BY ORDER OF THE COMMANDER
AIR FORCE SPECIAL OPERATIONS
COMMAND

AIR FORCE SPRCIAL OPERATIONS
INSTRUCTION 33-201

8 OCTOBER 2008

Communications and Information

CONTROLLED ACCESS AREA

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

ACCESSIBILITY: Publications and forms are available for downloading or ordering on the e-Publishing website at www.af.mil/e-publishing on AF Link.
RELEASABILITY: There are no releasability restrictions on this publication.

OPR: HQ AFSOC/A6OS

Certified by: HQ AFSOC/A6O
(Lt Col Kyna R. McCall)

Pages: 7

This instruction implements AFI 33-201V8, *Communications Security Protected Distribution Systems (PDS)*. It provides AFSOC guidance to Emissions Security (EMSEC), Protected Distribution System (PDS) and Facility Hardening requirements necessary to meet the Controlled Access Area (CAA) intent. Facility compliance with this instruction will enable SECRET level communications without PDS for RED and BLACK lines of voice, video and data transfer. Higher levels of classification require additional measures of protection. This instruction does not apply to the Air National Guard (ANG) and Air Force Reserve Command (AFRC) units which augment HQ AFSOC. Ensure all records created as a result of processes prescribed in this publication are maintained in accordance with AFMAN 33-363, *Management of Records*, and disposed of in accordance with the Air Force Records Disposition Schedule (RDS) located at https://afrims.amc.af.mil/. Refer recommended changes and questions about this publication to the Office of Primary Responsibility (OPR) using the AF Form 847, *Recommendation for Change of Publication*, and route AF Form 847s from the field through the appropriate functional chain of command.

1. Definitions. National Security Information (NSI) is categorized as Confidential, Secret, or Top Secret. A Protected Distribution System (PDS) is a system of carriers (conduits, ducts, etc) that are used to distribute NSI. TEMPEST is the controlling of compromising emanations for PDSs, cable shielding and RED/BLACK separation as required by TEMPEST countermeasure instructions.

2. Controlled Access Area (CAA). A CAA is a physical area, building or room, which is under physical control and to which only personnel cleared to the level of the information being processed are authorized unrestricted access. All other personnel are either escorted by authorized personnel or are under continuous surveillance (manually or via camera). A PDS may originate and terminate in a CAA controlled at the level of the NSI carried by the PDS. Within a CAA, a PDS will not be required for systems at or below classification level of the CAA. Safeguarding of magnetic and hardcopy media will be in accordance with AFI 33-202V1, *Networks and Computer Security*, and AFI 33-401, *Implementing Air Force Architectures*. When the CAA is not occupied, it must be secured in such a manner that an undetected break-in would not be possible. The PDS Certification Authority (CA), the host base IA, certifies a CAA.

2.1. The local Designated Approving Authority (commander or Designated Approving Authority Representative) may certify a CAA when no PDS is required. All the distribution systems must be within the CAA. The CAA certification must be provided in the accreditation documentation for the network.

2.2. The objective of the CAA is to deter unauthorized personnel from gaining access to classified systems, including attached workstations, and to ensure unauthorized access is discovered.

2.2.1. Any interior or exterior wall, floor and roof shall be of permanent construction materials from floor to ceiling. Doors shall be solid core and will have a high security, dead bolt lock. When double doors are used, an astragal (a protective exterior molding) will be installed on the active leaf of the door. The hinge pins of out swing doors shall be preened, brazed, or spot-welded to prevent removal. Locks used to secure a CAA must be resistant to drilling and physical penetration and lock pick. Federal spec FF-L-2740 is typically the XO7/9 series used on safes and secure rooms. Medeco Maxum, ASSA and Schlage also offer locks used to secure a CAA (Maxum series SKU D11W-0100, 0102; V6000 series ASSA locks; Primus cylinder B-860 series locks respectively).

2.2.2. All windows which might reasonably afford visual observation of classified activities shall be made opaque or equipped with blinds, drapes, or other coverings. All windows that are less than 18 feet above the ground measured from the bottom of the window, or are easily accessible by means of objects directly beneath the windows shall be constructed from or covered with materials which provide indications of any attempt of forced entry.

