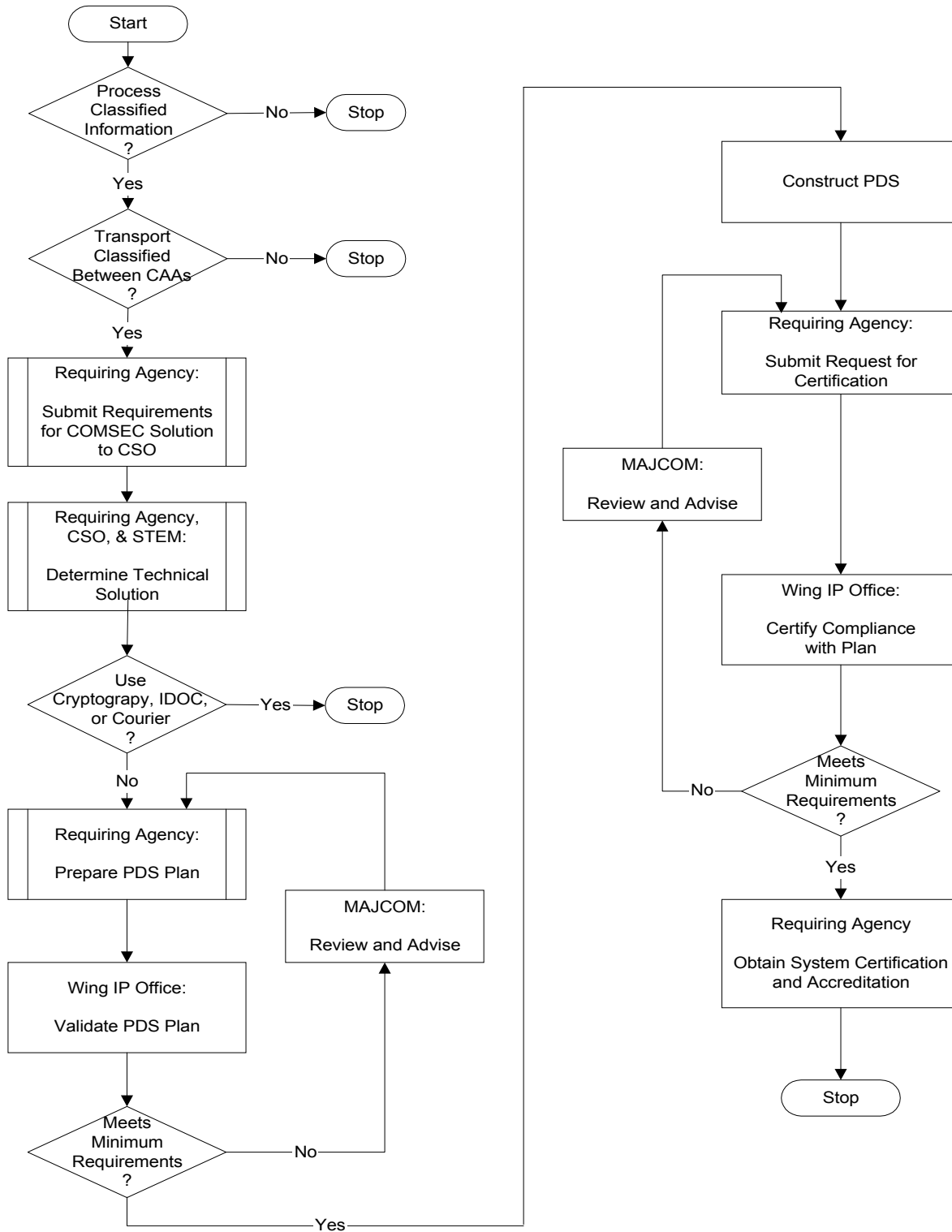
**NOTE:** This definition does not include intrusion detection optical communications systems (IDOCS) approved by the National Security Agency.

**Uncontrolled Access Area.** The area external or internal to a facility over which no personnel access controls can be or are exercised.

**PDS APPROVAL FLOW CHART**

This is a flow chart of the PDS plan, validation, construction, certification, and approval process.

**Figure A2.1. The PDS Plan, Validation, Construction, Certification and Approval Process.**





**PDS CONSTRUCTION CRITERIONS**

**A3.1. General.** This attachment provides criterions for constructing a PDS to provide the required physical security of the wire line. It does not provide the requirements for safety standards, local building codes, electrical codes, grounding requirements, and so forth. The steps required to construct a PDS vary based upon classification level, type of data handled, and area through which the distribution system is installed. Table A3.1 contains a construction criterion matrix. Find the classification of the information processed and the protection level of the area through which the classified information will be transmitted and implement the paragraphs listed in the box.

