ATTACHMENT O

VASD POLICE SERVICES PHYSICAL SECURITY REQUIREMENT CHECKLIST

IT Telecom/Data Connection Closets

LOCATION EVALUATED: **IT Telecom/Data Connection Closets**

DATE EVALUATED:_____

EVALUATION CONDUCTED BY: _____SERVICE REPRESENTATIVE: _____

FACILITY:_____BUILDING:_____ROOM(S):_____

REQUIREMENTS PER VA HANDBOOK 0730/4 APPENDIX B FOR THIS AREA INCLUDES:

A. Walls:

Exterior walls of brick and masonry construction are acceptable. Exterior walls which are composed of wood frame and siding require an interior backing of steel security screen mesh or sheet partition.

REQUIREMENT MET ☐ **DOES NOT MEET REQUIREMENT** ☐

B. Doors and Door Locks:

The locking requirements (including access controlled egress doors) outlined in National Fire Protection Association (NFPA) Life Safety Code standard, latest edition, 101-7.2.1.5 and 7.2.1.6 must be followed.

(1) Door Construction.

Doors are of 45 mm (1-3/4 in.) solid core hardwood or hollow steel construction. Dutch or half doors are unacceptable. Removable hinge pins on door exteriors must be retained with set pins or spot welded, preventing their removal. This applies only if the hinge pins are on the outside of the doors and door frames. Hinge pins will be on the outside if the door opens outward.

(2) Mechanical locking systems.

Where mechanical lock systems are used, installed lock sets must allow for single motion egress. The installation of high security exit devices meeting NFPA Life Safety Code standards is appropriate**.**

(a) Glass doors or doors with glass panes must have one lock set that is key operated from the interior of the protected area. **Note:** Fire code prohibits locks from being locked from the inside that require a key to exit. The intent is that there must be two locks, one of which must be key operated. The other lock can be key, combination or electronic. (NFPA 101, 7.2.1.5.2) locks, if provided, shall not require the use of a key, a tool or special knowledge or effort for the operations from the egress side.

(b) Steel doors will not be set into wooden frames.

(c) Doors set in steel frames must be fitted with a mortise lock with a deadlock feature. IAW ANSI/BHMA A156.13 American National Standards for Mortise Locks. (d) The day lock on the main door must be automatically locking, with a minimum 19 mm (3/4 in.) dead bolt and inside thumb latch. Access to electronic locking systems, combinations or keys to day locks will be restricted to service employees and electronic access and/or combinations changed

immediately on the termination or reassignment of an employee. See paragraph 8 of this appendix for a detailed description of key control systems.

(3) Electronic/Magnetic locking systems.
Where installed, electronic locking systems will include an automatic “request to exit” sensor and a “push to exit” manual lock release switch. Refer to the NFPA Life Safety Code for details.

REQUIREMENT MET ☐ **DOES NOT MEET REQUIREMENT** ☐

C. Other Room Access Means:
Interstitial overhead areas which enable entry into a secure room from an unsecured room must be barricaded by the installation of a suitable partition in the interstitial space which prevents "up and over" access. Openings in construction above ceilings or below raised access floors shall be protected as below requirement.
All vents, ducts, and similar openings more than 96 square inches (620 cm2) that enter or pass through space shall be protected with either bars or grills. If one dimension of the duct measures less than six inches (150 mm) or duct is less than 96 square inches (620 cm2), bars are not required; however, all ducts must be treated to provide sufficient sound attenuation. If bars are used, they must be 1/2-inch (12.7 mm) diameter steel welded vertically and horizontally six (6) inches (150 mm) on center; if grills are used, they must be of 9-gauge expanded steel.

REQUIREMENT MET ☐ **DOES NOT MEET REQUIREMENT** ☐

D. Special Key Control:
Room door lock keys and day lock combinations, where applicable, are Special Keys as defined in paragraph 8.d. (10) of this appendix.

