SECTION 28 13 11
PHYSICAL ACCESS CONTROL SYSTEM (PACS)

PART 1 – GENERAL

1.1 DESCRIPTION

Provide and install a complete Physical Access Control System, hereinafter referred to as the PACS.

1.2 RELATED WORK

A. For firestopping application and use, Section 07 84 00, FIRESTOPPING.

B. For labeling and signs, Section 10 14 00, SIGNAGE.

C. For connection of high voltage, Section 26 05 11, REQUIREMENTS FOR ELECTRICAL INSTALLATIONS.

D. For power cables, Section 26 05 21, LOW-VOLTAGE ELECTRICAL POWER CONDUCTORS AND CABLES (600 VOLTS AND BELOW).

E. For grounding of equipment, Section 26 05 26, GROUNDING AND BONDING FOR ELECTRICAL SYSTEMS.

F. For infrastructure, Section 26 05 33, RACEWAYS AND BOXES FOR ELECTRICAL SYSTEMS.

G. For alarm systems, INTRUSION DETECTION SYSTEM (IDS).

H. For control and operation of all security systems, ACCESS CONTROL SYSTEM AND DATABASE MANAGEMENT.

I. For Warranty of Construction, see GENERAL CONDITIONS.

J. For General Requirements, Section 01 00 00, GENERAL REQUIREMENTS.

1.3 QUALITY CONTROL

A. The Contractor shall be responsible for providing, installing, and the operation of the PACS as shown. The Contractor shall also provide certification as required.

B. The security system will be installed and tested to ensure all components are fully compatible as a system and can be integrated with all associated security subsystems, whether the security system is stand-alone or a part of a complete Information Technology (IT) computer network.

C. The Contractor or security sub-contractor shall be a licensed security Contractor as required within the state or jurisdiction of where the installation work is being conducted.

1.4 SUBMITTALS

A. Submit below items in conjunction with Master Specification Sections 01 33 23, SHOP DRAWINGS, PRODUCT DATA, and SAMPLES, and Section 02 41 00, DEMOLITION.
B. Provide certificates of compliance with Section 1.3, Quality Assurance.
C. Provide a complete and thorough pre-installation and as-built shop drawing(s) package in both electronic format and on paper, minimum size 48 x 48 inches (1220 x 1220 millimeters); drawing submittals shall be per the established project schedule.
D. Pre-installation Shop Drawings and As-Built packages shall include, but not be limited to:
   1. Index Sheet that shall:
      a. Define each page of the design package to include facility name, building name, floor, and sheet number.
      b. Provide a complete list of all security abbreviations and symbols.
      c. Reference all general notes that are utilized within the design package.
      d. Specification and scope of work pages for all individual security systems that is applicable to the design package that will:
         1) Outline all general and job specific work required within the design package.
         2) Provide a detailed device identification table outlining device Identification (ID) and use for all security systems equipment utilized in the design package.
   2. Drawing sheets that will be plotted on the individual floor plans or site plans shall:
      a. Include a title block as defined above.
      b. Clearly define the drawings scale in both standard and metric measurements.
      c. Provide device identification and location.
      d. Address all signal and power conduit runs and sizes that are associated with the design of the electronic security system and other security elements (e.g., barriers, etc.).

e. Identify all pull box and conduit locations, sizes, and fill capacities.
f. Address all general and drawing specific notes for a particular drawing sheet.

3. A detailed riser drawing for each applicable security subsystem shall:
   a. Indicate the sequence of operation.
   b. Relationship of integrated components on one diagram.
   c. Include the number, size, identification, and maximum lengths of interconnecting wires.
   d. Wire/cable types shall be defined by a wire and cable schedule. The schedule shall utilize a lettering system that will correspond to the wire/cable it represents (example: A = 18 AWG/1 Pair Twisted, Unshielded). This schedule shall also provide the manufacturer’s name and part number for the wire/cable being installed.
4. A detailed system drawing for each applicable security system shall:
   a. Clearly identify how all equipment within the system, from main panel to device, shall be laid out and connected.
   b. Provide full detail of all system components wiring from point-to-point.
   c. Identify wire types utilized for connection, interconnection with associate security subsystems.
   d. Show device locations that correspond to the floor plans.
   e. All general and drawing specific notes shall be included with the system drawings.
5. A detailed schedule for all of the applicable security subsystems shall be included. All schedules shall provide the following information:
   a. Device ID.
   b. Device Location (e.g. site, building, floor, room number, location, and description).
   c. Mounting type (e.g. flush, wall, surface, etc.).
   d. Power supply or circuit breaker and power panel number.

e. In addition, for the PACS, provide the door ID, door type (e.g. wood or metal), locking mechanism (e.g. strike or electromagnetic lock) and control device (e.g. card reader or biometrics).

6. Detail and elevation drawings for all devices that define how they were installed and mounted.

E. Pre-installation Shop Drawing package shall be submitted to the Contracting Officer for review and approval. The Contractor shall not proceed with work, until this has been approved.

F. Provide manufacturer security system product cut-sheets. Submit for approval at least 30 days prior to commencement of formal testing, a Security System Operational Test Plan. Include procedures for operational testing of each component and security subsystem, to include performance of an integrated system test.

G. Submit manufacture’s certification of Underwriters Laboratories, Inc. (UL) listing as specified. Provide all maintenance and operating manuals per Section 01 00 00, GENERAL REQUIREMENTS.

1.5 APPLICABLE PUBLICATIONS

A. The publications listed below (including amendments, addenda, revisions, supplement, and errata) form a part of this specification to the extent referenced. The publications are referenced in the text by the basic designation only.