**TABLE A3.1. MINIMUM PDS CONSTRUCTION CRITERIA**

TYPE OF DATA	TYPE OF AREA					
	UAA	LCA	CONFIDENTIAL CAA	SECRET CAA	TOP SECRET CAA	SCI CAA
CONFIDENTIAL	A3.2	A3.2	Note <sup>1</sup>	Note <sup>1</sup>	Note <sup>1</sup>	A3.4.1
	A3.3	A3.3	A3.4.1	A3.4.1	A3.4.1	A3.4.2
	A3.4.1	A3.4.1				
	A3.5.1	A3.5.2				
SECRET	A3.2	A3.2	A3.2	Note <sup>1</sup>	Note <sup>1</sup>	A3.4.1
	A3.3	A3.3	A3.3	A3.4.1	A3.4.1	A3.4.2
	A3.4.1	A3.4.1	A3.4.1			
	A3.5.1	A3.5.1	A3.5.2			
TOP SECRET	A3.2	A3.2	A3.2	A3.2	Note <sup>1</sup>	A3.4.1
	A3.3	A3.3	A3.3	A3.3	A3.4.1	A3.4.2
	A3.4.1	A3.4.1	A3.4.1	A3.4.1		
	A3.5.1	A3.5.1	A3.5.1	A3.5.2		
SCI	A3.2	A3.2	A3.2	A3.2	A3.2	Note <sup>1</sup>
	A3.3	A3.3	A3.3	A3.3	A3.3	A3.4.2
	A3.4.2	A3.4.2	A3.4.2	A3.4.2	A3.4.2	
	A3.5.1	A3.5.1	A3.5.1	A3.5.2	A3.5.2	

<sup>1</sup> PDS not required, consider as RED signal lines within the controlled access area.

**A3.2. Physical Security Criterion.** The purpose of a PDS is to ensure uncleared or inappropriately cleared personnel do not gain access to the distribution system without readily discovering such access. Therefore:

A3.2.1. Do not conceal a PDS from view by placing it behind walls, above ceilings, or below floors. Provide at least 2 inches clearance from other wires, cables, ducts, and other material that may obstruct viewing during visual inspections. If a user wants to conceal the PDS from view, make the area concealing the PDS a controlled access area and meet the physical security requirements for an unattended controlled access area. Within a controlled access area, consider the distribution system and wire line as a RED signal wire line, not as a PDS. If the user alarms the unattended controlled access area with an area alarm or PDS alarm, failure of the alarm requires applying physical control measures (continuous viewing) to the area or cease use of the RED signal wire line until returning the alarm protecting the controlled access area to full service and verifying the integrity of the wire line by a technical inspection.

A3.2.2. Provide for route inspections at the minimum intervals according to Table A3.2.

A3.2.2.1. Conduct close visual inspections of the PDS for signs of penetration, tampering, and any other anomaly that may cause a deterioration of protection safeguards. The close visual inspection must include the total surface of the PDS (especially those parts close to walls and so forth); use of a mirror is recommended.

A3.2.2.2. The persons selected to accomplish the route inspections need not be qualified installers or technicians, but they must know enough about the PDS construction to recognize physical changes in the PDS including attempts at penetration and tampering.

A3.2.2.3. A continuously-viewed PDS or a PDS protected by an alarm system does not require periodic lines route inspections. A continuously-viewed PDS must be under continual observation (24-hours a day, 7 days a week), whether in use or not.

A3.2.3. Provide for technical inspections at the minimum intervals according to Table A3.3. Conduct technical inspections according to attachment 4.

A3.2.4. In tactical environments, locate the PDS within areas directly under U.S. Forces physical control.

A3.2.4.1. Protect the perimeters or keep under surveillance, with armed guards or patrols, the area surrounding the PDS.

A3.2.4.2. Provide protection commensurate with the level of information passed through the PDS.

A3.2.4.3. The responsible commander assesses the risks associated with maintaining the security of the system. Include factors such as stability of the area and technical intelligence collection proficiency of adversaries, to include the host country, and their capability to collect and relay information obtained.