REQUIREMENT MET ☐ **DOES NOT MEET REQUIREMENT** ☐

OPTIONAL MEASURES PER VA HANDBOOK 0730/4 APPENDIX B FOR THIS AREA INCLUDES:

E. Electronic Physical Access Control Systems (PACS:
For monitoring and controlling access to areas identified as requiring high or medium levels of assurance.
PACS systems are not used for recording employee time and attendance.

(1) For pharmacies and similar Services, PACS will be used to protect the perimeter of operations areas. In the case of pharmacies, this refers to spaces where pharmaceuticals are mixed, packaged, assembled or otherwise prepared for distribution to patients. Administrative offices and similar spaces do not need to be protected with PACS, unless indicated by a local vulnerability assessment.

(a) Access Safeguard. To prevent learning codes through keypad observations or use of stolen or found access cards.

(b) Time Sensitive. The ability to program access by user, by shift and day.

(c) Area Sensitive. The ability to program access by door and area for each individual user.

(d) Fail-Safe. The ability to maintain access security if the system goes down (i.e. bypass key).

(e) Access Record/Audit Trail. The ability to provide for periodic or on demand print-out of names and time/dates of individual accessing. Records of access or audit trails will not be used for employee time and attendance purposes.

(f) User Coverage. The number of individual access codes that the system will accommodate.

(g) Personal Identifier Number (PIN) Codes. Access control systems protecting PACS high security areas, such as controlled substance storage, primary computer and communications rooms, research or clinical laboratories that store, use or develop bio-hazardous materials, require a PIN number as a secondary personal authentication to be used in addition to card readers. "Scramble Pad" type PIN readers are recommended when PIN systems are installed. See the table below for specific VA identified required locations.

(h) Biometric Systems. Biometric security systems are those that use a personal measurement, such as fingerprints, hand geometry, facial geometry or iris scans, as authentication. Biometric devices can be used in lieu of PIN systems in PACS high protected spaces, but only as a secondary form of authentication. Biometric measurements may also be used in addition to a PIN in high security applications.

(i) Compliance with Federal Standards. New installations or retrofitted access control systems will be compliant with technology described in Federal Information Processing Standard (FIPS) Publication 201, Personal Identity Verification of Federal Employees and Contractors, and the document "PACS Implementation Guidance, Version 2.2 (July 30, 2004), published by the Physical Access Interagency Interoperability Working Group of the GSA Government Smart Card Interagency Advisory Board. This requires that such systems will meet the ISO/IEC 14443 a/b, Parts 1-4 standard for contactless (proximity) card systems, or the ISO/IEC 7816 Standard for contact-type cards. Facilities may continue to use existing PACS that operate on older technology (Magnetic Stripe, 2nd Generation bar code, etc.) as an interim measure until replacement systems are acquired and installed as part of normal equipment lifecycles.

Further information on VA Smart Card operated PACS requirements can be found in the most recent edition of the document: "Physical Access Control Recommendations for the Department of Veterans Affairs." Guidance and assistance with the standards can be obtained from the OS&LE.

(j) PACS Assurance Level Designations. PACS provide a level of assurance regarding the identity of persons entering a protected space. The levels of assurance required are determined because of vulnerability or risk assessments and physical security surveys. In addition, the following indicates minimum requirements for specified VA protected activities.

For purposes of this policy, levels of assurance are defined as:

- **High** - Entry requires a valid access card used in conjunction with a secondary form of authentication. Either a Personal Identification Number (PIN) known only to the card holder, or a biometric measurement, or both, is used as the secondary authenticator.
- **Medium** - Entry requires the use of a valid access card.
- **Low** - Entry requires the visual authentication of a valid access card or facility identification card. The card may be inspected by a police officer or other designated staff upon entry into the protected space, or may just require that it is worn always in a visible manner; see VA Directive 0730, paragraph 2.n. Facilities may choose to use a more stringent protection level for any of these locations.

In addition, facilities may choose to protect other activities with PACS. Further information on PACS Assurance level designations is found in VA Handbook 0730, Part E, Paragraph 1.g.(5).