2.2.3. After work hours the CAA shall have procedures to ensure doors are secured at the end of the work day. During work hours the CAA shall be occupied or have access controlled through use of a cipher or simplex lock or a swipe badge system or have the doors locked when unoccupied.

3. Restricted Access Area (RAA). A physical area (e.g. building, room or annex) to which only personnel cleared to the level of the information being processed are authorized unrestricted access but does not meet all of the physical security requirements of a CAA (See Attachment 2).

3.1. A PDS may be terminated in an RAA controlled at the level of the NSI carried by the PDS if: 1) a lock box is used to protect the PDS termination, 2) workstations will be secured or the removable hard disk will be removed and stored in a GSA approved security container. The access requirements are the same as a CAA. The physical security required is less than a CAA. The PDS CA certifies an RAA. A PDS and a lock box equipped with a GSA approved PDS lock are required in an RAA. The PDS shall be extended within the RAA to a location in close proximity to the workstation and shall be terminated in the lock box which contains the connection for the network. The workstation shall be connected to the network via this termination. The workstation shall be disconnected from the network and the termination secured when left unattended and at the end of the day.

3.2. Printers and other devices attached to a classified system shall be located in either a CAA or Secure Room (SR) location. A SR is one in which access is controlled to preclude unauthorized access. This may be accomplished through the use of a cleared person or by an access control device or system. Access shall be limited to authorized persons who have an appropriate security clearance and a need-to-know for the classified material/information within the area. Persons without the appropriate level of clearance and/or need to know shall be escorted at all times by an authorized person. SR processing classified material shall be accorded supplemental protection during non-working hours. If a printer is located in a RAA, then the network connection will be disconnected and secured when not in use and at the end of the day. Tamper evident tape will be used to seal all printer openings processing classified information that allow access to the printer electronics or cartridge area. Classified magnetic media must be properly stored. Contact Wing Information Assurance (IA) for tamper tape distributors.

3.3. The walls, floor and roof construction shall be of permanent construction materials; i.e. plaster, gypsum wallboard, metal panels, hardboard, wood, plywood or other materials offering resistance to, and evidence of unauthorized entry into the area. Walls need not be true floor to ceiling. Door requirements are the same as CAA requirements except solid core door is not required. The door shall be substantially constructed, access doors locked with a high security lock, swipe badge or cipher lock used to control access, hinge pins of out swing doors shall be preened, brazed or spot-welded to prevent removal. When double doors are used, an astragal (a protective exterior molding) will be installed on the active leaf of the door.

3.4. Windows shall be made opaque or blinds, curtains, or shades shall be used to prevent visual observation. Windows that are less than 18 feet above the ground will be locked at all times or permanently sealed. The locking mechanism shall be such as to provide indications of any attempt of forced entry.

3.5 Entry to an RAA must be controlled through the use of high security locks, swipe card system, or cipher locks. Cipher locks are not the preferred method and must be changed frequently. Whenever any individual with access to the combination departs or no longer has access to the RAA, the cipher lock combination must be changed. When lock boxes are open and/or classified is not secure, the owner/user must ensure that physical security measures are in place to prevent unauthorized access. This includes accidental or inadvertent access. This will include the closing of office doors, limiting access to hallways that may allow inadvertent viewing, and the posting of “classified work in progress” signs. Unauthorized personnel must be physically blocked from gaining access or viewing work spaces when lock boxes are open or classified is in use. Implementing CAA entry control standards for an RAA may be deemed necessary based on the volume and frequency of NSI usage.

4. Limited Access Area (LAA). A physical area which is under direct U.S. physical control, and to which only authorized personnel are admitted (e.g. a military base). Access is based on presentation of approved credential such as picture badge with/without other technologies or visitor pass issued after verification of picture ID. Verification can be via guard inspection or electronic processing (See Attachment 2).

4.1. Potential LAA areas of interest are breezeways between facilities, foyers that bridge CAA locations, etc. and will always require PDS. A PDS shall not terminate within a LAA (even into a lock box).

5. Unlimited Access Area (UAA). A physical area (e.g. military base in an OCONUS location) which is not under direct U.S. physical control and to which unauthorized personnel may gain unrestricted access. A PDS shall not be installed in a UAA.