**TABLE A3.2. PDS LINES ROUTE INSPECTION SCHEDULE<sup>1</sup>**

HIGHEST CLASSIFICATION OF DATA CARRIED	FACILITY LOCATION					
	U.S.		Outside U.S. in Low Threat Environment <sup>2</sup>		Outside U.S. in Medium Threat Environment <sup>2</sup>	
	UAA	LCA	UAA	LCA	UAA	LCA
SCI or TOP SECRET	2	1	2	1	3	1
SECRET	1	Weekly	1	Weekly	2	1
CONFIDENTIAL	Weekly	None	Weekly	None	1	1

<sup>1</sup> Minimum number of randomly scheduled inspections per day per location, unless specified as weekly or monthly.  
<sup>2</sup> The threat environment is defined by NSTISSI 7000 (C), *TEMPEST Countermeasures for Facilities* (U), Annex A (S), *TEMPEST Threat to Facilities* (U).

**TABLE A3.3. PDS TECHNICAL INSPECTION SCHEDULE<sup>1</sup>**

HIGHEST CLASSIFICATION OF DATA CARRIED	FACILITY LOCATION		
	U.S.	Outside U.S. in Low Threat Environment <sup>2</sup>	Outside U.S. in Medium Threat Environment <sup>2</sup>
SCI or TOP SECRET	1	1	3
SECRET	1	1	2
CONFIDENTIAL	1	1	1

<sup>1</sup> Minimum number of randomly scheduled technical inspections per year.  
<sup>2</sup> The threat environment is defined by NSTISSI 7000 (C), *TEMPEST Countermeasures for Facilities* (U), Annex A (S), *TEMPEST Threat to Facilities* (U).

**A3.3. Wire Line Criterion.** While the PDS provides physical security for the transmitted information, prevent the detection of the intended signal emanations from the wire line within the PDS. Meet this mandatory requirement as follows:

- A3.3.1. Use shielded twisted-pair or shielded multiconductor wire cables. Each cable must have a minimum of one overall non-ferrous shield meeting the requirements of AFSSM 7011, *The Emission Security Countermeasures Review*, or
- A3.3.2. Use shielded coaxial (triaxial) cable. Each cable must have a minimum of one overall non-ferrous shield and must meet the requirements of AFSSM 7011, or
- A3.3.3. Use opaque-clad fiber optic cable. Fiber optic cable must not contain a metallic conductor of any type.

**A3.4. Circuit Separation Security Criterion.** Ensure the distribution system is not accessed by those without appropriate clearance. Inhibit inappropriate cross connection of circuits.

A3.4.1. Access Controls for Collateral Circuits.

A3.4.1.1. Circuits of more than one classification level may use components of a single distribution system.

A3.4.1.2. Where the sharing of a single distribution system is feasible, the following criteria are mandatory:

A3.4.1.2.1. Access Points. Access to all points with breakouts of the higher level circuits must be restricted to appropriately cleared personnel. Access points containing classified circuits of different classification levels that do not have breakouts of the higher level circuits can be serviced by lower level cleared personnel when escorted by appropriately cleared personnel.

A3.4.1.2.2. Termination Boxes. Locate all termination boxes within the controlled access area.

A3.4.2. Access Controls for SCI. Ask the cognizant Special Security Office (SSO) for criteria and requirements pertaining to access controls for SCI.

**A3.5. Construction Criterion.** PDS construction criteria combined with operational security procedures are intended to allow for rapid detection of any attempted penetration of the PDS rather than ensuring the prevention of a penetration. Varying degrees of protection are afforded a PDS based on the PDS construction and other physical protection measures incorporated. Construction and protection requirements are determined from Table A3.1 and the geographical location of the PDS (within the United States or outside the United States). Determine requirements from Table A3.1.

**A3.5.1. Hardened Distribution System.** This must provide significant physical security protection for the wire line and is implemented by either the hardened carrier, alarmed carrier, or the continuously-viewed carrier as follows:

**A3.5.1.1. Hardened Carrier.**

A3.5.1.1.1. Construct the carrier of electrical metallic tubing (emt), ferrous conduit or pipe, or rigid-sheet steel ducting, using elbows, couplings, nipples, and connectors of the same material.

A3.5.1.1.2. Permanently seal (weld or epoxy) all connections completely around all surfaces. You may use hinged covers for rigid sheet ducting if you weld the hinges or fasten them with tamper-proof bolts and GSA listed high-security combination padlocks meeting federal specification FF-P-110 to secure the covers. If pull boxes are used, either seal the pull-box covers around the mating surfaces after construction or secure the pull boxes with a GSA listed high-security combination padlock meeting federal specification FF-P-110. Do not use boxes with prepunched knockouts.

