



CAMP PENDLETON REQUIREMENTS SUPPLEMENT

MCIWEST G-6 TELECOMMUNICATION REQUIREMENTS SECTION 271400 (PDS)

Clayton CIV Steve S

Garland N. Copeland
Assistant Chief of Staff/MCIWEST G-6
MCB Camp Pendleton, California

OCTOBER 17, 2014

271400 TELECOMMUNICATIONS PROTECTIVE DISTRIBUTION SYSTEM

PART 1 GENERAL

1.0 REFERENCES

SECNAV M-5530.36	Physical Security Manual Secure Rooms
SECNAV M-5530.30	Information Security Manual
MCO IA/PUB 5239-22	PDS Policy and Regulations
UFC-3-580-10	UFC Design Specifications
Military Handbook 1013/1b	Construction Design
NSTISSI No 7003	
NSTISM 2/95	RED/BLACK information Systems Security Instruction
HSPD-7	Critical Infrastructure Protection Program
HSPD-12	Background Vetting
MCO 5510.14A	Marine Corps Physical Security Program Level II Restricted Areas

1.1 CLASSIFIED INFORMATION INFRASTRUCTURE SYSTEMS

National Security Telecommunications and Information Systems Security Instruction (NSTISSI) No. 7003, Protective Distribution Systems (PDS), provides guidance for the protection of wire line and optical fiber PDS to transmit unencrypted classified National Security Information (NSI). This instruction is effective upon receipt and supersedes NACSI No. 4009, Protected Distribution Systems, dated 30 December 1998 and Appendix K, NACSEM 5203, Guidelines for facility Design and RED/BLACK Installation, dated 30 June 1982. Please check with your agency for applicable implementing documents. Any agency that are contemplating the use of a PDS solution must protect the transmission of unencrypted classified National Security information (NSI) and must follow the Protective Distribution Systems dated Dec 13, 1996.

1.1.1 PLANNING, DESIGN AND ESTIMATING

MCIWEST G-6 requires design approvals of all Protected Distribution Systems (PDS) Design prior to the installation of the PDS. The overall security afforded by PDS is the result of a layered approach incorporating various protection techniques. The emphasis is placed on "detection" of attempted penetration in lieu of "prevention" of penetration. Criteria called out are based on threat or risk analysis relative to the location of the PDS. This generally results in reduced requirements and cost savings during installation and maintenance of PDS. The decision as to what extent the guidance provided in ANNEX B is followed ultimately rests with the department or agency Approval Authority. The references listed in UFC-3-580-10 will be adhered to when PDS are included on designs for new facilities that will require secure space modifications for processing up to secret information.

PART 2 CLASSIFICATION OF SPACES AND COMPONENTS

2.1 CLASSIFIED INFORMATION INFRASTRUCTURE SPACES

2.1.1 UNCONTROLLED/PROTECTED ACCESS AREA (UAA)

A physical area (e.g., a military base in a foreign country) that is not under direct U. S.

Marine Corps Installation West (MCIWEST) G-6

Camp Pendleton Requirements (CPR) Section 271400 (PDS)

Page 1

10/2014

physical control and to which unauthorized personnel may gain access. Access to the area is not necessarily based upon the presentation of an approved credential. A PDS shall not be installed in a UAA. If other approved protective measures (e.g., use of a NSA Type 1 cryptographic device) cannot be implemented, a waiver shall be requested from either CNO (N612) via the Space and Naval Warfare Systems Center (SPAWARSYSCEN) Charleston (Code 723) PDS Certification Authority or Headquarters Marine Corps Command, Control, Communications, and Computers (HQMC C4) via the Certification and Accreditation Activity at the Marine Corps Network Operations and Security Command (MCNOSC).

2.1.2 LIMITED ACCESS AREA (LAA)

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

2.1.3 RESTRICTED ACCESS AREA (RAA)

A physical area (e.g., building, room, etc) that is under physical control and to which only personnel cleared to level of the information being processed are authorized unrestricted access. Authorized personnel escort all other personnel. A RAA shall comply with RAA physical requirements section 4. Safeguarding and storage of magnetic and hard copy media will be in accordance with IA 5239-22.

2.1.3.1 DOORS (RAA)

The access door to the area shall be a security deadbolt lock with a one inch throw, with cylinder which meets the requirements of Underwriters Laboratories Inc. UL-437 standard key lock, 7TH edition dated 4 Aug 2000. The hinge pins of out swing doors shall be pinned brazed or spot weld to prevent removal. Doors other than access doors shall be secured from the inside (for example, by a dead bolt lock, panic dead bolt lock, or rigid wood or metal bar which extends across the width of the door, or by any other means that will prevent entry from the outside).

2.1.3.2 LOCKS (RAA)

The locks shall meet FF-L-2890 Specifications, UL-437 Key Cylinder High Security dead bolt with a 1 inch throw, are requirements, for Camp Pendleton, we use the UL-437 Schlage Primus or Everest due to lock smith having the ability and training to R-KEY locks. This should include blank keys for every facility.

