SECTION 28 13 00
PHYSICAL ACCESS CONTROL SYSTEM

PART 1 – GENERAL

1.1 DESCRIPTION

A. This section specifies the finishing, installation, connection, testing and certification of a complete and fully operating Physical Access Control System, hereinafter referred to as the PACS.

B. This Section includes a Physical Access Control System consisting of field-installed Controllers connected by a high-speed electronic data transmission network. The PACS shall have the following:

1. Physical Access Control:
   a. Regulating access through doors and gates
   b. Anti-passback
   c. Surge and tamper protection
   d. Push-button switches
   e. RS-232 ASCII interface
   f. Monitoring of field-installed devices
   g. Reporting

D. PACS shall provide secure and reliable identification of Federal employees and contractors by utilizing credential authentication per FIPS-201.

E. Physical Access Control System (PACS) shall consist of:

1. Field installed controllers,
2. Card readers,
3. Power supplies,
4. Interfaces with:
   a. Video Surveillance and Assessment System,
   b. Gate controls,
   c. Automatic door operators,
   d. Intrusion Detection System,
   e. Intercommunication System
   f. Fire Protection System,
   g. HVAC,
   h. Building Management System,

1.2 RELATED WORK

A. Section 01 00 00 - GENERAL REQUIREMENTS. For General Requirements.

B. Section 07 84 00 - FIRESTOPPING. Requirements for firestopping application and use.

C. Section 08 71 00 - DOOR HARDWARE. Requirements for door installation.

D. Section 10 14 00 - SIGNAGE. Requirements for labeling and signs.

E. Section 26 05 21 - LOW VOLTAGE ELECTRICAL POWER CONDUCTORS AND CABLES (600 VOLTS AND BELOW). Requirements for power cables.

F. Section 26 05 33 – RACEWAYS AND BOXES FOR ELECTRICAL SYSTEMS. Requirements for infrastructure.

G. Section 26 05 41 - UNDERGROUND ELECTRICAL CONSTRUCTION. Requirements for underground installation of wiring.

H. Section 26 56 00 - EXTERIOR LIGHTING. Requirements for perimeter lighting.

I. Section 28 05 00 - COMMON WORK RESULTS FOR ELECTRONIC SAFETY AND SECURITY. For general requirements that are common to more than one section in Division 28.

J. Section 28 05 13 - CONDUCTORS AND CABLES FOR ELECTRONIC SAFETY AND SECURITY. Requirements for conductors and cables.

K. Section 28 05 26 - GROUNDING AND BONDING FOR ELECTRONIC SAFETY AND SECURITY. Requirements for grounding of equipment.

L. Section 28 05 28.33 - CONDUITS AND BOXES FOR ELECTRONIC SAFETY AND SECURITY. Requirements for infrastructure.

M. Section 28 23 00 - VIDEO SURVEILLANCE. Requirements for security camera systems.

N. Section 28 31 00 - FIRE DETECTION AND ALARM. Requirements for integration with fire detection and alarm system.

1.3 QUALITY ASSURANCE

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. Contractor Qualifications:

1. The Contractor or security sub-contractor shall be a licensed security Contractor within the state or jurisdiction of where the

installation work is being conducted. The Contractor shall be an authorized regional representative of the Security Management System’s (PACS) manufacturer.

1.4 SUBMITTALS

A. Submit below items in conjunction with Master Specification Sections 01 33 23, SHOP DRAWINGS, PRODUCT DATA, AND SAMPLES.

B. Provide certificates of compliance with Section 1.3, Quality Assurance.

C. Provide a complete and thorough pre-installation and as-built design 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. Shop drawing 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 are 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 design packages shall go through a full review process conducted by the Contractor along with a VA representative to ensure all work has been clearly defined and completed. All reviews shall be conducted in accordance with the project schedule. There shall be four (4) stages to the review process:

1. 35 percent
2. 65 percent
3. 90 percent
4. 100 percent

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, and Section 28 05 00 COMMON WORK RESULTS FOR ELECTRONIC SAFETY AND SECURITY.