The following are minimum protection and assurance levels for facilities that have installed PACS:

Location PACS Assurance Level:

IT Telecom/Data Connection Closets= **High**

OPTIONAL MEASURE IN PLACE ☐

F. Closed Circuit TV:

Security Surveillance TV camera with motion detector feature on cameras and at monitor location. Telecommunications Support Service (197) may be contacted for obtaining technical assistance. See VA Handbook 0730, Part E for further details and considerations.

OPTIONAL MEASURE IN PLACE ☐

NOTES/OBSERVATIONS:

ATTACHMENT P

VASD POLICE SERVICES PHYSICAL SECURITY REQUIREMENT CHECKLIST

Warehouse/Bulk Storage

LOCATION EVALUATED: **WAREHOUSE STORAGE/BULK**

DATE EVALUATED:

EVALUATION CONDUCTED BY:_____ SERVICE REPRESENTATIVE:_____

FACILITY: _____BUILDING: _____ROOM(S):_____

REQUIREMENTS PER VA HANDBOOK 0730/4 APPENDIX B FOR THIS AREA INCLUDES:

A. Walls.

Exterior walls of brick and masonry construction are acceptable. Exterior walls which are composed of wood frame and siding require an interior backing of steel security screen mesh or sheet partition.

REQUIREMENT MET ☐ **DOES NOT MEET REQUIREMENT** ☐

B. Doors and Door Locks.

The locking requirements (including access controlled egress doors) outlined in National Fire Protection Association (NFPA) Life Safety Code standard, latest edition, 101-7.2.1.5 and 7.2.1.6 must be followed.

(1) Door Construction:

Doors are of 45 mm (1-3/4 in.) solid core hardwood or hollow steel construction. Dutch or half doors are unacceptable. Removable hinge pins on door exteriors must be retained with set pins or spot welded, preventing their removal. This applies only if the hinge pins are on the outside of the doors and door frames. Hinge pins will be on the outside if the door opens outward.

(2) Mechanical locking systems. Where mechanical lock systems are used, installed lock sets must allow for single motion egress. The installation of high security exit devices meeting NFPA Life Safety Code standards is appropriate**.**

(a) Glass doors or doors with glass panes must have one lock set that is key operated from the interior of the protected area.

Note: Fire code prohibits locks from being locked from the inside that require a key to exit. The intent is that there must be two locks, one of which must be key operated. The other lock can be key, combination or electronic. (NFPA 101, 7.2.1.5.2) locks, if provided, shall not require the use of a key, a tool or special knowledge or effort for the operations from the egress side.

(b) Steel doors will not be set into wooden frames.

(c) Doors set in steel frames must be fitted with a mortise lock with a deadlock feature. IAW ANSI/BHMA A156.13 American National Standards for Mortise Locks.

(d) The day lock on the main door must be automatically locking, with a minimum 19 mm (3/4 in.) dead bolt and inside thumb latch. Access to electronic locking systems, combinations or keys to day locks will be restricted to service employees and electronic access and/or combinations changed immediately on the termination or reassignment of an employee. See paragraph 8 of this appendix for a detailed description of key control systems.

(3) Electronic/Magnetic locking systems.
Where installed, electronic locking systems will include an automatic “request to exit” sensor and a “push to exit” manual lock release switch. Refer to the NFPA Life Safety Code for details.

REQUIREMENT MET ☐ **DOES NOT MEET REQUIREMENT** ☐

C. Other Room Access Means.
Interstitial overhead areas which enable entry into a secure room from an unsecured room must be barricaded by the installation of a suitable partition in the interstitial space which prevents "up and over" access. Openings in construction above ceilings or below raised access floors shall be protected as below requirement.
All vents, ducts, and similar openings more than 96 square inches (620 cm2) that enter or pass through space shall be protected with either bars or grills. If one dimension of the duct measures less than six inches (150 mm) or duct is less than 96 square inches (620 cm2), bars are not required; however, all ducts must be treated to provide sufficient sound attenuation. If bars are used, they must be 1/2-inch (12.7 mm) diameter steel welded vertically and horizontally six (6) inches (150 mm) on center; if grills are used, they must be of 9-gauge expanded steel.