2.1.4 WALLS, FLOORS AND ROOF (CAA)

The construction shall be of permanent construction materials (i.e. plaster, gypsum, wallboard, metal panels, hardwood, plywood, or other materials) that offer resistance to and evidence of unauthorized entry into area. Wall shall be extended from true floor to true ceiling with permanent materials or 18-gauge expanded steel screen. If the walls cannot be extended, then an intrusion detection system shall be installed to monitor the space above the terminal.

2.1.4.1 DOORS (CAA)

The access door to the area shall be substantially constructed of wood, metal or solid material. If double doors are installed, an astragal will be installed on active leaf of the door.

2.1.4.2 LOCKS (CAA)

The locks shall meet FF-L-2890 Specifications requirements, for Camp Pendleton. CAA doors will use XO-9 Locks.

2.1.4.3 WINDOWS (CAA)

All windows which might reasonably afford visual observation of classified activities within the facility shall be made opaque or equipped with blinds, drapes or other coverings. Windows less than 18 feet above the ground (measured from bottom of window), or are easily accessible by means of objects directly beneath the windows, will be locked at all times. The locking mechanism and window construction shall be such as to provide indications, of any attempt of forced entry. If the construction is inadequate to provide said indication, then protective coverings, such as bars, need to places over the windows. The protection provided to the windows need be no stronger than the strength of the contiguous walls. Windows containing climate control units (e.g. air conditioners) must be secured in a manner to provide indications of any attempt at forces entry.

2.1.4.4 OPENINGS (CAA)

Utility openings such as ducts and vent shall be kept at less than man-passable (96 square inches). Openings larger than 96 square inches shall be hardened per Military Handbook 1013/1B.

PART 3 DESIGN CONSIDERATIONS

3.1 PROTECTION DISTRIBUTION SYSTEMS (PDS) DESIGN CONSIDERATIONS

The approval for system design **MUST** be approved by the MCIWEST G-6 prior to construction.

3.1.1 PDS DESIGN CONSIDERATIONS

A system of carriers (conduits or a duct-bank) that are used to distribute NSI.

- a. PDS must originate within a SR or CAA
- b. PDS must terminate within a SR, CAA, or RAA
 - 1. Lock box must be utilized when terminating within a RAA.
 - 2. Workstations must be protected in a RAA
- c. PDS may traverse but not terminate within a LAA
- d. PDS may not traverse or terminate in a UAA

3.2 CATEGORIES OF PROTECTION DISTRIBUTION SYSTEMS (PDS)

3.2.1 BURIED

- a. Maintenance/Hand holes must be sealed (welded) or locked with an approved lock that is inspect-able or alarmed.
- b. The carrier should enter the building from underground.
- c. Carriers traversing crawlspaces require rigid steel pipe and/or other additional measures.
- d. If the carrier enters the side of the building, metal conduit or plastic conduit encased in concrete must be used.

3.2.2 SUSPENDED

- a. Uncommon.
- b. Used between buildings in close proximity when a buried carrier is not possible or cost effective.
- c. The carrier must be 5 meters high with no poles.
- d. The ends of carrier must terminate in SR or CAA.
- e. Area traversed must be owned or leased by U.S.

3.2.3 HARDENED

- a. Most common type of carrier inside buildings.
- b. The carrier must be constructed from metallic conduit (such as EMT).
- c. Armored cable and flexible spiral wound conduit cannot be used.
- d. Joints must be sealed with epoxy

3.2.4 ALARMED

- a. Does not require a daily visual inspection.
- b. Subject to false alarms.
- c. Used when an IDS is already installed in the facility.
- d. Used for a PDS installed out of view, such as above false ceilings and below raised floors.
- e. Two types of Alarmed Carriers approved:
 - 1. Volumetric IDS, Area surrounding entire length of PDS must be covered.
 - 2. Fiber Optic Intrusion Detection System (FOIDS) (such as Fiber SenSys or Interceptor).

3.2.5 CONTINUOUSLY VIEWED CARRIER

- a. Uncommon.
- b. Used when the area is already monitored by a guard or a camera monitoring system.
- c. The carrier must be in metal or plastic conduit.
- d. Must be viewed 24/7.

PART 4 EXECUTION

4.1 PRODUCT / INSTALLATION



4.1.1 PDS CARRIER

- a. The PDS carrier must be installed in view.
 - 1. Except Alarmed carriers.
 - 2. Generally installed just below false ceiling.
 - 3. May not be installed above false ceiling, behind furniture or in walls.
- b. The carrier should be marked at distances less than 3 meters (do not use the red markings).
- c. The PDS is routed across/along hallways below the ceiling as shown below.

4.1.1 PULL AND DROP BOXES

- a. Boxes must be continuous metal.
- b. No knockouts or pre-punched knockouts.
- c. Covers must be welded or sealed with epoxy.
- d. No removable hinges.
 - 1. Hinges with exposed ends are not allowed, even with epoxy.

- e. Lock boxes may be used for re-entry into pull boxes or for terminations in an RAA.
- f. Lock boxes must meet requirements of pull box.
- g. Must have permanently secured locking hardware.
 - 1. No screws.
 - 2. A locking tab protruding through a slot in the door is the best type.
- h. In a RAA, the network cable must be secured in the lock box.

Good Example

- Hidden Hinge
- No knockouts
- Tab protruding through slot

McKinstry Enclosures (No longer available) or approved equal shown below



Good Example

- Hidden Hinge
- No knockouts
- External Tab

Performance Metal Fabricators (9930-805-CB-series) or approved equal shown below



Good Example

Joints must be sealed around all mating surfaces as shown below



Good Example

Non-locking pull boxes and conduits must be bonded around all mating surfaces as shown below



4.1.2 PHYSICAL SECURITY LOCKS FOR RAA

- a. UL-437 (with 1 inch throw) with a security tumbler as shown below



4.1.3 PULL/LOCK BOX LOCKS

- a. The only lock currently available that meets the PDS lock specification is the S&G 8077.
- b. National Stock Number for bulk purchase (24) of 8077-102 is 5340 00 285 6523.
- c. Unified Facilities Criteria (UFC) Protected Distribution Systems for Classified Information Infrastructure 21400.



PART 5 PDS CERTIFICATION

5.1 PDS CERTIFICATION GUIDANCE

5.1.1 MCIWEST G-6 PDS INSPECTOR

All PDS solution that is installed will be inspected by the MCIWEST G-6 PDS inspector. Once locally approved the PDS package will be submitted to the Certified Tempest Technical Authority (CTTA). Please direct questions to the MCIWEST G-6 PDS Inspector at (760) 763-1975.

5.1.2 CERTIFIED TEMPEST TECHNICAL AUTHORITY (CTTA)

The CTTA will validate the package and submit the package for approval to the Certification Authority (CA), HQMC Designated Approving Authority (DAA).

5.1.3 CERTIFICATION AUTHORITY (CA) HQMC DAA

The CA shall validate all areas described in the PDS approval request except SR, CAA or RAA that does not protect magnetic media, follow SECNAVINST 5510.36. Once approved by the CA an Authority to Connect (ATC) and Authority to Operate (ATO) will be provided to the MCIWEST G-6 PDS Inspector.

PART 6 DAMAGE OF TELECOMMUNICATION INFRASTRUCTURE

6.1 CONTRACTOR DAMAGE

In the event of damage to a telecommunication pathway or cabling the contractor must **IMMEDIATELY contact the MCIWEST G-6 Help Desk at (760) 763-0173**. Restoration of services must be completed within **24 HOUR** of outage origination. Promptly repair indicated telecommunication pathways and infrastructure damaged during site preparation or construction. Damages to telecommunication pathways or infrastructure

that was not indicated by as-built provided or not identified by third party locating services, which are caused by contractor operations, shall be treated as Changes under the terms of the Contract Clauses. When Contractor is advised in writing of the location of a non-indicated line or system, such notice shall provide that portion of the line or system with "indicated" status in determining liability for damages. **All repairs MUST be approved by the MCIWEST G-6.** Compounds or tape are not acceptable substitutes for heat shrinkable end caps and will not be approved.

PART 7 ACCESSSES TO CONTROLLED SPACES

7.1 REFERENCES

DISA CCRI	Command Cyber Readiness Inspection Regulations
MCO 5530.14A	Marine Corps Physical Security Program
SECNAV M-5510.36	Physical Security Program
CVS HSPD-12	Homeland Security Protection Directive (Vetting of all DoD, Federal, Active and Contractors)
HSDP-7	Critical Infrastructure Protection Program

7.2 REQUESTING ACCESS TO A CONTROL MCIWEST G-6 SPACE

All contractors requiring access to Restricted Area (LEVEL II) or Secure Spaces must follow and be familiar with HSPD-12 regulations and Industrial Security Program DD-254 Regulations for access to secure spaces Ref: SECNAVISNT M-5530.36. Those contractors that meet these regulations may obtain a DOD CAC card under the CVS Program; this will eliminate the G-6 having to escort those contractors that require access to controlled spaces. Once a contractor is properly vetted he/she will receive a proper credential and receive a security brief prior to given access to MCIWEST G-6 controlled spaces. That DOD CAC also allows him/her to obtain a base DECAL for the duration of the contract. Not all contractors require a DOD CAC. There can be a few that can escort the remaining contractors that require access to controlled spaces, those security measures will be covered during the security brief. Access will be coordinated through the MCIWEST G-6 Information Technology Security Manager (ITSM) (760) 763-1975 or the Customer Service Desk (760) 763-0173.

Any questions pertaining to this document please contact MCIWEST G-6 Infrastructure Planning (760) 763-5263.