6. Physical Security and Access Control. Access procedures IAW this document are an owner/user responsibility. Specific procedures must be detailed in facility and unit Operating Instructions. SRs, CAAs and RAAs require access control to the level of information processed. Consideration must be taken concerning unescorted custodial and delivery personnel, not just employees. Foreign nationals, even with a clearance, cannot have unescorted access unless they are authorized account holders on the network. Visitors are allowed if escorted and cannot view classified information unless visitors are sponsored, have security clearances verified by the visited unit's security manager and the visitor(s) has/have a need to know.

7. Badging Process for Visitors in a CAA. CAA visitors are required to send security clearances through JPAS to the visited organization's security manager.

7.1. Unescorted access to a CAA will be limited to individuals who have a valid and current clearance level commensurate with the level of NSI stored within. Entry authority may also be verified by a DoD picture ID and a check on the JPAS roster. Certain automated entry control systems (AECS) may also be utilized to grant unescorted access to a CAA. Authorized AECS for access into a CAA include a swipe card and PIN or swipe card and biometric validation. The swipe card is only issued to personnel that require access and have a valid clearance. The PIN or biometric Personally Identifiable Information (PII) ensures that the swipe card is only used by the authorized user. Swipe card systems that do not validate the user as the owner of that swipe card are not authorized access into a CAA. A CAC card AECS with biometric verification would also be sufficient for access to a CAA if the AECS allows the manager of the CAA to build an Entry Authorization List (EAL) in the AECS system. These systems must limit entry to personnel who have been identified by the owning agency as cleared into the CAA and had their clearances validated in JPAS. These systems must be immediately updated when personnel on the EAL no longer have access. Future biometric systems that validate both the identity of the individual and the individual's clearance level may be considered for entry into a CAA.

7.2. Escorted badges are granted to active duty military members, civilians and contractors who do not have SECRET level clearances or higher. Visitors with escort badges must be accompanied by their sponsor at all times within the CAA.

8. Janitorial Employees, Concessionaires, and Maintenance Within a CAA. Janitorial employees and concessionaires within a CAA must have a clearance to the level of the facility/area being accessed; be escorted or be on visual surveillance at all times.

ANTHONY W. FAUGHN, Colonel, USAF
Director, Communications and Information

Attachment 1

GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

References

AFI 33-201V8, *Communications Security Protected Distribution Systems (PDS)*
AFI 33-202V1, *Networks and Computer Security*
AFI 33-401, *Implementing Air Force Architectures*
AFMAN 33-363, *Management of Records*
DOD 5200.1R, *Information Security Program*

Abbreviations and Acronyms

AECS---Automated Entry Control Systems
CA---Certification Authority
CAA---Controlled Access Area
CAC---Common Access Card
EAL---Entry Authorization List
EMSEC---Emissions Security
IA---Information Assurance
IDS---Intrusion Detection System
LAA---Limited Access Area
NSI---National Security Information
PDS---Protected Distribution System
PII---Personally Identifiable Information
PIN---Personal Identification Number
RA---Restricted Area
RAA---Restricted Access Area
SR---Secure Room
UAA---Unlimited Access Area

Attachment 2

PHYSICAL REQUIREMENTS

Table A2.1. Physical Requirements

	Secure Room	**Area Type CAA**	**RAA**
Construction			
Solid core construction	Yes	Yes	Yes
True ceiling, wire mesh, or Intrusion Detection System (IDS)	Yes	Yes	Yes
Openings			
No openings, openings <96 sq in. manbars or IDS	Yes	Yes	No
Doors			
Substantial construction	Yes	Yes	Yes
Solid core, metal or metal clad	Yes	Yes	No
Non-removable hinge	Yes	Yes	Yes
Astragal on active leaf	Yes	Yes	Yes
Locks			
Approved Locks (e.g. GSA, NSA, AFCA)	Yes	No	No
Access Control			
Swipe proximity or cipher lock	Yes	Yes	Yes
IDS, continuous occupancy, or periodic inspection	Yes	No	No
Viewing			
Opaque windows, blinds or curtains, or not in view	Yes	Yes	Yes
Windows			
No windows, or covered windows, or windows with manbars, or windows greater than 18 ft	Yes	No	No
No windows, or covered windows, or windows with manbars, or windows less than 18 ft or tamper evident	No	Yes	No
No windows, or covered windows, or windows with manbars, or windows less than 18 ft or substantial lock	No	No	Yes