B. American National Standards Institute (ANSI)/ Security Industry Association (SIA):

AC-01.....Access Control: Wiegand Card Reader Interface Standard

AC-03.....Access Control: Badging Techniques

C. American National Standards Institute (ANSI)/ International Code Council (ICC):

A117.1.....Standard on Accessible and Usable Buildings and Facilities

D. Department of Justice American Disability Act (ADA)

28 CFR Part 36-90.....ADA Standards for Accessible Design

E. Government Accountability Office (GAO):

GAO-03-8-02.....Security Responsibilities for Federally Owned and Leased Facilities

F. National Electrical Contractors Association

303-2005.....Installing Closed Circuit Television (CCTV) Systems

G. National Electrical Manufactures Association (NEMA):

250-03.....Enclosures for Electrical Equipment (1000 Volts Maximum)

H. National Fire Protection Association (NFPA):

70-05..... Article 780-National Electrical Code

I. Underwriters Laboratories, Inc. (UL):

294-99.....Standard for Access Control

305-97.....Standard for Panic Hardware

639-97.....Standard for Intrusion-Detection Units

752-05.....Standard for Bullet-Resisting Equipment

827-96.....Central Station Alarm Services

1076-95.....Standards for Proprietary Burglar Alarm Units and Systems

1981-03.....Central Station Automation System

2058-05.....High Security Electronic Locks

J. Homeland Security Presidential Directive (HSPD):

HSPD-12.....Policy for a Common Identification Standard for Federal Employees and Contractors

K. Federal Information Processing Standards (FIPS):

FIPS-201.....Personal Identity Verification (PIV) of Federal Employees and Contractors

L. National Institute of Standards and Technology (NIST):

IR 6887 V2.1.....Government Smart Card Interoperability Specification (GSC-IS)

Special Pub 800-96.....PIV Card Reader Interoperability Guidelines

M. Institute of Electrical and Electronics Engineers (IEEE):

C62.41.....IEEE Recommended Practice on Surge Voltages in Low-Voltage AC Power Circuits

N. International Organization for Standardization (ISO):

7810.....Physical Characteristics of Credit Card Size Document

7811.....Physical Characteristics for Magnetic Stripe Cards

7816-1.....Physical Characteristics of the Card

7816-2.....Dimensions and Contact Position of the card
7816-3.....Electrical Signals and Transmission Protocols
7816-4.....Inter-Industry Command for Interchange
14443.....RFID cards; Contactless Proximity Cards Operating at 13.56 MHz in up to 5 inches distance
15693.....RFID cards; Contactless Vicinity Cards Operating at 13.56 MHz in up to 50 inches distance

O. Uniform Federal Accessibility Standards (UFAS) 1984
P. ADA Standards for Accessible Design 1994

1.6 WARRANTY OF CONSTRUCTION.

Warrant PACS work subject to the Article “Warranty of Construction” of FAR clause 52.246-21.

PART 2 – PRODUCTS

2.1 EQUIPMENT AND MATERIALS

A. All equipment associated within the PACS shall be UL 294 compliant and rated for continuous operation. Environmental conditions (i.e. temperature, humidity, wind, and seismic activity) shall be taken under consideration at each facility and site location prior to installation of the equipment.
B. All equipment shall operate on a 120 or 240 volts alternating current (VAC); 50 Hz or 60 Hz AC power system unless documented otherwise in subsequent sections listed within this specification. All equipment shall have a back-up source of power that will provide a minimum of 96 hours of run time in the event of a loss of primary power to the facility.
C. The system shall be designed, installed, and programmed in a manner that will allow for easy of operation, programming, servicing, maintenance, testing, and upgrading of the system.
D. All PACS components located in designated “HAZARDOUS ENVIRONMENT” areas where fire or explosion could occur due to the presence of natural gases or vapors, flammable liquids, combustible residue, or ignitable

fibers or debris, shall be rated Class II, Division I, Group F, and installed in accordance with NFPA 70, Chapter 5.

E. All equipment and materials for the system will be compatible to ensure correct operation as outlined in FIPS 201, March 2006 and HSPD-12.

2.2 EQUIPMENT ITEMS

A. The security system characteristics listed in this section will serve as a guide in selection of equipment and materials for the PACS. If updated or more suitable versions are available then the Contracting Officer will approve the acceptance of prior to an installation.

B. PACS equipment shall meet or exceed all requirements listed below.

C. A PACS shall be comprised of, but not limited to, the following components:

1. Control/Communications Panels
2. Electronic Security Management System
3. Card Reader and Credential Cards
4. Portal Control Devices
5. Door Status Indicators
6. Entry Control Device
7. Power Supplies
8. Wires and Cables

D. Control/Communication Panels:

1. Shall be a central point provided for monitoring, controlling, and programming the PACS.
2. Shall provide a means of controlling up to 16 doors per panel.
3. Shall be expandable and provide a means of networking multiple panels to provide overall control of all doors on the PACS via a primary panel.
4. Shall be system specific addressable, Internet Protocol (IP) addressable, and programmable via a computer.
5. Shall be able to be interfaced directly from a computer or via the Internet or Intranet. Access to the panels shall be password protected. All individuals with access to the panels shall have a user specific password.
6. Shall be of the same manufacturer and part number to ensure full compatibility within the system.

7. The operating system for the panel must utilize a single seamlessly integrated relational database for all functionality. This integration shall be provided with one operating environment. The operating environment shall be the fully multi-tasking multi-threading Microsoft Windows XP, Windows 7, Windows Server 2005/2008R2 Operating Systems, and shall be fully compatible with VA Long Beach security system.
8. The panel's web enabled client applications shall be capable of running on independent client operating systems including Windows XP and Windows 7. The web-enabled applications shall utilize the same common database as the other system modules. The applications shall be fully compatible with VA Long Beach security system.
9. The panel programming shall be written so that all system modules (e.g. access control, alarm monitoring, credential management, digital video, visitor management, intrusion detection, asset management, etc.) are developed and built from a unified 32-bit source code set. There absolutely shall not be separate source code bases for the individual modules of the PACS.
10. Shall allow for the operation and control of up to 16 doors.
11. Shall consist of or have the equivalent of, at a minimum, a General Control Module and an Access Control Module. Both modules shall be programmable via a computer.
12. The General Control Module shall:
    a. Provide for full distributed processing of access control and alarm monitoring operations.
    b. Store the following information and function using a high speed, local 32-bit microprocessor:
        1) access levels
        2) hardware configurations
        3) programmed alarm outputs assigned at a administration client workstation
    c. Process all access granted/denied decisions to provide fast responses to card reader transactions. A fully configured general control module with 64 card readers shall require less than one-half (0.5) seconds to grant access to an authorized cardholder or deny access to an unauthorized cardholder.