A3.5.1.1.3. When the signal lines from the PDS terminate at a user equipment terminal location not maintained as a controlled access area 24 hours a day, protect the termination when not in use. Extend the PDS to a lock box using the same construction requirements as the rest of the PDS. Use a steel lock box with welded hinges or tamper-proof bolts, and tamper-proof hasp. Permanently mount the box to the facility structure at a location convenient to the terminal and to where the PDS terminates within the controlled access area. Secure the box cover with a GSA-listed high-security combination padlock meeting federal specification FF-P-110.

A3.5.1.1.4. If you bury the hardened carrier, bury it a minimum of 1 meter below the surface and on property owned or leased by the U.S. Government or the contractor having control of the PDS. Secure manholes with GSA-listed high-security combination padlocks meeting federal specification FF-P-110. If specification locks cannot be used, then use a standard locking manhole cover and approved microswitch alarms. If the carrier is buried in the earth on an installation outside the United States, encase it in approximately 8 inches of concrete or a concrete and steel container (of sufficient size to preclude surreptitious penetration in a period less than two hours as confirmed by laboratory tests).

A3.5.1.1.5. Install suspended hardened carrier systems only if the property traversed is owned or leased by the U.S. Government or contractor having control of the PDS. Elevate suspended systems a minimum of 5 meters. Install the elevated PDS to provide unimpeded inspection and clear of any obstruction or device that would encroach upon the system to facilitate tampering.

A3.5.1.1.6. Inspect the system at intervals indicated in Table A3.2. Illuminate the area containing the PDS.

**A3.5.1.2. Alarmed Carrier.** The principle protection concept for a PDS is to provide for unencumbered visual inspections to detect penetration, tampering, or unauthorized access to the clear text (unencyphered) classified information carried by the transmission line. Routing a PDS through an area which does not allow unrestricted visual inspection (above suspended ceilings, in walls, below raised floors) requires the use of alarms to detect attempts of penetration, tampering, or unauthorized access to the PDS.

A3.5.1.2.1. There are two alarming methods:

A3.5.1.2.1.1. Area Alarm. Intrusion detection alarms may be applied to the area through which the transmission line passes thus making this area a controlled access area and the transmission line a RED signal line. Use intrusion detection alarms which are approved by the cognizant security authority and meet the criteria in AFI 31-101V1, *The Air Force Physical Security Program*, for a controlled access area at the classification level of the information processed.

A3.5.1.2.1.2. PDS Alarm. Alarms may be applied to the PDS itself which, in effect, make the PDS a controlled access area. Use alarms which are approved by the cognizant security authority and meet the criteria in AFI 31-101V1, *The Air Force Physical Security Program*, for a controlled access area at the classification level of the information processed. Operational plans and procedures for a PDS alarm will be the same as if the PDS were an alarmed controlled access area.

A3.5.1.2.2. The cognizant security authority ensures appropriate intrusion detection capabilities are used and that all alarm information is included in the PDS plan. An alarm condition will shut down the RED signal line within the alarmed area or the alarmed PDS. Use of the RED signal line is not allowed until an inspection is performed and the reason for the alarm is determined.

A3.5.1.2.3. Construct the carrier of electrical metallic tubing (emt), ferrous conduit or steel pipe, using elbows, couplings, nipples, and connectors of the same material. Connections and pull boxes need not be sealed when the PDS is alarmed. Do not use boxes with prepunched knockouts.

A3.5.1.2.4. When the signal lines from the PDS terminate at a user equipment terminal location not maintained as a controlled access area 24 hours a day, protect the termination when not in use. Extend the PDS to a lock-box. Spot weld or epoxy all joints of the PDS within the user equipment terminal location. Use a steel lock-box with welded hinges or tamper-proof bolts, and tamper-proof hasp. Permanently mount the lock-box to the facility structure at a location convenient to the terminal. Secure the lock-box cover with a GSA-listed high-security combination padlock meeting federal specification FF-P-110.

A3.5.1.2.5. Perform technical inspections at intervals indicated in Table A3.3. Perform alarm verification checks at intervals specified by the cognizant security authority.

A3.5.1.3. **Continuously-Viewed Carrier.** To use a continuously-viewed carrier PDS, the guard force must keep the circuit under continuous observation 24 hours per day (not just when operational). Such circuits may be grouped together, but must be separate from all non-continuously-viewed circuits to ensure an open field of view.

A3.5.1.3.1. Standing orders include the requirement to investigate any attempt to disturb the distribution system.

A3.5.1.3.2. Appropriate security personnel investigate the area of attempted penetration within 15 minutes.

A3.5.1.3.3. This type of PDS cannot be used for TOP SECRET or Sensitive Compartmented Information (SCI) data in any areas outside the United States or off-base within the United States.