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-03..................Access Control: Access Control Guideline Dye Sublimation Printing Practices for PVC Access Control Cards

TVAC-01................CCTV to Access Control Standard - Message Set for System Integration

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..........ADA Standards for Accessible Design 2010

E. Department of Veterans Affairs (VA):

PACS-R: Physical Access Control System (PACS) Requirements

VA Handbook 0730 Security and Law Enforcement

F. Government Accountability Office (GAO):

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

G. National Electrical Contractors Association

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

H. National Electrical Manufactures Association (NEMA):

250-08..................Enclosures for Electrical Equipment (1000 Volts Maximum)

I. National Fire Protection Association (NFPA):

70-11................... National Electrical Code

J. Underwriters Laboratories, Inc. (UL):

294-99..................The Standard of Safety for Access Control System Units

305-08..................Standard for Panic Hardware

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

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

827-08..................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

K. Homeland Security Presidential Directive (HSPD):

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

L. Federal Communications Commission (FCC):

(47 CFR 15) Part 15 Limitations on the Use of Wireless Equipment/Systems

M. Federal Information Processing Standards (FIPS):

FIPS-201-1..............Personal Identity Verification (PIV) of Federal Employees and Contractors

N. 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

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

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

P. International Organization for Standardization (ISO):

7810....................Identification cards – Physical characteristics

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

7816-1..................Identification cards - Integrated circuit(s) cards with contacts - Part 1: Physical characteristics

7816-2..................Identification cards - Integrated circuit cards - Part 2: Cards with contacts -Dimensions and location of the contacts

7816-3..................Identification cards - Integrated circuit cards - Part 3: Cards with contacts - Electrical interface and transmission protocols

7816-4..................Identification cards - Integrated circuit cards - Part 11: Personal verification through biometric methods

14443...................Identification cards - Contactless integrated circuit cards; Contactless Proximity Cards Operating at 13.56 MHz in up to 5 inches distance

15693...................Identification cards -- Contactless integrated circuit cards - Vicinity cards; Contactless Vicinity Cards Operating at 13.56 MHz in up to 50 inches distance

Q. Uniform Federal Accessibility Standards (UFAS) 1984

R. ADA Standards for Accessible Design 2010

1.6 DEFINITIONS

A. ABA Track: Magnetic stripe that is encoded on track 2, at 75-bpi density in binary-coded decimal format; for example, 5-bit, 16-character set.

B. Access Control List: A list of (identifier, permissions) pairs associated with a resource or an asset. As an expression of security policy, a person may perform an operation on a resource or asset if and only if the person’s identifier is present in the access control list (explicitly or implicitly), and the permissions in the (identifier, permissions) pair include the permission to perform the requested operation.

C. Access Control: A function or a system that restricts access to authorized persons only.

D. API Application Programming Interface

E. Assurance Level (or E-Authentication Assurance Level): A measure of trust or confidence in an authentication mechanism defined in OMB Memorandum M-04-04 and NIST Special Publication (SP) 800-63, in terms of four levels: [M-04-04]

1. Level 1: LITTLE OR NO confidence
2. Level 2: SOME confidence
3. Level 3: HIGH confidence
4. Level 4: VERY HIGH confidence

F. Authentication: A process that establishes the origin of information, or determines an entity’s identity. In this publication, authentication often means the performance of a PIV authentication mechanism.

G. Authenticator: A memory, possession, or quality of a person that can serve as proof of identity, when presented to a verifier of the appropriate kind. For example, passwords, cryptographic keys, and fingerprints are authenticators.

H. Authorization: A process that associates permission to access a resource or asset with a person and the person’s identifier(s).

I. BIO or BIO-A: A FIPS 201 authentication mechanism that is implemented by using a Fingerprint data object sent from the PIV Card to the PACS. Note that the short-hand “BIO (-A)” is used throughout the document to represent both BIO and BIO-A authentication mechanisms.

J. Biometric: An authenticator produced from measurable qualities of a living person.

K. CAC EP – CAC End Point with end point PIV applet

L. CAC NG – CAC Next Generation with transitional PIV applet

M. Card Authentication Key (CAK): A PIV authentication mechanism (or the PIV Card key of the same name) that is implemented by an asymmetric or symmetric key challenge/response protocol. The CAK is an optional mechanism defined in NIST SP 800-73. [SP800-73] NIST strongly recommends that every PIV Card contain an asymmetric CAK and corresponding certificate, and that agencies use the asymmetric CAK protocol, rather than a symmetric CAK protocol, whenever the CAK authentication mechanism is used with PACS.

N. CCTV: Closed-circuit television.

O. Central Station: A PC with software designated as the main controlling PC of the PACS. Where this term is presented with initial capital letters, this definition applies.

P. Controller: An intelligent peripheral control unit that uses a computer for controlling its operation. Where this term is presented with an initial capital letter, this definition applies.

Q. CPU: Central processing unit.

R. Credential: Data assigned to an entity and used to identify that entity.

S. File Server: A PC in a network that stores the programs and data files shared by users.

T. FIPS Federal Information Processing Standards

U. FRAC – First Responder Authentication Credential

V. HSPD Homeland Security Presidential Directive

W. I/O: Input/Output.

X. Identifier: A credential card, keypad personal identification number or code, biometric characteristic, or other unique identification entered as data into the entry-control database for the purpose of identifying an individual. Where this term is presented with an initial capital letter, this definition applies.

Y. IEC International Electrotechnical Commission

Z. ISO International Organization for Standardization

AA. KB Kilobyte

BB. kbit/s Kilobits / second

CC. LAN: Local area network.

DD. LED: Light-emitting diode.

EE. Legacy CAC – Contact only Common Access Card with v1 and v2 applets

FF. Location: A Location on the network having a PC-to-Controller communications link, with additional Controllers at the Location connected to the PC-to-Controller link with RS-485 communications loop. Where this term is presented with an initial capital letter, this definition applies.

GG. NIST: National Institute of Standards and Technology

HH. PACS: Physical Access Control System

II. PC/SC: Personal Computer / Smart Card

JJ. PC: Personal computer. This acronym applies to the Central Station, workstations, and file servers.

KK. PCI Bus: Peripheral component interconnect; a peripheral bus providing a high-speed data path between the CPU and peripheral devices (such as monitor, disk drive, or network).

LL. PDF: (Portable Document Format.) The file format used by the Acrobat document exchange system software from Adobe.

MM. PIV: Personal Identification Verification

NN. PIV-I – PIV Interoperable credential

OO. PPS: Protocol and Parameters Selection

PP. RF: Radio frequency.

QQ. ROM: Read-only memory. ROM data are maintained through losses of power.

RR. RS-232: An TIA/EIA standard for asynchronous serial data communications between terminal devices. This standard defines a 25-pin connector and certain signal characteristics for interfacing computer equipment.

SS. RS-485: An TIA/EIA standard for multipoint communications.

TT. TCP/IP: Transport control protocol/Internet protocol incorporated into Microsoft Windows.

UU. TPDU: Transport Protocol Data Unit

VV. TWIC – Transportation Worker Identification Credential

WW. UPS: Uninterruptible power supply.

XX. Vcc: Voltage at the Common Collector

YY. WAN: Wide area network.

ZZ. WAV: The digital audio format used in Microsoft Windows.

AAA. Wiegand: Patented magnetic principle that uses specially treated wires embedded in the credential card.

BBB. Windows: Operating system by Microsoft Corporation.

CCC. Workstation: A PC with software that is configured for specific limited security system functions.

1.7 COORDINATION

A. Coordinate arrangement, mounting, and support of electronic safety and security equipment:

1. To allow maximum possible headroom unless specific mounting heights that reduce headroom are indicated.
2. To provide for ease of disconnecting the equipment with minimum interference to other installations.
3. To allow right of way for piping and conduit installed at required slope.
4. So connecting raceways, cables, wireways, cable trays, and busways will be clear of obstructions and of the working and access space of other equipment.

B. Coordinate installation of required supporting devices and set sleeves in cast-in-place concrete, masonry walls, and other structural components as they are constructed.

C. Coordinate location of access panels and doors for electronic safety and security items that are behind finished surfaces or otherwise concealed.

1.8 MAINTENANCE & SERVICE

A. General Requirements

1. The Contractor shall provide all services required and equipment necessary to maintain the entire integrated electronic security system in an operational state as specified for a period of one (1) year after formal written acceptance of the system. The Contractor shall provide all necessary material required for performing scheduled adjustments or other non-scheduled work. Impacts on facility operations shall be minimized when performing scheduled adjustments or other non-scheduled work. See also General Project Requirements.

1.9 WARRANTY OF CONSTRUCTION.

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

B. Demonstration and training shall be performed prior to system acceptance.

PART 2 – PRODUCTS

2.1 GENERAL

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

B. 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.

2.2 CARD READERS

A. Power: Card reader shall be powered from its associated Controller, including its standby power source.

B. Response Time: Card reader shall respond to passage requests by generating a signal that is sent to the Controller. Response time shall be 800 ms or less, from the time the card reader finishes reading the credential card until a response signal is generated.

C. Enclosure: Suitable for surface, semiflush, or pedestal mounting. Mounting types shall additionally be suitable for installation in the following locations:

1. Indoors, controlled environment.
2. Indoors, uncontrolled environment.
3. Outdoors, with built-in heaters or other cold-weather equipment to extend the operating temperature range as needed for operation at the site.

D. Display: LED or other type of visual indicator display shall provide visual[and audible] status indications and user prompts. Indicate power on/off, whether user passage requests have been accepted or rejected, and whether the door is locked or unlocked.

E. 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.

F. Will be fully programmable and addressable, locally and remotely, and hardwired to the system.

G. Shall be individually home run to the main panel.

H. Shall be installed in a manner that they comply with:

1. The Uniform Federal Accessibility Standards (UFAS)
2. The Americans with Disabilities Act (ADA)
3. The ADA Standards for Accessible Design

I. 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, ISO/IEC 7816 compliant. The reader output can be Wiegand, RS-22, 485 or TCP/IP.

J. Shall be housed in an aluminum bezel with a wide lead-in for easy card entry.

K. Shall contain read head electronics, and a sender to encode digital door control signals.

L. LED's shall be utilized to indicate card reader status and access status.

M. Shall be able to support a user defined downloadable off-line mode of operation (e.g. locked, unlocked), which will go in effect during loss of communication with the main control panel.

N. 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 audible feedback.

O. Shall have a minimum of two programmable inputs and two programmable outputs.

P. All card readers that utilize keypad controls along with a reader and shall meet the following specifications:

   1. 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.

Q. 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.

1. 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.
2. Shall be powered from the source as designed and shall not dissipate more than 150 Watts.
3. Shall be suitable for surface, semi-flush, pedestal, or weatherproof mounting as required.
4. Shall provide a means for users to indicate a duress situation by entering a special code.

R. PIV Contact Card Reader

1. Application Protocol Data Unit (APDU) Support: At a minimum, the contact interface shall support all card commands for contact based access specified in Section 7, End-point PIV Card Application Card Command Interface of SP 800-73-1, Interfaces for Personal Identity Verification.
2. Buffer Size: The reader must contain a buffer large enough to receive the maximum size frame permitted by International Organization for Standardization International Electrotechnical Commission (ISO/IEC) 7816-3:1997, Section 9.4.
3. Programming Voltage: PIV Readers shall not generate a Programming Voltage.
4. Support for Operating Class: PIV Readers shall support cards with Class A Vccs as defined in ISO/IEC 7816-3:1997 and ISO/IEC 7816-3:1997/Amd 1:2002.
5. Retrieval Time: Retrieval time[1] for 12.5 kilobytes (KB) of data through the contact interface of the reader shall not exceed 2.0 seconds.
6. Transmission Protocol: The PIV Reader shall support both the character-based T=0 protocol and block-based T=1 protocol as defined in ISO/IEC 7816-3:1997.
7. Support for PPS Procedure: The reader shall support Protocol and Parameters Selection (PPS) procedure by having the ability to read character TA1 of the Answer to Reset (ATR) sent by the card as defined in ISO/IEC 7816-3:1997.

S. 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.
   c. 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. APDU Support: At a minimum, the contactless interface shall support all card commands for contactless based access specified in Section 7, End-point PIV Card Application Card Command Interface of SP 800-73-1, Interfaces for Personal Identity Verification.
   e. Buffer Size: The reader shall contain a buffer large enough to receive the maximum size frame permitted by ISO/IEC 7816-3, Section 9.4.
   f. ISO 14443 Support: The PIV Reader shall support parts (1 through 4) of ISO/IEC 14443 as amended in the References of this publication.
   g. Type A and B Communication Signal Interfaces: The contactless interface of the reader shall support both the Type A and Type B communication signal interfaces as defined in ISO/IEC 14443-2:2001.

h. Type A and B Initialization and Anti-Collision The contactless interface of the reader shall support both Type A and Type B initialization and anti-collision methods as defined in ISO/IEC 14443-3:2001.

i. Type A and B Transmission Protocols: The contactless interface of the reader shall support both Type A and Type B transmission protocols as defined in ISO/IEC 14443-4:2001.

j. Retrieval Time: Retrieval time for 4 KB of data through the contactless interface of the reader shall not exceed 2.0 seconds.

k. Transmission Speeds: The contactless interface of the reader shall support bit rates of fc/128 (~106 kbits/s), fc/64(~212 kbits/s), and configurable to allow activation/deactivation.

l. Readibility Range: The reader shall not be able to read PIV card more than 10cm(4inch) from the reader

m. Card readers, key pads, and the like shall be of the same manufacturer and of the same model as existing devices in order to match and remain compatible with campus standard.

2.3 KEYPADS

A. Designed for use with unique combinations of alphanumeric and other symbols as an Identifier. Keys of keypads shall contain an integral alphanumeric/special symbol keyboard with symbols arranged in [ascending ASCII-code ordinal sequence] [random scrambled order]. Communications protocol shall be compatible with Controller.

1. Keypad display or enclosure shall limit viewing angles of the keypad as follows:

a. Maximum Horizontal Viewing Angle: 5 degrees or less off in either direction of a vertical plane perpendicular to the plane of the face of the keypad display.

b. Maximum Vertical Viewing Angle: 15 degrees or less off in either direction of a horizontal plane perpendicular to the plane of the face of the keypad display.

2. Duress Codes: Provide duress situation indication by entering a special code.

2.4 SYSTEM SENSORS AND RELATED EQUIPMENT

A. 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).

2.5 PORTAL CONTROL DEVICES

A. Entry Control Devices:

1. Shall be hardwired to the PACS main control panel and operated by a card reader 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 VDC, 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. Electric Mortise Locks shall:

a. These locks shall be provided and installed by the Division 8 “DOOR HARDWARE” Contractor.

b. Have integrated Request to Exit switch for doors receiving physical access control devices.

c. Provide integration of the Electric Mortise Locks with the PACS for:

1) Lock Power

2) Request to Exit switch.

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 electromagnetic locks shall be surface mounted to the door frame and the door plate shall be surface mounted to the door.

c. Ensure a diode is installed in line with the DC voltage supplying power to the unit in order to prevent back-check on the system when the electromagnetic lock is powered.

e. Electromagnetic locks shall meet the following minimum technical characteristics:

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

2.6 WIRES AND CABLES

A. Refer to section 280513 "CONDUCTORS AND CABLES FOR ELECTRONIC SAFETY AND SECURITY".

B. Comply with Division 28 Section "CONDUCTORS AND CABLES FOR ELECTRONIC SAFETY AND SECURITY."

C. Plenum-Type, RS-232 Cable: Paired, 2 pairs, No. 22 AWG, stranded (7x30) tinned copper conductors, plastic insulation, and individual aluminum foil-polyester tape shielded pairs with 100 percent shield coverage; plastic jacket. Pairs are cabled on common axis with No. 24 AWG, stranded (7x32) tinned copper drain wire.

1. NFPA 70, Type CMP.
2. Flame Resistance: NFPA 262 Flame Test.

D. RS-485 communications require 2 twisted pairs, with a distance limitation of 4000 feet (1220 m).

E. Plenum-Type, RS-485 Cable: Paired, 2 pairs, No. 22 AWG, stranded (7x30) tinned copper conductors, fluorinated-ethylene-propylene insulation, unshielded, and fluorinated-ethylene-propylene jacket.

1. NFPA 70, Type CMP.
2. Flame Resistance: NFPA 262 Flame Test.

F. Multiconductor, Readers and Wiegand Keypads Cables: No. 22 AWG, paired and twisted multiple conductors, stranded (7x30) tinned copper conductors, semirigid PVC insulation, overall aluminum foil-polyester tape shield with 100 percent shield coverage, plus tinned copper braid shield with 65 percent shield coverage, and PVC jacket.

1. NFPA 70, Type CMG.
2. Flame Resistance: UL 1581 Vertical Tray.
3. For TIA/EIA-RS-232 applications.

G. Plenum-Type, Paired, Readers and Wiegand Keypads Cable: Paired, 3 pairs, No. 22 AWG, stranded (7x30) tinned copper conductors, plastic insulation, individual aluminum foil-polypropylene tape shielded pairs each with No. 22 AWG, stranded tinned copper drain wire, 100 percent shield coverage, and fluorinated-ethylene-propylene jacket.

1. NFPA 70, Type CMP.
2. Flame Resistance: NFPA 262 Flame Test.

H. Plenum-Type, Multiconductor, Readers and Keypads Cable: 6 conductors, No. 20 AWG, stranded (7x28) tinned copper conductors, fluorinated-ethylene-propylene insulation, overall aluminum foil-polyester tape shield with 100 percent shield coverage plus tinned copper braid shield with 85 percent shield coverage, and fluorinated-ethylene-propylene jacket.

1. NFPA 70, Type CMP.
2. Flame Resistance: NFPA 262 Flame Test.

I. Plenum-Type, Paired Lock Cable: 1 pair, twisted, No. 16 AWG, stranded (19x29) tinned copper conductors, PVC insulation, unshielded, and PVC jacket.

1. NFPA 70, Type CMP.
2. Flame Resistance: NFPA 262 Flame Test.

J. Plenum-Type, Paired Lock Cable: 1 pair, twisted, No. 18 AWG, stranded (19x30) tinned copper conductors, fluorinated-ethylene-propylene insulation, unshielded, and plastic jacket.

1. NFPA 70, Type CMP.
2. Flame Resistance: NFPA 262 Flame Test.

K. Plenum-Type, Paired Input Cable: 1 pair, twisted, No. 22 AWG, stranded (7x30) tinned copper conductors, fluorinated-ethylene-propylene insulation, aluminum foil-polyester tape shield (foil side out), with No. 22 AWG drain wire, 100 percent shield coverage, and plastic jacket.

1. NFPA 70, Type CMP.
2. Flame Resistance: NFPA 262 Flame Test.

L. Plenum-Type, Paired AC Transformer Cable: 1 pair, twisted, No. 18 AWG, stranded (19x30) tinned copper conductors, fluorinated-ethylene-propylene insulation, unshielded, and plastic jacket.

1. NFPA 70, Type CMP.
2. Flame Resistance: NFPA 262 Flame Test.

M. LAN (Ethernet) Cabling: Comply with Division 28 Section "Conductors and Cables for Electronic Safety and Security."

PART 3 - EXECUTION

3.1 GENERAL

A. The Contractor shall install all system components and appurtenances in accordance with the manufacturers’ instructions, ANSI C2, and shall furnish all necessary interconnections, services, and adjustments required for a complete and operable system as specified. Control signals, communications, and data transmission lines grounding shall be installed as necessary to preclude ground loops, noise, and surges from affecting system operation. Equipment, materials, installation, workmanship, inspection, and testing shall be in accordance with manufacturers’ recommendations and as modified herein.

B. Consult the manufacturers’ installation manuals for all wiring diagrams, schematics, physical equipment sizes, etc., before beginning system installation. Refer to the Riser/Connection diagram for all schematic system installation/termination/wiring data.

C. All equipment shall be attached to walls and ceiling/floor assemblies and shall be held firmly in place (e.g., sensors shall not be supported solely by suspended ceilings). Fasteners and supports shall be adequate to support the required load.

3.2 CURRENT SITE CONDITIONS

A. The Contractor shall visit the site and verify that site conditions are in agreement with the design package. The Contractor shall report all changes to the site or conditions which will affect performance of the system to the Owner in a report as defined in paragraph Group II Technical Data Package. The Contractor shall not take any corrective action without written permission from the Owner.

3.3 EXAMINATION

A. Examine pathway elements intended for cables. Check raceways, cable trays, and other elements for compliance with space allocations, installation tolerances, hazards to cable installation, and other conditions affecting installation.

B. Examine roughing-in for LAN and control cable conduit systems to PCs, Controllers, card readers, and other cable-connected devices to verify actual locations of conduit and back boxes before device installation.

C. Proceed with installation only after unsatisfactory conditions have been corrected.

3.4 CABLING

A. Comply with NECA 1, "Good Workmanship in Electrical Contracting."

B. Install cables and wiring according to requirements in Division 28 Section "Conductors and Cables for Electronic Safety and Security."

C. Wiring Method: Install wiring in raceway and cable tray except within consoles, cabinets, desks, and counters. Conceal raceway and wiring except in unfinished spaces.

D. Wiring Method: Install wiring in raceway and cable tray except within consoles, cabinets, desks, and counters and except in accessible ceiling spaces and in gypsum board partitions where unenclosed wiring method may be used. Use NRTL-listed plenum cable in environmental air spaces, including plenum ceilings. Conceal raceway and cables except in unfinished spaces.

E. Install LAN cables using techniques, practices, and methods that are consistent with Category 6 rating of components and that ensure Category 6 performance of completed and linked signal paths, end to end.

F. Install cables without damaging conductors, shield, or jacket.

G. Boxes and enclosures containing security system components or cabling, and which are easily accessible to employees or to the public, shall be provided with a lock. Boxes above ceiling level in occupied areas of the building shall not be considered to be accessible. Junction boxes and small device enclosures below ceiling level and easily accessible to employees or the public shall be covered with a suitable cover plate and secured with tamperproof screws.

H. Install end-of-line resistors at the field device location and not at the Controller or panel location.

3.5 CABLE APPLICATION

A. Comply with EIA/TIA-569, "Commercial Building Standard for Telecommunications Pathways and Spaces."

B. Cable application requirements are minimum requirements and shall be exceeded if recommended or required by manufacturer of system hardware.

C. RS-232 Cabling: Install at a maximum distance of 50 feet (15 m).

D. RS-485 Cabling: Install at a maximum distance of 4000 feet (1220 m).

E. Card Readers and Keypads:

1. Install number of conductor pairs recommended by manufacturer for the functions specified.
2. Unless manufacturer recommends larger conductors, install No. 22 AWG wire if maximum distance from Controller to the reader is 250 feet (75 m), and install No. 20 AWG wire if maximum distance is 500 feet (150 m).
3. For greater distances, install "extender" or "repeater" modules recommended by manufacturer of the Controller.
4. Install minimum No. 18 AWG shielded cable to readers and keypads that draw 50 mA or more.

F. Install minimum No. 16 AWG cable from Controller to electrically powered locks. Do not exceed 250 feet (75 m).

G. Install minimum No. 18 AWG ac power wire from transformer to Controller, with a maximum distance of [25 feet (8 m)] <Insert distance>.

3.6 GROUNDING

A. Comply with Division 26 Section "Grounding and Bonding for Electrical Systems."

B. Comply with IEEE 1100, "Power and Grounding Sensitive Electronic Equipment."

C. Ground cable shields, drain conductors, and equipment to eliminate shock hazard and to minimize ground loops, common-mode returns, noise pickup, cross talk, and other impairments.

D. Signal Ground:

1. Terminal: Locate in each equipment room and wiring closet; isolate from power system and equipment grounding.
2. Bus: Mount on wall of main equipment room with standoff insulators.
3. Backbone Cable: Extend from signal ground bus to signal ground terminal in each equipment room and wiring closet.

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

1. 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

Physical Access Control System and Database Management of an alarm event.

b. For additional PACS requirements as they relate to the EPPS,

E. The Contractor shall visit the site and verify that site conditions are in agreement with the design package. The Contractor shall report all changes to the site or conditions that will affect performance of the system. The Contractor shall not take any corrective action without written permission from the Government.

F. The Contractor shall visit the site and verify that site conditions are in agreement/compliance with the design 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.

G. 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.

H. 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.

I. 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.

J. 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.

K. 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.

L. Door Status Indicators:

1. Install all signal input and output cables as well as all power cables.
2. 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).

M. Entry Control Devices:

1. Install all signal input and power cables.
2. 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.
3. Electromagnetic locks shall be installed with the mag-lock mounted to the door frame and the metal plate mounted to the door.

3.8 FIELD QUALITY CONTROL

A. Perform the following field tests and inspections and prepare test reports:

1. LAN Cable Procedures: Inspect for physical damage and test each conductor signal path for continuity and shorts. Use Class 2, bidirectional, Category 5 tester. Test for faulty connectors, splices, and terminations. Test according to TIA/EIA-568-1, "Commercial Building Telecommunications Cabling Standards - Part 1 General Requirements." Link performance for UTP cables must comply with minimum criteria in TIA/EIA-568-B.
2. Test each circuit and component of each system. Tests shall include, but are not limited to, measurements of power supply output under maximum load, signal loop resistance, and leakage to ground where applicable. System components with battery backup shall be operated on battery power for a period of not less than 10 percent of the calculated battery operating time. Provide special equipment and software if testing requires special or dedicated equipment.

3. Operational Test: After installation of cables and connectors, demonstrate product capability and compliance with requirements. Test each signal path for end-to-end performance from each end of all pairs installed. Remove temporary connections when tests have been satisfactorily completed.

3.9 DEMONSTRATION AND TRAINING

A. Provide services of manufacturer’s technical representative for four hours to instruct VA personnel in operation and maintenance of units.

B. Submit training plans and instructor qualifications in accordance with the requirements of Section 28 08 00 – COMMISSIONING OF ELECTRONIC SAFETY AND SECURITY SYSTEMS.

C. Develop separate training modules for the following:

1. Computer system administration personnel to manage and repair the LAN and databases and to update and maintain software.
2. Operators who prepare and input credentials to man the control station and workstations and to enroll personnel.
3. Security personnel.
4. Hardware maintenance personnel.
5. Corporate management.

D. All testing and training shall be compliant with the VA General Requirements, Section 01 00 00, GENERAL REQUIREMENTS.

-----END----