d. Meet the following minimum requirements:
   1) A minimum host communications speed of 115,200 bps.
   2) Support direct connect connections.
   3) Have remote dial up.
   4) Minimum on-board memory of eight (8) MB.
   5) Local Area Network (LAN) Support RJ45 (10/100baseT) Ethernet Interface Token Ring four (4) MB connectivity.
   6) Minimum memory storage of up to 5,000 cardholders and 100,000 events.
   7) Downstream ports for connecting card readers and data gathering panels via RS-485 multi-drop wiring configuration.
   8) Support of multiple card technologies.
   9) Supervised Communications with PACS system software.
   10) Support of up to eight card formats and facility codes.
   11) RS-485 Full Duplex, UL 1076 Grade AA communication channel to the system head-end.
   12) Integration with all manufacturers’ card readers.
   13) 12 VAC or 12 volts direct current (VDC) input power via a UL certified step-down transformer or power supply.
   14) Issue Code Support for Wiegand, HID and PIV-II Card Formats.
   15) Individual Shunt Times
   16) Up to Nine Digit PIN Codes.
   17) Downstream serial RS-232 device support.
   18) Status LED’s to identify normal component and communication status.

13. The access control module shall:
   a. Control up to 16 doors utilizing input and output relays that are fully programmable via network software.
   b. Input relays shall meet the following minimum requirements:
      1) Provide up to 16 UL 1076 analog unsupervised alarm input zones to monitor and report alarm conditions, power faults, and tampers.
      2) Operate independently and in conjunction with output relays, which will send an output signal to a corresponding output device upon alarm input activation. Once an alarm has been

received, the input relay shall activate any or all alarm outputs.

3) Contain the following features:
   a) UL 294 Certified.
   b) Alarm contact status scanning at up to 120 times per second for each zone.
   c) A low power Complementary-symmetry/metal-oxide semiconductor (CMOS) microprocessor.
   d) Filtered data for noise rejection to prevent false alarms.
   e) Up to 16 supervised inputs.
   f) 12 VAC or 12 VDC Input Power.
   g) Two (2) dedicated inputs for tamper and power status.

14. Output relays shall meet the following minimum requirements:
    a. Shall be capable of controlling a corresponding output device upon any input activation or on command from the PACS.
    b. Shall be capable of responding to:
       1) Input alarms.
       2) Commands from a System Operator.
       3) Time zone control commands for automatic operation.
    c. Shall be capable of:
       1) Pulsing for a predetermined duration. Duration shall be programmable for each relay individually.
       2) Responding on command from the System Operator to pulse, command on, command off, or reset to normal state.
       3) Operating outputs rated at 5 amps (A) @ 30 VDC.

E. Electronic Security Management System (SMS):
   1. Shall allow the configuration of an enrollment and badging, alarm monitoring, administrative, asset management, digital video management, intrusion detection, visitor enrollment, remote access level management, and integrated client workstations or any combination of all or some.
   2. Shall be expandable to support an unlimited number of individual module or integrated client workstations. All access control field hardware, including Intelligent System Controllers (ISC), shall be connected to all Windows 2003/2000/XP based access control system workstation on the network.

3. Shall have the ability to compose, file, maintain, update, and print reports for either individuals or the system as follows.
   a. Individual reports that consist of an employees name, office location, phone number or direct extension, and normal hours of operation. The report shall provide a detail listing of the employee’s daily events in relation to accessing points within a facility.
   b. System reports shall be able to produce information on a daily/weekly/monthly basis for all events, alarms, and any other activity associated with a system user.
   c. All reports shall be in a date/time format and all information shall be clearly presented.
4. Shall be designed to allow it to work with any industry standard network protocol and topology listed below:
   a. Transmission Control Protocol (TCP)/IP
   b. Novell Netware (IPX/SPX)
   c. Banyan VINES
   d. IBM LAN Server (NetBEUI)
   e. Microsoft LAN Manager (NetBEUI)
   f. Network File System (NFS) Networks
5. Shall provide full interface and control of the PACS to include the following subsystems within the PACS:
   a. Public Key Infrastructure
   b. Card Management
   c. Identity and Access Management
   d. Personal Identity Verification
6. Shall have the following features or compatibilities:
   a. The ability to be operated locally or remotely via a LAN, WAN, internet, or intranet.
   b. Event and Alarm Monitoring
   c. Database Partitioning
   d. Ability to fully integrate with all other security subsystems
   e. Enhanced Monitoring Station with Split Screen Views
   f. Alternate and Extended Shunt by Door
   g. Escort Management
   h. Enhanced IT-based Password Protection

i. N-man Rule and Occupancy Restrictions
j. Open Journal Data Format for Enhanced Reporting
k. Automated Personnel Import
l. ODBC Support
m. Windows 2000 Professional, Windows Server 2003, Windows XP Professionals for Servers
n. Field-Level Audit Trail
o. Cardholder Access Events

7. For the SMS network a server and client workstation shall be required and must meet the following minimum technical characteristics:

a. Server:

Processor	3.4 GHz Intel
Free Hard Disk Space	Min 500.0 GB
Memory	Min 12.0 GB
Network Card	10/100/1000 Base-T
CD-ROM Drive	10X
Monitor/Video Adapter board	17” SVGA (1024 x 768)
Operating System	Windows Server 2005, Windows Server 2008R2 with Microsoft SQL Server
Ports	2 serial, 1 parallel, USB
Backup	Tape or CDRW
Modem	56.7 Kbps

b. Client Workstation:

Processor	3.4 GHz Intel
Free Hard Disk Space	Min 250 GB
Memory	12 GB RAM
Network Card	10100/1000 Base-T
CD-ROM Drive	10X
Monitor/Video Adapter board	17” SVGA (1024 x 768), 64 MB RAM
Operating Systems	Windows XP Professional or Windows 7

F. Card Readers and Credential Cards:

1. Shall be utilized for controlling the locking hardware on a door and allows for reporting back to the main control panel with the time/date the door was accessed, the name of the person accessing the point of entry, and its location.
2. Will be fully programmable and addressable, locally and remotely, and hardwired to the system.
3. Shall be individually home run to the main panel.
4. Shall be installed in a manner that they comply with:
   a. The Uniform Federal Accessibility Standards (UFAS)
   b. The Americans with Disabilities Act (ADA)
   c. The ADA Standards for Accessible Design
5. Shall support a variety of card readers that must encompass a wide functional range. The PACS may combine any of the card readers described below for installations requiring multiple types of card reader capability (i.e., card only, card and/or PIN, card and/or biometrics, card and/or pin and/or biometrics, supervised inputs, etc.). These card readers shall be available in the approved technology to meet FIPS 201 and is ISO 14443 A or B compliant. The reader output can be Wiegand, RS-22, 485 or TCP/IP.
6. Are to be housed in an aluminum bezel with a wide lead-in for easy card entry.
7. Shall contain read head electronics, and a sender to encode digital door control signals.
8. LED’s shall be utilized to indicate card reader status and access status.
9. Shall be able to support a user defined downloadable off-line mode of operation (e.g. locked, unlocked, or facility code), which will go in effect during loss of communication with the main control panel.
10. Shall provide audible feedback to indicate access granted/denied decisions. Upon a card swipe, two audible tones or beeps shall indicate access granted and three tones or beeps shall indicate access denied. All keypad buttons shall provide (tactile?? What does this mean) audible feedback.
11. Shall have a minimum of two programmable inputs and two programmable outputs.

12. All card readers that utilize keypad controls along with a reader and shall meet the following specifications:
    a. Entry control keypads shall use a unique combination of alphanumeric and other symbols as an identifier. Keypads shall contain an integral alphanumeric/special symbols keyboard with symbols arranged in ascending ASCII code ordinal sequence. Communications protocol shall be compatible with the local processor.
    b. Shall include a Light Emitting Diode (LED) or other type of visual indicator display and provide visual or visual and audible status indications and user prompts. The display shall indicate power on/off, and whether user passage requests have been accepted or rejected. The design of the keypad display or keypad enclosure shall limit the maximum horizontal and vertical viewing angles of the keypad. The maximum horizontal viewing angle shall be plus and minus five (5) degrees or less off a vertical plane perpendicular to the plane of the face of the keypad display. The maximum vertical viewing angle shall be plus and minus 15 degrees or less off a horizontal plane perpendicular to the plane of the face of the keypad display.
    c. Shall respond to passage requests by generating a signal to the local processor. The response time shall be 800 milliseconds or less from the time the last alphanumeric symbol is entered until a response signal is generated.
    d. Shall be powered from the source as designed and shall not dissipate more than 150 Watts.
    e. Shall be suitable for surface, semi-flush, pedestal, or weatherproof mounting as required.
    f. Shall provide a means for users to indicate a duress situation by entering a special code.
13. Card readers shall come in the following formats:

    c. Wiegand Card Reader:
        1) Shall be utilized during the transition from the existing technology to the contactless smart card technology as defined in FIPS-201.

2) Shall read credential cards which are encoded using Wiegand effect ferromagnetic wires laminated into the credential card.
3) Shall create a magnetic field and output a coded representation of the unique pattern of magnetic flux changes produced by moving the credential card through the card reader.
4 The output shall be a series of electrical signals and shall constitute a unique identification code number.
5) Wiegand credential cards shall use at least 24 binary digits to generate a unique credential card identification code.
6) The card reader shall meet or exceed the following technical characteristics:

Card Speed	5 to 30 inches (203 to 1270mm) per second
Data Rate	1ms per bit
Connections	RJ-45 Jack or multi- conductor quick disconnect
Output Formats	26 or 34-bit
Power	Per Manufacturers Specifications
Lifetime	600,000 pass read head
Error Rate	false accept
Static Discharge	Withstands 20,000 volts
LED	If required per the design package
Card Output Format	EMPI 26 or 34-bit ANSI/ABA All bits Clock-and-Data up to 37 characters 10 Digit ANSI/ABA 26 or 34-bit

c. Contactless Smart Cards and Readers:
1) Smart card readers shall read credential cards whose characteristics of size and technology meet those defined by ISO/IEC 7816, 14443, 15693.
2) The readers shall have "flash" download capability to accommodate card format changes.
3) The card reader shall have the capability of reading the card data and transmitting the data to the main monitoring panel.

4) The card reader shall be contactless and meet or exceed the following technical characteristics:
   a) Data Output Formats: FIPS 201 low outputs the FASC-N in an assortment of Wiegand bit formats from 40 – 200 bits. FIPS 201 medium outputs a combination FASC-N and HMAC in an assortment of Wiegand bit formats from 32 – 232 bits. All Wiegand formats or the upgradeability from Low to Medium Levels can be field configured with the use of a command card.
   b) FIPS 201 readers shall be able to read, but not be limited to, DESfire and iCLASS cards.

   Reader range shall comply with ISO standards 7816, 14443, and 15693, and also take into consideration conditions, are at a minimum 1″ to 2″ (2.5 – 5 cm).

d. Proximity (PROX) Card Reader:
   1) Shall be utilized during the transition from the existing technology to the contactless smart card technology as defined in FIPS-201.
   2) Shall use active/passive proximity detection and shall not require contact with the proximity credential card for operation.
      a) Active detection proximity card readers shall provide power to compatible credential cards through magnetic induction and receive and decode a unique identification code number transmitted from the credential card.
      b) Passive detection proximity card readers shall use a swept-frequency, radio frequency field generator to read the resonant frequencies of tuned circuits laminated into compatible credential cards. The resonant frequencies read shall constitute a unique identification code number.
   3) Shall read proximity cards in a range from 0 to at least six (6) inches (0 to at least 15 cm) from the reader. The credential card design shall allow for a minimum of 32,000 unique identification codes per facility.
   4) Shall be able to read cards from two (2) inches (5cm) to 6 inches (15cm).