REQUIREMENT MET ☐ **DOES NOT MEET REQUIREMENT** ☐

D. Motion Intrusion Detectors.
An intrusion detection alarm system which detects entry into the room and which broadcasts a local alarm of sufficient volume to cause an illegal entrant to abandon a burglary attempt. Intrusion detector equipment which operates on the principle of narrow beam interception, door contacts, microwave, or photoelectric eyes are unacceptable as the primary means of detection. Intrusion detectors must have the following essential features.

(1) An internal, automatic charging DC standby power supply and a primary AC power operations.

(2) A remote, key operated activation/deactivation switch installed outside the room and adjacent to the room entrance door frame and/or a central alarm ON-OFF control in the Police office or other monitoring location. For personal safety reasons, alarm switches and panels will be located outside of the protected space.

(3) An automatic reset capability following intrusion detection.

(4) A local alarm level of 80 dB (min) to 90 dB (max) within the configuration of the protected area.

(5) An integral capability for the attachment of wiring for remote alarm and intrusion indicator equipment (visual or audio).

(6) A low nuisance alarm rate as defined in VA Master Specifications, Division 28 - Electronic Safety and Security "28 16 11 INTRUSION DETECTION SYSTEM."

(7) Installation Notes

(a) A locally sounding alarm should not be installed in a room which is close to an ICU, cardiac care, or other special treatment areas where a loud alarm would have an injurious effect on patients.

(b) In addition to the locally sounding alarm, remote visual and/or audio annunciators must be at a location within the facility which ensures 24-hour monitoring. These annunciators will have the capability of identifying individually protected zones.

(c) In protected rooms of outpatient clinics not on facility grounds, intrusion detector alarms will be routed to a commercial security alarm monitoring firm, a local police department, or a security office charged with building security. The remote alarms
will be in addition to locally broadcast alarms in the protected areas.

(d) Remote bulk storage warehouse facilities will have one or more local broadcasting alarms inside and outside of the protected area.

(e) When replacing existing systems, or purchasing new, consideration will be given to intrusion detection equipment that integrates with CCTV and physical access control systems.

REQUIREMENT MET ☐ **DOES NOT MEET REQUIREMENT** ☐

E. Special Key Control.

Room door lock keys and day lock combinations, where applicable, are Special Keys as defined in paragraph 8.d. (10) of this appendix.

REQUIREMENT MET ☐ **DOES NOT MEET REQUIREMENT** ☐

F. Electronic Physical Access Control Systems (PACS).

For monitoring and controlling access to areas identified as requiring high or medium levels of assurance.

PACS systems are not used for recording employee time and attendance.

(1) For pharmacies and similar Services, PACS will be used to protect the perimeter of operations areas. In the case of pharmacies, this refers to spaces where
pharmaceuticals are mixed, packaged, assembled or otherwise prepared for distribution to patients. Administrative offices and similar spaces do not need to be protected with PACS, unless indicated by a local vulnerability assessment.

(a) Access Safeguard. To prevent learning codes through keypad observations or use of stolen or found access cards.

(b) Time Sensitive. The ability to program access by user, by shift and day.

(c) Area Sensitive. The ability to program access by door and area for each individual user.

(d) Fail-Safe. The ability to maintain access security if the system goes down (i.e. bypass key).

(e) Access Record/Audit Trail. The ability to provide for periodic or on demand print-out of names and time/dates of individual accessing. Records of access or audit trails will not be used for employee time and attendance purposes.

(f) User Coverage. The number of individual access codes that the system will accommodate.

(g) Personal Identifier Number (PIN) Codes. Access control systems protecting PACS high security areas, such as controlled substance storage, primary computer and communications

rooms, research or clinical laboratories that store, use or develop bio-hazardous materials, require a PIN number as a secondary personal authentication to be used in addition to card readers. “Scramble Pad” type PIN readers are recommended when PIN systems are installed. See the table below for specific VA identified required locations.

(h) Biometric Systems. Biometric security systems are those that use a personal measurement, such as fingerprints, hand geometry, facial geometry or iris scans, as authentication. Biometric devices can be used in lieu of PIN systems in PACS high protected spaces, but only as a secondary form of authentication. Biometric measurements may also be used in addition to a PIN in high security applications.