A3.5.2. **Simple Distribution System.** This system provides a reduced level of physical protection as compared to the hardened distribution system. When allowed by Table A3.1, construct the simple distribution system as follows:

A3.5.2.1. **Hardened Carrier.** The PDS may use any hardened carrier in existence.

A3.5.2.2. **Simple Carrier.**

A3.5.2.2.1. The data cables must be installed in a carrier.

A3.5.2.2.2. Construct the carrier of emt, ferrous conduit, or polyvinyl chloride (PVC) pipe of at least a schedule-40 grade material. Spot weld or epoxy emt joints. Use PVC solvent to seal PVC joints. Contain access points within the controlled access area.

A3.5.2.2.3. If pull boxes are used, either seal by spot welding or epoxy the pull-box covers after construction or secure the pull boxes with a GSA listed high-security combination padlock meeting federal specification FF-P-110. Do not use boxes with prepunched knockouts.

A3.5.2.2.4. Inspect the system at intervals shown in Table A3.2.

**NOTE:** Take precautions to ensure that general construction practices do not void the security requirements of other paragraphs in this attachment.

### TECHNICAL INSPECTIONS

**A4.1. General.** This attachment provides requirements for establishing and completing technical inspections of an installed PDS. Conduct technical inspections at the minimum intervals according to Table A.3.3. Technical inspections must be performed within the intervals specified, but the schedule should remain random and unannounced. The intervals specified in Table A.3.3 are minimum requirements. Sometimes the local threat assessment and risk analysis results may indicate a need for more frequent inspections. In these situations, the DAA should increase the frequency as deemed appropriate.

**A4.2. Responsibilities.** Ensuring completion of inspections according to the schedule is the responsibility of the activity identified in the PDS plan, this is normally the owning or using activity. The identified organization will either complete the inspections or coordinate with other organizations on base (for example, wing communications organization) to have appropriately cleared personnel complete the inspection.

A.4.2.1. Because of the technical nature of PDS technical inspections, personnel familiar with communications systems installations and maintenance, or similar technical experience and knowledge of electronics, should conduct or assist in conducting the technical inspections.

**A4.3. Requirements.** Technical inspections consist of a detailed visual inspection of the entire PDS route and an electrical characterization of the PDS when visual inspections are not possible, as in the case of a buried PDS.

A4.3.1. The detailed visual inspections should include all components, such as: terminal boxes, junction boxes, pull boxes, associated box covers and cover gaskets, manhole access points, connections, connectors, amplifiers, line conditioning equipment, distribution frame connections, optical transmitters, optical receivers, ground connections, locks, lock hasps, hinges, and lock mechanisms.

A4.3.1.1. Open and inspect every manhole cover, locked terminal box, and other locations where locks are used to secure access points. Change all lock combinations as part of the inspection. Record and store lock combinations according to established directives. Report instances of inoperative locks as a physical security COMSEC incident according to AFI 33-212, *Reporting COMSEC Incidents*, and the established reporting procedures.

A4.3.1.2. Accomplish an initial technical inspection at the completion of the PDS installation. This should be accomplished by personnel of the installing activity assisted by personnel from the activity identified to perform the continuing inspections. During the initial inspection, take photographs of the PDS to document the physical configuration. Pay particular attention to any terminal boxes, junction boxes, pull boxes, manhole access points, and any other areas where access to the PDS cables or wiring may be possible. Ensure each photograph is marked as to the exact position or location of the area photographed. You may devise any system of labeling which will provide for the positive identification of the location shown in the photograph. Narratives which further describe the area shown should also accompany these photographs.

A4.3.1.3. Place the photographs and accompanying narratives in the completed PDS file for use during subsequent inspections to assist in identification of possible tampering. A compilation of photographs, when identified with a specific PDS or system and location may be classified. In all cases treat as sensitive information; handle, mark, and store accordingly.

A4.3.1.4. During the subsequent technical inspections look for changes in the technical aspects of the PDS; for example, bypass circuitry, attachment or removal of devices or components, inappropriate or suspicious signal levels, and mechanical integrity of the PDS.

A4.3.2. Where the PDS is buried and cannot receive a close visual scrutiny, establish an electrical characterization of the PDS. 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 recorded readings, and any other electrical measurements that may be recorded and retained. Use a characterization method which will allow use of locally available test equipment and is within the capabilities of the local operating and maintaining function for conducting subsequent technical inspections. Record and compare measurements taken at subsequent technical inspections to the previously recorded baseline measurements to aid in identifying possible tampering attempts. When test equipment is locally available and resident expertise allows, complete an electrical characterization of all PDS installations.