5) For exterior parking lots or garages shall be 16 inches (40 cm).
6) The operating frequency shall be determined by the type of access control system being utilized.

e. Credential Cards: Shall be in accordance with FIPS 201 and controlled by the PIV enrollment and issuance system.

I. Portal Control Devices:
1. Shall be used to assist the PACS.
2. Such devices shall:
   a. Provide a means of monitoring the doors status.
   b. Allow for exiting a space via either a push button, request to exit, or panic/crash bar.
   c. Provide a means of override to the PACS via a keypad or key bypass.
   d. Assist door operations utilizing automatic openers and closures.
   e. Provide a secondary means of access to a space via a keypad.
3. Shall be connected to and monitored by the main PACS panel.
4. Shall be installed in a manner that they comply with:
   a. The Uniform Federal Accessibility Standards (UFAS)
   b. The Americans with Disabilities Act (ADA)
   c. The ADA Standards for Accessible Design
5. Shall provide a secondary means of access control within a secure area.
6. Keypads: Refer to Section 2.2.F.12 for keypad requirements.
7. Push-Button Switches:
   a. Shall be momentary contact, back lighted push buttons, and stainless steel switch enclosures for each push button as shown. Buttons are to be utilized for secondary means of releasing a locking mechanism.
   b. In an area where a push button is being utilized for remote access of the locking device then no more than two (2) buttons shall operate one door from within one secure space. Buttons will not be wired in series with one other.
   C. In an area where locally stationed guards control entry to multiple secure points via remote switches. An interface board shall be designed and constructed for only the amount of buttons

it shall house. These buttons shall be flush mounted and clearly labeled for ease of use. All buttons shall be connected to the PACS and SMS system for monitoring purposes.

d. Shall have double-break silver contacts that will make 720 VA at 60 amperes and break 720 VA at 10 amperes.

8. Crash Bar:

a. Emergency Exit with Alarm (Panic):

1. Entry control portals shall include panic bar emergency exit hardware as designed.
2. Panic bar emergency exit hardware shall provide an alarm shunt signal to the PACS and SMS.
3. The panic bar shall include a conspicuous warning sign with one (1) inch (2.5 cm) high, red lettering notifying personnel that an alarm will be annunciated if the panic bar is operated.
4. Operation of the panic bar hardware shall generate an intrusion alarm that reports to both the SMS and Intrusion Detection System. The use of a micro switch installed within the panic bar shall be utilized for this.
5. The panic bar shall a fully mechanical connection only and shall not depend upon electric power for operation.
6. The panic bar shall be compatible with mortise or rim mount door hardware and shall operate by retracting the bolt manually by either pressing the panic bar or with a key by-pass. Refer to Section 2.2.I.9 for key-bypass specifications.

b. Normal Exit:

1) Entry control portals shall include panic bar non-emergency exit hardware as designed.
2) Panic bar non-emergency exit hardware shall be monitored by and report to the SMS.
3) Operation of the panic bar hardware shall not generate a locally audible or an intrusion alarm within the IDS.
4) When exiting, the panic bar shall depend upon a mechanical connection only. The exterior, non-secure side of the door shall be provided with an electrified thumb latch or lever to

provide access after the credential I.D. authentication by the SMS.

5) The panic bar shall be compatible with mortise or rim mount door hardware and shall operate by retracting the bolt manually by either pressing the panic bar or with a key by-pass. Refer to Section 2.2.I.9 for key-bypass specifications. The strikes/bolts shall include a micro switch to indicate to the system when the bolt is not engaged or the strike mechanism is unlocked. The signal switches shall report a forced entry to the system in the event the door is left open or accessed without the identification credentials.

9. Key Bypass:
   a. Shall be utilized for all doors that have a mortise or rim mounted door hardware.
   b. Each door shall be individually keyed with one master key per secured area.
   c. Cylinders shall be six (6)-pin and made of brass or equivalent. Keys for the cylinders shall be constructed of solid material and produced and cut by the same distributor. Keys shall not be purchased, cut, and supplied by multiple dealers.
   d. All keys shall have a serial number cut into the key. No two serial numbers shall be the same.
   e. All keys and cylinders shall be stored in a secure area that is monitored by the Intrusion Detection System.
10. Automatic Door Opener and Closer:
   a. Shall be low energy operators.
   b. Door closing force shall be adjustable to ensure adequate closing control.
   c. Shall have an adjustable back-check feature to cushion the door opening speed if opened violently.
   d. Motor assist shall be adjustable from 0 to 30 seconds in five (5) second increments. Motor assist shall restart the time cycle with each new activation of the initiating device.
   e. Unit shall have a three-position selector mode switch that shall permit unit to be switched “ON” to monitor for function activation, switched to “H/O” for indefinite hold open function

or switched to “OFF,” which shall deactivate all control functions but will allow standard door operation by means of the internal mechanical closer.

f. Door control shall be adjustable to provide compliance with the requirements of the Americans with Disabilities Act (ADA) and ANSI standards A117.1.

g. All automatic door openers and closers shall:

1) Meet UL standards.
2) Be fire rated.
3) Have push and go function to activate power operator or power assist function.
4) Have push button controls for setting door close and door open positions.
5) Have open obstruction detection and close obstruction detection built into the unit.
6) Have door closer assembly with adjustable spring size, back-check valve, sweep valve, latch valve, speed control valve and pressure adjustment valve to control door closing.
7) Have motor start-up delay, vestibule interface delay; electric lock delay and door hold open delay up to 30 seconds. All operators shall close door under full spring power when power is removed.
8) Are to be hard wired with power input of 120 VAC, 60Hz and connected to a dedicated circuit breaker located on a power panel reserved for security equipment.

11. Request-to-Exit (RTE):

a. Shall be utilized to de-energize the locking hardware on a door to allow for exiting a secure area.

b. Shall be either an infrared sensor or a push button.

c. Infrared sensors shall meet the following minimum technical characteristics:

Alarm Output	2 Form "C" relay contacts
Indicators	1 activation LED
Power Requirements	12 or 24 VAC, 12 or 24 VDC, 26 mA @ 12 VDC
Relay Latch	Time Adjustable to 60 seconds

J. Door Status Indicators:
   1. Shall monitor and report door status to the SMS.
   2. Door Position Sensor:
      a. Shall provide an open or closed indication for all doors operated on the PACS and report directly to the SMS.
      b. Shall also provide alarm input to the Intrusion Detection System for all doors operated by the PACS and all other doors that require monitoring by the intrusion detection system.
      c. Switches for doors operated by the PACS shall be double pole double throw (DPDT). One side of the switch shall monitor door position and the other side if the switch shall report to the intrusion detection system. For doors with electromagnetic locks a magnetic bonding sensor (MBS) can be used in place of one side of a DPDT switch, in turn allowing for the use of a single pole double throw (SPDT) switch in it place of a DPDT switch.
      d. Switches for doors not operated by the PACS shall be SPDT and report directly to the IDS.
      e. Shall be surface or flush mounted and wide gap with the ability to operate at a maximum distance of up to 2″ (5 cm).

K. Entry Control Devices:
   1. Shall be hardwired to the PACS main control panel and operated by either a card reader or a biometric device via a relay on the main control panel.
   2. Shall be fail-safe in the event of power failure to the PACS system.
   3. Shall operate at 24 VCD, with the exception of turnstiles and be powered by a separate power supply dedicated to the door control system. Each power supply shall be rated to operate a minimum of two doors simultaneously without error to the system or overload the power supply unit.
   4. Shall have a diode or metal-oxide veristor (MOV) to protect the controller and power supply from reverse current surges or back-check.
   5. Electric Strikes/Bolts: Shall be:
      a. Made of heavy-duty construction and tamper resistant design.
      b. Tested to over one million cycles.

c. Rated for a minimum of 1000 lbs. holding strength.
d. Utilize an actuating solenoid for the strike/bolt. The solenoid shall move from fully open to fully closed position and back in not more than 500 milliseconds and be rated for continuous duty.
e. Utilize a signal switch that will indicate to the system if the strike/bolt is not engaged or is unlocked when it should be secured.
f. Flush mounted within the door frame.

6. Electric Mortise Locks: Shall be installed within the door and an electric transfer hinge shall be utilized to allow the wires to be transferred from the door frame to the lock. If utilized with a double door then the lock shall be installed inside the active leaf.
7. Electromagnetic Locks:
   a. These locks shall be without mechanical linkage utilizing no moving parts, and securing the door to its frame solely on electromagnetic force.
   b. Shall be comprised of two pieces, the mag-lock and the door plate. The mag-lock shall be surface mounted to the door frame and the door plate shall be surface mounted to the door.
   c. Ensure a diode or MOV is installed in line with the DC voltage supplying power to the unit in order to prevent back-check on the system when the mag-lock is powered.
   d. Shall utilize a magnetic bonding sensor (MBS) to monitor the door status and report that status to the SMS.
   e. Electromagnetic locks shall meet the following minimum technical characteristics:

Operating Voltage		24 VDC
Current Draw		.5A
Holding Force	Swing Doors	1500 lbs (675 Kg)
	Sliding Doors	500 lbs (225 Kg)

L. Power Supplies:
1. Shall be UL rated and able to adequately power two entry control devices on a continuous base without failure.
2. Shall meet the following minimum technical characteristics:

INPUT POWER	110 VAC 60 HZ 2 amp
OUTPUT VOLTAGE	12 VDC Nominal (13.8 VDC) 24 VDC Nominal (27.6 VDC) Filtered and Regulated
BATTERY	Dependant on Output Voltage shall provide up to 14 Ah
OUTPUT CURRENT	10 amp max. @ 13.8 VDC 5 amp max. @ 27.6 VDC
PRIMARY FUSE SIZE	6.3 amp (non-removable)
BATTERY FUSE SIZE	12 amp, 3AG
CHARGING CIRCUIT	Built-in standard

M. Wires and Cables

1. Shall meet or exceed the manufactures recommendations for power and signal.
2. Shall be carried in an enclosed conduit system, utilizing electromagnetic tubing (EMT) to include the equivalent in flexible metal, rigid galvanized steel (RGS) to include the equivalent of liquid tight, polyvinylchloride (PVC) schedule 40 or 80.
3. All conduits will be sized and installed per the NEC. All security system signal and power cables that traverse or originate in a high security office space will contained in either EMT or RGS conduit.
4. All conduit, pull boxes, and junction boxes shall be clearly marked every with colored permanent tape or paint that will allow it to be distinguished from all other conduit and infrastructure.
5. Conduit fills shall not exceed 50 percent unless otherwise documented.
6. A pull rope shall be pulled along with signal and power cables to assist in future work.
7. At all locations where core drilling is conducted to allow for conduit to be installed, then fire stopping shall be applied to that area.
8. High power and signal cables shall not share the same conduit and shall be kept separate up to the point of connection. High power for

the security system shall be defined as any cable or sets of cables carrying 30 VDC/VAC or higher.

9. Signal Cables:
   a. Shall meet or exceed all specifications and requirements called out by the manufactures.
   b. Shall be twisted pairs.
   c. All cables and conductors, except fiber optic cables, that act as a control, communication, or signal lines shall include surge protection. Surge protection shall be furnished at the equipment end and additional triple electrode gas surge protectors rated for the application on each wire line circuit shall be installed within 3 feet, (1 meter) of the building cable entrance. The inputs and outputs shall be tested in both normal and common mode using the following wave forms:
      1) A 10 microsecond rise time by 1000 microsecond pulse width waveform with a peak voltage of 1500 volts and peak current of 60 amperes.
      2) An 8 microsecond rise time by 20 microsecond pulse width wave form with a peak voltage of 1000 volts and peak current of 500 amperes.
10. Power Cables:
   a. Shall be rated for either 110 or 220 VAC, 50 or 60 Hz, and shall comply with VA Master Spec 26 05 21 Low Voltage Electrical Power Conductors and Cables (600 Volts and Below).
   b. Shall be sized according and comply with the NEC. High voltage power cables will be a minimum of three conductors, 14 AWG, stranded, and coated with a non-conductive polyvinylchloride (PVC) jacket.
   c. Low Voltage Power Cables:
      1) All cables shall be a minimum of 18 AWG, Stranded and have a polyvinylchloride outer jacket.
      2) Specific cable size shall determined using a basic voltage over distance calculation and shall comply with the NEC’s requirements for low voltage cables.
   d. All equipment connected to AC power shall be protected from surges. Equipment protection shall withstand surge test waveforms

described in IEEE C62.41. Fuses shall not be used as a means of surge protection.

2.3 INSTALLATION KIT

A. General: The kit shall be provided that at, a minimum includes all connectors and terminals, labeling systems, audio spade lugs, barrier strips, punch blocks or wire wrap terminals, heat shrink tubing, cable ties, solder, hangers, clamps, bolts, conduit, cable duct, and/or cable tray, etc., required to accomplish a neat and secure installation. All wires shall terminate in a spade lug and barrier strip, wire wrap terminal or punch block. Unfinished or unlabeled wire connections shall not be allowed. All unused and partially opened installation kit boxes, coaxial, fiber-optic, and twisted pair cable reels, conduit, cable tray, and/or cable duct bundles, wire rolls, physical installation hardware shall be turned over to the Contracting Officer. The following sections outlined are the minimum required installation sub-kits:

1. System Grounding:
   a. The grounding kit shall include all cable and installation hardware required. All head end equipment and power supplies shall be connected to earth ground via internal building wiring, according to the NEC.
   b. This includes, but is not limited to:
      1) Coaxial Cable Shields
      2) Control Cable Shields
      3) Data Cable Shields
      4) Equipment Racks
      5) Equipment Cabinets
      6) Conduits
      7) Cable Duct blocks
      8) Cable Trays
      9) Power Panels
      10) Grounding
      11) Connector Panels
2. Coaxial Cable: The coaxial cable kit shall include all coaxial connectors, cable tying straps, heat shrink tabbing, hangers, clamps, etc., required to accomplish a neat and secure installation.

3. Wire and Cable: The wire and cable kit shall include all connectors and terminals, audio spade lugs, barrier straps, punch blocks, wire wrap strips, heat shrink tubing, tie wraps, solder, hangers, clamps, labels etc., required to accomplish a neat and orderly installation.
4. Conduit, Cable Duct, and Cable Tray: The kit shall include all conduit, duct, trays, junction boxes, back boxes, cover plates, feed through nipples, hangers, clamps, other hardware required to accomplish a neat and secure conduit, cable duct, and/or cable tray installation in accordance with the NEC and this document.
5. Equipment Interface: The equipment kit shall include any item or quantity of equipment, cable, mounting hardware and materials needed to interface the systems with the identified sub-system(s) according to the OEM requirements and this document.
6. Labels: The labeling kit shall include any item or quantity of labels, tools, stencils, and materials needed to label each subsystem according to the OEM requirements, as-installed drawings, and this document.
7. Documentation: The documentation kit shall include any item or quantity of items, computer discs, as installed drawings, equipment, maintenance, and operation manuals, and OEM materials needed to provide the system documentation as required by this document and explained herein.

PART 3

3.1 INSTALLATION

A. System installation shall be in accordance with UL 294, manufacturer and related documents and references, for each type of security subsystem designed, engineered and installed.
B. Components shall be configured with appropriate “service points” to pinpoint system trouble in less than 30 minutes.
C. The Contractor shall install all system components including Government furnished equipment, and appurtenances in accordance with the manufacturer's instructions, documentation listed in Sections 1.4 and 1.5 of this document, and shall furnish all necessary connectors, terminators, interconnections, services, and adjustments required for a operable system.

D. The PACS will be designed, engineered, installed, and tested to ensure all components are fully compatible as a system and can be integrated with all associated security subsystems, whether the system is a stand alone or a network.

E. For integration purposes, the PACS shall be integrated where appropriate with the following associated security subsystems:

1. CCTV:
   a. Provide 24 hour coverage of all entry points to the perimeter and agency buildings. As well as all emergency exits utilizing a fixed color camera.
   b. Be able to monitor, control and record cameras on a 24 hours basis.
   c. Be programmed automatically call up a camera when an access point is but into an alarm state.
   d. For additional PACS system requirements as they relate to the CCTV, refer to Section 28 23 00, VIDEO SURVEILLANCE.
2. IDS:
   a. Be able monitor door control sensors.
   b. Be able to monitor and control the IDS on a 24 hours basis.
   c. Be programmed to go into an alarm state when an IDS device is put into an alarm state, and notify the operator via an audible alarm.
   d. For additional PACS system requirements as they relate to the IDS, refer to Section 28 16 11, INTRUSION DETECTION SYSTEM.
3. Security Access Detection:
   a. Be able to monitor all objects that have been screened with an x-ray machine and be able to monitor all data acquired by the bomb detection unit.
   b. For additional PACS system requirements as they relate to the Security Access Detection, refer to Section 28 13 53, SECURITY ACCESS DETECTION.
4. EPPS:
   a. Be programmed to go into an alarm state when an emergency call box or duress alarm/panic device is activated, and notify the Access Control System and Database Management of an alarm event.

b. For additional PACS requirements as they relate to the EPPS, refer to Section 28 26 00, ELECTRONIC PERSONAL PROTECTION SYSTEM.

E. Integration with these security subsystems shall be achieved by computer programming or the direct hardwiring of the systems.

F. For programming purposes refer to the manufacturers requirements for correct system operations. Ensure computers being utilized for system integration meet or exceed the minimum system requirements outlined on the systems software packages.

G. The Contractor shall visit the site and verify that site conditions are in agreement/compliance with the Pre-installation Shop Drawing package. The Contractor shall report all changes to the site or conditions that will affect performance of the system to the Contracting Officer in the form of a report. The Contractor shall not take any corrective action without written permission received from the Contracting Officer.

I. Existing Equipment:

1. The Contractor shall connect to and utilize existing door equipment, control signal transmission lines, and devices as outlined in the approved Pre-Installation Shop Drawing package. Door equipment and signal lines that are usable in their original configuration without modification may be reused with Contracting Officer approval.
2. The Contractor shall perform a field survey, including testing and inspection of all existing door equipment and signal lines intended to be incorporated into the PACS, and furnish a report to the Contracting Officer as part of the site survey report. For those items considered nonfunctioning, provide (with the report) specification sheets, or written functional requirements to support the findings and the estimated cost to correct the deficiency. As part of the report, the Contractor shall include a schedule for connection to all existing equipment.
3. The Contractor shall make written requests and obtain approval prior to disconnecting any signal lines and equipment, and creating equipment downtime. Such work shall proceed only after receiving Contracting Officer approval of these requests. If any device fails after the Contractor has commenced work on that device, signal or control line, the Contractor shall diagnose the failure and perform any necessary corrections to the equipment.

4. The Contractor shall be held responsible for repair costs due to Contractor negligence, abuse, or improper installation of equipment.
5. The Contracting Officer shall be provided a full list of all equipment that is to be removed or replaced by the Contractor, to include description and serial/manufacturer numbers where possible. The Contractor shall dispose of all equipment that has been removed or replaced based upon approval of the Contracting Officer after reviewing the equipment removal list. In all areas where equipment is removed or replaced the Contractor shall repair those areas to match the current existing conditions.

J. Enclosure Penetrations: All enclosure penetrations shall be from the bottom of the enclosure unless the system design requires penetrations from other directions. Penetrations of interior enclosures involving transitions of conduit from interior to exterior, and all penetrations on exterior enclosures shall be sealed with rubber silicone sealant to preclude the entry of water and will comply with VA Master Specification 07 84 00, Firestopping. The conduit riser shall terminate in a hot-dipped galvanized metal cable terminator. The terminator shall be filled with an approved sealant as recommended by the cable manufacturer and in such a manner that the cable is not damaged.

K. Cold Galvanizing: All field welds and brazing on factory galvanized boxes, enclosures, and conduits shall be coated with a cold galvanized paint containing at least 95 percent zinc by weight.

L. Control Panels:
1. Connect power and signal lines to the controller.
2. Program the panel as outlined by the design and per the manufacturer’s programming guidelines.

M. SMS:
1. Coordinate with the VA agency’s IT personnel to place the computer on the local LAN or Intranet and provide the security system protection levels required to insure only authorized VA personnel have access to the system.
2. Program and set-up the SMS to ensure it is in fully operation.

N. Card Readers:
1. Connect all signal inputs and outputs as shown and specified.
2. Terminate input signals as required.

3. Program and address the reader as per the design package.
4. Readers shall be surface or flushed mounted and all appropriate hardware shall be provided to ensure the unit is installed in an enclosed conduit system.

O. Portal Control Devices:
1. Install all signal input and output cables as well as all power cables.
2. Devices shall be surface or flush mounted as per the design package.
3. Program all devices and ensure they are working.

P. Door Status Indicators:
1. Install all signal input and output cables as well as all power cables.
2. RTE’s shall be surface mounted and angled in a manner that they cannot be compromised from the non-secure side of a windowed door, or allow for easy release of the locking device from a distance no greater than 6 feet from the base of the door.
3. Door position sensors shall be surface or flush mounted and wide gap with the ability to operate at a maximum distance of up to 2” (5 cm).

Q. Entry Control Devices:
1. Install all signal input and power cables.
2. Strikes and bolts shall be mounted within the door frame.
3. Mortise locks shall be mounted within the door and an electric transfer hinge shall be utilized to transfer the wire from within the door frame to the mortise lock inside the door.
4. Electromagnetic locks shall be installed with the mag-lock mounted to the door frame and the metal plate mounted to the door.

R. System Start-Up:
1. The Contractor shall not apply power to the PACS until the following items have been completed:
   a. PACS equipment items and have been set up in accordance with manufacturer's instructions.
   b. A visual inspection of the PACS has been conducted to ensure that defective equipment items have not been installed and that there are no loose connections.

c. System wiring has been tested and verified as correctly connected as indicated.
d. All system grounding and transient protection systems have been verified as installed and connected as indicated.
e. Power supplies to be connected to the PACS have been verified as the correct voltage, phasing, and frequency as indicated.

2. Satisfaction of the above requirements shall not relieve the Contractor of responsibility for incorrect installation, defective equipment items, or collateral damage as a result of Contractor work efforts.

S. Supplemental Contractor Quality Control:

1. The Contractor shall provide the services of technical representatives who are familiar with all components and installation procedures of the installed PACS; and are approved by the Contracting Officer.
2. The Contractor will be present on the job site during the preparatory and initial phases of quality control to provide technical assistance.
3. The Contractor shall also be available on an as needed basis to provide assistance with follow-up phases of quality control.
4. The Contractor shall participate in the testing and validation of the system and shall provide certification that the system installed is fully operational as all construction document requirements have been fulfilled.

3.2 TESTING AND TRAINING

All testing and training shall be compliant with the VA General Requirements, Section 01 00 00, GENERAL REQUIREMENTS. **The Contractor shall submit the Operation & Maintenance Manual & Training Material, to the Contracting Officer, for review and approval, prior to scheduling the training. Anticipate 30 days for Government review, to include review by VA COTR, VA Police and VA IT. The Contractor shall provide at least 14 days advance notice of scheduled training.**

-----END----