(i) Compliance with Federal Standards. New installations or retrofitted access control systems will be compliant with technology described in Federal Information Processing Standard (FIPS) Publication 201, Personal Identity Verification of Federal Employees and Contractors, and the document “PACS Implementation Guidance, Version 2.2 (July 30, 2004), published by the Physical Access Interagency Interoperability Working Group of the GSA Government Smart Card Interagency Advisory Board. This requires that such systems will meet the ISO/IEC 14443 a/b, Parts 1-4 standard for contactless (proximity) card systems, or the ISO/IEC 7816 Standard for contact-type cards. Facilities may continue to use existing PACS that operate on older technology (Magnetic Stripe, 2nd Generation bar code, etc.) as an interim measure until replacement systems are acquired and installed as part of normal equipment lifecycles. Further information on VA Smart Card operated PACS requirements can be found in the most recent edition of the document: “Physical Access Control Recommendations for the Department of Veterans Affairs.” Guidance and assistance with the standards can be obtained from the OS&LE.

(j) PACS Assurance Level Designations

PACS provide a level of assurance regarding the identity of persons entering a protected space. The levels of assurance required are determined because of vulnerability or risk assessments and physical security surveys. In addition, the following indicates minimum requirements for specified VA protected activities.

For purposes of this policy, levels of assurance are defined as:

- **High** - Entry requires a valid access card used in conjunction with a secondary form of authentication. Either a Personal Identification Number (PIN) known only to the card holder, or a biometric measurement, or both, is used as the secondary authenticator.
- **Medium** - Entry requires the use of a valid access card.
- **Low** - Entry requires the visual authentication of a valid access card or facility identification card. The card may be inspected by a police officer or other designated staff upon entry into the protected space, or may just require that it is worn always in a visible manner; see VA Directive 0730, paragraph 2.n. Facilities may choose to use a more stringent protection level for any of these locations.

In addition, facilities may choose to protect other activities with PACS. Further information on PACS Assurance level designations is found in VA Handbook 0730, Part E, Paragraph 1.g. (5).
The following are minimum protection and assurance levels for facilities that have installed PACS:

Location PACS Assurance Level

Warehouse Storage/Bulk= **Medium**

REQUIREMENT MET ☐ **DOES NOT MEET REQUIREMENT** ☐

OPTIONAL MEASURES PER VA HANDBOOK 0730/4 APPENDIX B FOR THIS AREA INCLUDES:

G. Windows.

When below 12 m (40 ft.) from ground level or the roof of a lower abutment, or less than 7.5 m (25 ft.) from windows of an adjoining building, or accessible by a building ledge leading to windows of other floor rooms, security mesh, screening for windows is required. Security measures that exceed these requirements may be authorized in writing by OS&LE. Required specifications for stainless steel security mesh screening are:

(1) All #304 stainless steel woven mesh 0.7 mm (.028 in.) wire diameter, with tensile strength of 15 kg/mm (800 pounds per linear inch).

(2) Mesh 12x12 per 25 mm (1 in.) with main and sub frames of 2.7 mm (12gauges) carbon steel with baked enamel finish and internal key locking slide bolts.

OPTIONAL MEASURE IN PLACE ☐

H. Secure Property Storage Containers.

For bulk retail merchandise, medical supplies and other items requiring off-shelf protection, steel storage cabinets with adjustable shelving are available through the Federal supply service, group 71, class 7125.

OPTIONAL MEASURE IN PLACE ☐

I. Robbery/Panic/Duress Alarms.

These types of alarm systems are used to provide rapid notification of police during an actual incident. The alarm may be activated by a covertly placed switch or button. Once activated, the switch or button can only be re-set by a key or other special tool that is in the possession of the VA police unit or other responder. The alarm annunciator will be monitored by police whenever the protected area is operational. The exact location of panic/duress alarm switches will be determined by a physical security survey of the protected area. Panic/Duress alarms must always be installed in the interior of pharmacy controlled substance or other Type I or Type II vaults.

OPTIONAL MEASURE IN PLACE ☐

NOTES/OBSERVATIONS: