

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. The system shall be an extension of the existing Johnson Controls P2000 system. The new components shall seamlessly integrate into the facility's existing physical access control system.
- B. The existing physical access control system is under service contract with Johnson Controls (Point of Contact: Mark Bradford - 571-287-1333 Mark.K.Bradford@jci.com). The existing warranty and service contract in-place shall be maintained and not void by work performed under this project.
- C. This Section includes a Physical Access Control System consisting of a system server, operating system and application software, and 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.
- D. Physical Access Control System (PACS) shall consist of:
 - 1. Head-End equipment server,
 - 2. One or more networked PC-based workstations,
 - 3. Physical Access Control System and Database Management Software,
 - 4. Field installed controllers,
 - 5. Card readers,
 - 6. Request to exit push buttons,
 - 7. Request to exit PIR motion sensors,
 - 8. Door position switches/contacts,
 - 9. Electric Strikes,
 - 10. Power supplies
- E. Head-End equipment server, workstations and controllers shall be connected by a high-speed electronic data transmission network.
- F. Information system supporting PACS , Head-End equipment server, workstations, network switches, routers and controllers shall comply with FIPS 200 requirements (Minimum Security Requirements for Federal

Information and Information Systems) and NIST Special Publication 800-53 (Recommended Security Controls for Federal Information Systems).

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 28 05 11 - REQUIREMENTS FOR ELECTRONIC SAFETY AND SECURITY. For general requirements that are common to more than one section in Division 28.
- E. Section 28 05 13 - CONDUCTORS AND CABLES FOR ELECTRONIC SAFETY AND SECURITY. Requirements for conductors and cables.
- F. Section 28 05 33 - RACEWAYS AND BOXES FOR ELECTRONIC SAFETY AND SECURITY. Requirements for infrastructure.
- G. Section 28 08 00 - COMMISSIONING OF ELECTRONIC SAFETY AND SECURITY. For requirements for commissioning, systems readiness checklists, and training.
- H. Section 28 23 00 - VIDEO SURVEILLANCE. Requirements for security camera systems.

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. Manufacturers Qualifications: The manufacturer shall regularly and presently produce, as one of the manufacturer's principal products, the equipment and material specified for this project, and shall have manufactured the item for at least three years.
- D. Product Qualifications:
 - 1. Manufacturer's product shall have been in satisfactory operation, on three installations of similar size and type as this project, for approximately three years.

2. The Government reserves the right to require the Contractor to submit a list of installations where the products have been in operation before approval.

E. Contractor Qualifications:

1. The Contractor or security sub-contractor shall be a licensed security Contractor with a minimum of five (5) years experience installing and servicing systems of similar scope and complexity. The Contractor shall be an authorized regional representative of the Security Management System's (PACS) manufacturer. The Contractor shall provide four (4) current references from clients with systems of similar scope and complexity which became operational in the past three (3) years. At least three (3) of the references shall be utilizing the same system components, in a similar configuration as the proposed system. The references must include a current point of contact, company or agency name, address, telephone number, complete system description, date of completion, and approximate cost of the project. The owner reserves the option to visit the reference sites, with the site owner's permission and representative, to verify the quality of installation and the references' level of satisfaction with the system. The Contractor shall provide copies of system manufacturer certification for all technicians. The Contractor shall only utilize factory-trained technicians to install, program, and service the PACS. The Contractor shall only utilize factory-trained technicians to install, terminate and service controller/field panels and reader modules. The technicians shall have a minimum of five (5) continuous years of technical experience in electronic security systems. The Contractor shall have a local service facility. The facility shall be located within 60 miles of the project site. The local facility shall include sufficient spare parts inventory to support the service requirements associated with this contract. The facility shall also include appropriate diagnostic equipment to perform diagnostic procedures. The COR reserves the option of surveying the company's facility to verify the service inventory and presence of a local service organization.
 - a. The Contractor shall provide proof project superintendent with BICSI Certified Commercial Installer Level 1, Level 2, or Technician to provide oversight of the project.

- b. Cable installer must have on staff a Registered Communication Distribution Designer (RCDD) certified by Building Industry Consulting Service International. The staff member shall provide consistent oversight of the project cabling throughout design, layout, installation, termination and testing.
- F. Service Qualifications: There shall be a permanent service organization maintained or trained by the manufacturer which will render satisfactory service to this installation within four hours of receipt of notification that service is needed. Submit name and address of service organizations.

1.4 SUBMITTALS

- A. Submit below items in conjunction with Master Specification Sections 01 33 23, SHOP DRAWINGS, PRODUCT DATA, AND SAMPLES, Section 02 41 00, DEMOLITION, and Section 28 05 00 COMMON WORK RESULTS FOR ELECTRONIC SAFETY AND SECURITY.
- 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. 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.
 - 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.
- 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.

H. Completed System Readiness Checklists provided by the Commissioning Agent and completed by the contractor, signed by a qualified technician and dated on the date of completion, in accordance with the requirements of Section 28 08 00 COMMISSIONING OF ELECTRONIC SAFETY AND SECURITY SYSTEMS.

I. General: Submittals shall be in full compliance of the Contract Documents. All submittals shall be provided in accordance with this section. Submittals lacking the breadth or depth these requirements will be considered incomplete and rejected. Submissions are considered multidisciplinary and shall require coordination with applicable divisions to provide a complete and comprehensive submission package. Additional general provisions are as follows:

1. The Contractor shall schedule submittals in order to maintain the project schedule. For coordination drawings refer to Specification Section 01 33 10 - DESIGN SUBMITTAL PROCEDURES, which outline basic submittal requirements and coordination. Section 01 33 10 shall be used in conjunction with this section.
2. The Contractor shall identify variations from requirements of Contract Documents and state product and system limitations, which may be detrimental to successful performance of the completed work or system.
3. Each package shall be submitted at one (1) time for each review and include components from applicable disciplines (e.g., electrical work, architectural finishes, door hardware, etc.) which are required to produce an accurate and detailed depiction of the project.
4. Manufacturer's information used for submittal shall have pages with items for approval tagged, items on pages shall be identified, and capacities and performance parameters for review shall be clearly marked through use of an arrow or highlighting. Provide space for COR and Contractor review stamps.
5. Technical Data Drawings shall be in the latest version of AutoCAD®, drawn accurately, and in accordance with VA CAD Standards. FREEHAND SKETCHES OR COPIED VERSIONS OF THE CONSTRUCTION DOCUMENTS WILL NOT BE ACCEPTED. The Contractor shall not reproduce Contract Documents or copy standard information as the basis of the Technical Data Drawings. If departures from the technical data drawings are subsequently deemed necessary by the Contractor, details of such

departures and the reasons thereof shall be submitted in writing to the COR for approval before the initiation of work.

6. Packaging: The Contractor shall organize the submissions according to the following packaging requirements.
 - a. Binders: For each manual, provide heavy duty, commercial quality, durable three (3) ring vinyl covered loose leaf binders, sized to receive 8.5 x 11 in paper, and appropriate capacity to accommodate the contents. Provide a clear plastic sleeve on the spine to hold labels describing the contents. Provide pockets in the covers to receive folded sheets.
 - 1) Where two (2) or more binders are necessary to accommodate data, correlate data in each binder into related groupings according to the Project Manual table of contents. Cross-referencing other binders where necessary to provide essential information for communication of proper operation and or maintenance of the component or system.
 - 2) Identify each binder on the front and spine with printed binder title, Project title or name, and subject matter covered. Indicate the volume number if applicable.
 - b. Dividers: Provide heavy paper dividers with celluloid tabs for each Section. Mark each tab to indicate contents.
 - c. Protective Plastic Jackets: Provide protective transparent plastic jackets designed to enclose diagnostic software for computerized electronic equipment.
 - d. Text Material: Where written material is required as part of the manual use the manufacturer's standard printed material, or if not available, specially prepared data, neatly typewritten on 8.5 inches by 11 inches 20 pound white bond paper.
 - e. Drawings: Where drawings and/or diagrams are required as part of the manual, provide reinforced punched binder tabs on the drawings and bind them with the text.
 - 1) Where oversized drawings are necessary, fold the drawings to the same size as the text pages and use as a foldout.
 - 2) If drawings are too large to be used practically as a foldout, place the drawing, neatly folded, in the front or rear pocket of the binder. Insert a type written page indicating the drawing title, description of contents and drawing location at the appropriate location of the manual.

- 3) Drawings shall be sized to ensure details and text is of legible size. Text shall be no less than 1/16" tall.
- f. Manual Content: In each manual include information specified in the individual Specification section, and the following information for each major component of building equipment and controls:
- 1) General system or equipment description.
 - 2) Design factors and assumptions.
 - 3) Copies of applicable Shop Drawings and Product Data.
 - 4) System or equipment identification including: manufacturer, model and serial numbers of each component, operating instructions, emergency instructions, wiring diagrams, inspection and test procedures, maintenance procedures and schedules, precautions against improper use and maintenance, repair instructions, sources of required maintenance materials and related services, and a manual index.
- g. Binder Organization: Organize each manual into separate sections for each piece of related equipment. At a minimum, each manual shall contain a title page, table of contents, copies of Product Data supplemented by drawings and written text, and copies of each warranty, bond, certifications, and service Contract issued. Refer to Group I through V Technical Data Package Submittal requirements for required section content.
- h. Title Page: Provide a title page as the first sheet of each manual to include the following information; project name and address, subject matter covered by the manual, name and address of the Project, date of the submittal, name, address, and telephone number of the Contractor, and cross references to related systems in other operating and/or maintenance manuals.
- i. Table of Contents: After the title page, include a type written table of contents for each volume, arranged systematically according to the Project Manual format. Provide a list of each product included, identified by product name or other appropriate identifying symbols and indexed to the content of the volume. Where more than one (1) volume is required to hold data for a particular system, provide a comprehensive table of contents for all volumes in each volume of the set.

- j. General Information Section: Provide a general information section immediately following the table of contents, listing each product included in the manual, identified by product name. Under each product, list the name, address, and telephone number of the installer and maintenance Contractor. In addition, list a local source for replacement parts and equipment.
- k. Drawings: Provide specially prepared drawings where necessary to supplement the manufacturers printed data to illustrate the relationship between components of equipment or systems, or provide control or flow diagrams. Coordinate these drawings with information contained in Project Record Drawings to assure correct illustration of the completed installation.
- l. Manufacturer's Data: Where manufacturer's standard printed data is included in the manuals, include only those sheets that are pertinent to the part or product installed. Mark each sheet to identify each part or product included in the installation. Where more than one (1) item in tabular format is included, identify each item, using appropriate references from the Contract Documents. Identify data that is applicable to the installation and delete references to information which is not applicable.
- m. Where manufacturer's standard printed data is not available and the information is necessary for proper operation and maintenance of equipment or systems, or it is necessary to provide additional information to supplement the data included in the manual, prepare written text to provide the necessary information. Organize the text in a consistent format under a separate heading for different procedures. Where necessary, provide a logical sequence of instruction for each operating or maintenance procedure. Where similar or more than one product is listed on the submittal the Contractor shall differentiate by highlighting the specific product to be utilized.
- n. Calculations: Provide a section for circuit and panel calculations.
- o. Loading Sheets: Provide a section for DGP Loading Sheets.
- p. Certifications: Provide section for Contractor's manufacturer certifications.

7. Contractor Review: Review submittals prior to transmittal.
Determine and verify field measurements and field construction criteria. Verify manufacturer's catalog numbers and conformance of submittal with requirements of contract documents. Return non-conforming or incomplete submittals with requirements of the work and contract documents. Apply Contractor's stamp with signature certifying the review and verification of products occurred, and the field dimensions, adjacent construction, and coordination of information is in accordance with the requirements of the contract documents.
 8. Resubmission: Revise and resubmit submittals as required within 15 calendar days of return of submittal. Make resubmissions under procedures specified for initial submittals. Identify all changes made since previous submittal.
 9. Product Data: Within 15 calendar days after execution of the contract, the Contractor shall submit for approval a complete list of all of major products proposed for use. The data shall include name of manufacturer, trade name, model number, the associated contract document section number, paragraph number, and the referenced standards for each listed product.
- Q. Completed System Readiness Checklists provided by the Commissioning Agent and completed by the contractor, signed by a qualified technician and dated on the date of completion, in accordance with the requirements of Section 28 08 00 COMMISSIONING OF ELECTRONIC SAFETY AND SECURITY SYSTEMS.

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 Manufacturers 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 800-63.....Electronic Authentication Guideline
- Special Pub 800-96.....PIV Card Reader Interoperability Guidelines
- Special Pub 800-73-3....Interfaces for Personal Identity Verification
(4 Parts)
-Pt. 1- End Point PIV Card Application
Namespace, Data Model & Representation
-Pt. 2- PIV Card Application Card Command
Interface
-Pt. 3- PIV Client Application Programming
Interface
-Pt. 4- The PIV Transitional Interfaces & Data
Model Specification
- Special Pub 800-76-1....Biometric Data Specification for Personal
Identity Verification
- Special Pub 800-78-2....Cryptographic Algorithms and Key Sizes for
Personal Identity Verification
- Special Pub 800-79-1....Guidelines for the Accreditation of Personal
Identity Verification Card Issuers
- Special Pub 800-85B-1...DRAFTPIV Data Model Test Guidelines
- Special Pub 800-85A-2...PIV Card Application and Middleware Interface
Test Guidelines (SP 800-73-3 compliance)
- Special Pub 800-96.....PIV Card Reader Interoperability Guidelines
- Special Pub 800-37.....Guide for Applying the Risk Management
Framework to Federal Information Systems
- Special Pub 800-96.....PIV Card Reader Interoperability Guidelines
- Special Pub 800-96.....PIV Card Reader Interoperability Guidelines
- Special Pub 800-104A....Scheme for PIV Visual Card Topography
- Special Pub 800-116.....Recommendation for the Use of PIV Credentials
in Physical Access Control Systems (PACS)
- 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

7816-10.....Identification cards - Integrated circuit cards
- Part 4: Organization, security and commands
for interchange

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

19794.....Information technology - Biometric data
interchange formats

Q. Uniform Federal Accessibility Standards (UFAS) 1984

R. ADA Standards for Accessible Design 2010

S. Section 508 of the Rehabilitation Act of 1973

1.6 DEFINITIONS

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.

B. Description of Work

1. The adjustment and repair of the security system includes all software updates, panel firmware, and the following new items computers equipment, communications transmission equipment and data transmission media (DTM), local processors, security system sensors, physical access control equipment, facility interface, signal transmission equipment, and video equipment.

C. Personnel

1. Service personnel shall be certified in the maintenance and repair of the selected type of equipment and qualified to accomplish all work promptly and satisfactorily. The COR shall be advised in writing of the name of the designated service representative, and of any change in personnel. The COR shall be provided copies of system manufacturer certification for the designated service representative.

D. Schedule of Work

1. The work shall be performed during regular working ours, Monday through Friday, excluding federal holidays. These inspections shall include:
 - a) The Contractor shall perform two (2) minor inspections at six (6) month intervals or more if required by the manufacturer, and two (2) major inspections offset equally between the minor inspections to effect quarterly inspection of alternating magnitude.
 - 1) Minor Inspections shall include visual checks and operational tests of all console equipment, peripheral equipment, local processors, sensors, electrical and mechanical controls, and adjustments on printers.
 - 2) Major Inspections shall include all work described for Minor Inspections and the following: clean all system equipment and local processors including interior and exterior surfaces; perform diagnostics on all equipment; operational tests of the CPU, switcher, peripheral equipment, recording devices, monitors, picture quality from each camera; check, walk test, and calibrate each sensor; run all system software diagnostics and correct all problems; and resolve any previous outstanding problems.

E. Emergency Service

1. The owner shall initiate service calls whenever the system is not functioning properly. The Contractor shall provide the Owner with an emergency service center telephone number. The emergency service center shall be staffed 24 hours a day 365 days a year. The Owner shall have sole authority for determining catastrophic and non-catastrophic system failures within parameters stated in General Project Requirements.
 - a. For catastrophic system failures, the Contractor shall provide same day four (4) hour service response with a defect correction time not to exceed eight (8) hours from [notification] [arrival on site]. Catastrophic system failures are defined as any system failure that the Owner determines will place the facility(s) at increased risk.
 - b. For non-catastrophic failures, the Contractor within eight (8) hours with a defect correction time not to exceed 24 hours from notification.

F. Operation

1. Performance of scheduled adjustments and repair shall verify operation of the system as demonstrated by the applicable portions of the performance verification test.

G. Records & Logs

1. The Contractor shall maintain records and logs of each task and organize cumulative records for each component and for the complete system chronologically. A continuous log shall be submitted for all devices. The log shall contain all initial settings, calibration, repair, and programming data. Complete logs shall be maintained and available for inspection on site, demonstrating planned and systematic adjustments and repairs have been accomplished for the system.

H. Work Request

1. The Contractor shall separately record each service call request, as received. The record shall include the serial number identifying the component involved, its location, date and time the call was received, specific nature of trouble, names of service personnel assigned to the task, instructions describing the action taken, the amount and nature of the materials used, and the date and time of commencement and completion. The Contractor shall deliver a record of the work performed within five (5) working days after the work was completed.

I. System Modifications

1. The Contractor shall make any recommendations for system modification in writing to the COR. No system modifications, including operating parameters and control settings, shall be made without prior written approval from the COR. Any modifications made to the system shall be incorporated into the operation and maintenance manuals and other documentation affected.

J. Software

1. The Contractor shall provide all software updates when approved by the Owner from the manufacturer during the installation and 12-month warranty period and verify operation of the system. These updates shall be accomplished in a timely manner, fully coordinated with the system operators, and incorporated into the operations and maintenance manuals and software documentation. There shall be at least one (1) scheduled update near the end of the first year's

warranty period, at which time the Contractor shall install and validate the latest released version of the Manufacturer's software. All software changes shall be recorded in a log maintained in the unit control room. An electronic copy of the software update shall be maintained within the log. At a minimum, the contractor shall provide a description of the modification, when the modification occurred, and name and contact information of the individual performing the modification. The log shall be maintained in a white 3 ring binder and the cover marked "SOFTWARE CHANGE LOG".

1.9 EQUIPMENT AND MATERIALS

- A. Materials and equipment furnished shall be of current production by manufacturers regularly engaged in the manufacture of such items, for which replacement parts shall be available.
- B. When more than one unit of the same class of equipment is required, such units shall be the product of a single manufacturer.
- C. Equipment Assemblies and Components:
 - 1. Components of an assembled unit need not be products of the same manufacturer.
 - 2. Manufacturers of equipment assemblies, which include components made by others, shall assume complete responsibility for the final assembled unit.
 - 3. Components shall be compatible with each other and with the total assembly for the intended service.
 - 4. Constituent parts which are similar shall be the product of a single manufacturer.
- D. Factory wiring shall be identified on the equipment being furnished and on all wiring diagrams.
- E. When Factory Testing Is Specified:
 - 1. The Government shall have the option of witnessing factory tests. The contractor shall notify the VA through the COR a minimum of 15 working days prior to the manufacturers making the factory tests.
 - 2. Four copies of certified test reports containing all test data shall be furnished to the COR prior to final inspection and not more than 90 days after completion of the tests.
 - 3. When equipment fails to meet factory test and re-inspection is required, the contractor shall be liable for all additional expenses, including expenses of the Government.

1.10 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.

1.11 GENERAL REQUIREMENTS

- A. For general requirements that are common to more than one section in Division 28 refer to Section 28 05 00, REQUIREMENTS FOR ELECTRONIC SAFETY AND SECURITY INSTALLATIONS.
- B. General requirements applicable to this section include:
 - 1. General Arrangement of Contract Documents,
 - 2. Delivery, Handling and Storage,
 - 3. Project Conditions,
 - 4. Electrical Power,
 - 5. Lightning, Power Surge Suppression, and Grounding,
 - 6. Electronic Components,
 - 7. Substitute Materials and Equipment, and
 - 8. Like Items.

PART 2 - PRODUCTS**2.1 GENERAL**

- A. The system shall be an extension of the existing Johnson Controls P2000 system. Model numbers listed are basis of design.
- B. All equipment and materials for the system will be compatible to ensure correct operation as outlined in FIPS 201, March 2006 and HSPD-12.
- C. 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.
- D. PACS equipment shall meet or exceed all requirements listed below.
- E. A PACS shall be comprised of, but not limited to, the following components:
 - 1. Controllers (Data Gathering Panel)
 - 2. Card Readers
 - 3. System Sensors and Related Equipment
 - 4. Push Button Switches
 - 5. Interfaces
 - 6. Cables

7. Power Supplies/Transformers

2.2 CONTROLLERS

A. Basis of Design Manufacturer:

1. Network Controller - Johnson Controls Model CK721-A
2. 2 Door Controller - Johnson Controls Model S300-DIN-RDR2SA
3. 8-door Controller: Johnson Controls Model S300-DIN-RDR2SA
4. Access Control Panel: Johnson Controls Panel SPA1D20012F10.

B. Controllers: Intelligent peripheral control unit, complying with UL 294, that stores time, date, valid codes, access levels, and similar data downloaded from the Central Station or workstation for controlling its operation.

C. Subject to compliance with requirements in this Article, manufacturers may use multipurpose Controllers.

D. Battery Backup: Sealed, lead acid; sized to provide run time during a power outage of 90 minutes, complying with UL 924.

E. Entry-Control Controller:

1. Function: Provide local entry-control functions including one- and two-way communications with access-control devices such as card readers, keypads, door strikes, magnetic latches, door operators, and exit push-buttons.
 - a. Operate as a stand-alone portal Controller using the downloaded database during periods of communication loss between the Controller and the field-device network.
 - b. Accept information generated by the entry-control devices; automatically process this information to determine valid identification of the individual present at the portal:
 - 1) On authentication of the credentials or information presented, check privileges of the identified individual, allowing only those actions granted as privileges.
 - 2) Privileges shall include, but not be limited to, time of day control, day of week control, group control, and visitor escort control.
 - c. Maintain a date-, time-, and Location-stamped record of each transaction. A transaction is defined as any successful or unsuccessful attempt to gain access through a controlled portal by the presentation of credentials or other identifying information.

2. Inputs:

- a. Data from entry-control devices; use this input to change modes between access and secure.
- b. Database downloads and updates from the Central Station that include enrollment and privilege information.
- 3. Outputs:
 - a. Indicate success or failure of attempts to use entry-control devices and make comparisons of presented information with stored identification information.
 - b. Grant or deny entry by sending control signals to portal-control devices and mask intrusion alarm annunciation from sensors stimulated by authorized entries].
 - c. Maintain a date-, time-, and Location-stamped record of each transaction and transmit transaction records to the Central Station.
 - d. Door Prop Alarm: If a portal is held open for longer than [20 seconds] [time listed in a schedule], alarm sounds.
- 4. With power supplies sufficient to power at voltage and frequency required for field devices and portal-control devices.
- 6. Controller Power: NFPA 70, Class II power supply transformer, with 12- or 24-V ac secondary, backup battery and charger.

2.3 CARD READERS

- A. Basis of Design Manufacturer: HID Model 6145C
- B. 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]<insert number>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.

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.

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

2.4 SYSTEM SENSORS AND RELATED EQUIPMENT

- A. The PACS (Physical Access Control System) and related Equipment provided by the Contractor shall meet or exceed the following performer specifications:

B. Request to Exit Detectors:

1. Passive Infrared Request to Exit Motion Detector (REX PIR) (1) The Contractor shall provide a surface mounted motion detector to signal the physical access control system request to exit input. The motion detector shall be a passive infrared sensor designed for wall or ceiling mounting 2134 to 4572 mm (7 to 15 ft) height. The detector shall provide two (2) form "C" (SPDT) relays rated one (1) Amp. @ 30 VDC for DC resistive loads. The detectors relays shall be user adjustable with a latch time from 1-60 seconds. The detector shall also include a selectable relay reset mode to follow the timer or absence of motion. The detection pattern shall be adjustable plus or minus fourteen (± 14) degrees. The detector shall operate on 12 VDC with approximately 26 mA continuous current draw. The detector shall have an externally visible activation LED. The motion detector shall measure approximately 38 mm H x 158 mm W x 38 mm D (1.5 x 6.25 x 1.5 in). The detector shall be immune to radio frequency interference. The detector shall not activate or set-up on critical frequencies in the range 26 to 950 Megahertz using a 50 watt transmitter located 30.5 cm (1 ft) from the unit or attached wiring. The detector shall be available on gray or black enclosures. The color of the housing shall be coordinated with the surrounding surface.

D. Delayed Egress (DE)

1. General:
 - a. The delay egress locking hardware shall provide a method to secure emergency exits and provide an approved delayed emergency exit method. The package shall be Underwriters Laboratories listed as a delay egress-locking device. The delay egress device shall be available to support configurations with both rated and non-rated fire doors. The delay egress device shall comply with Life Safety Codes (NFPA-101, BOCA) as it applies to special locking arrangements for delay egress locks. Unless specifically identified as a non-fire rated opening, all doors shall be equipped with fire rated door hardware. The Contractor shall be responsible for providing all equipment and installation to provide a fully functioning system. Need to amend to use crashbars type mechanical release switches.

2. The delay-locking device shall include all of the following features:
 - a. Delay Egress Mode
 - 1) The delayed egress device shall be a SDC 101V Series Exit Check with wall mounted control module. Upon activation of an approved panic bar the delay locking device shall begin a delay sequence of 30 seconds; a flush mounted wall LED panel adjacent to the door will indicate initiation of the countdown time. During the 30 second delay period, a local sounding device shall annunciate a tone activation of the delay cycle and verbal exit instructions. At the end of the delay cycle the locking device shall unlock and allow free egress. The reset of the local sounding device shall be user definable and include options to select either local sound until silenced by reset or local sounder silenced upon opening of the door. Unless otherwise indicated the local delay sounder shall be silenced upon opening of the door. The SDC's device trigger output shall be connected to the SMS DGP alarm panel for pre-activation warning. The contractor shall specify the bond sensor option when ordering the delayed egress hardware; this output shall be wired to the SMS DGP to activate an alarm if the door does not lock. Use of reset panel not top mounted device.
 - 2) Delayed egress doors will have bond sensors.
 - 3) Delayed egress activation shall also trigger CCTV call -up.
 - b. Fire Alarm Mode
 - 1) Upon activation of the facility's fire evacuation and water flow alarm signal the delay locking devices shall immediately unlock and provide free egress. The Contractor shall provide any required fire alarm relays or interface devices.
 - c. Reset Mode
 - 1) The delay egress device shall be manually reset by the Delayed Egress controller located at the door via key switch.
 - 2) The delay egress device shall automatically reset upon fire alarm system reset.
 - 3) The delayed egress shall be resettable through the SMS.
 - d. The Contractor shall provide a Master Open Switch for all the facility's delayed egress hardware, with protective cover and

permanent labeling in the Unit Control Room. The switch shall be wired into the fire alarm system to activate the evacuation alarms. When the switch is pressed all delayed egress or evacuation doors shall unlock and generate an alarm at the security console monitor showing and recording time and date of when the switch was pressed. The contractor is responsible for coordinating the wiring and connection with the fire alarm contactor. The Master Open Switch shall be linked to the fire alarm panel for the release of doors locks.

- e. Each individual delayed egress door shall have the ability to unlock through a manual action on the SMS.
- f. Unless otherwise indicated the Contractor shall provide all of the above reset methods for each door. All signs will meet the latest ADA requirements.
- g. Signs
 - 1) The delay egress package shall be provided with a warning sign complying with local code requirements. The warning sign shall be attached to the interior side of the controlled door. The sign shall be located on the interior side of the door above and within 304 mm (12 in) of the panic bar. The sign shall read:
EMERGENCY EXIT.
PUSH UNTIL
ALARM SOUNDS
DOOR CAN BE OPENED,
IN 30 SECONDS.
 - 2) Signs shall be coordinated and comply with the building's existing sign specifications. Signs shall include grade 2 Braille.
 - 3) Signs shall meet the current ADA requirements.
 - 4) In instances of code and specification conflicts, the life safety code requirement shall prevail.
 - 5) The Division 10 Contractor shall provide samples for approval with their submittal package.

3. Physical Access Control Interface

- a. The delay egress device shall be capable of interface with card access control systems.

- b. The system shall include a bypass feature that is activated via a dry contact relay output from the physical access control system. This bypass shall allow authorized personnel to pass through the controlled portal without creating an alarm condition or activating the delay egress cycle. The bypass shall include internal electronic shunts or door switches to prevent activation (re-arming) until the door returns to the closed position. An unused access event shall not cause a false alarm and shall automatically rearm the delay egress lock upon expiration of the programmed shunt time. The delay egress physical access control interface shall support extended periods of automated and/or manual lock and unlock cycles.

E. Crash Bar:

1. Emergency Exit with Alarm (Panic):

- a. Entry control portals shall include panic bar emergency exit hardware as designed.
- b. Panic bar emergency exit hardware shall provide an alarm shunt signal to the PACS and SMS.
- c. 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.
- d. 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.
- e. The panic bar shall utilize a fully mechanical connection only and shall not depend upon electric power for operation.
- f. 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.

g. 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 bypass. 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.

G. Automatic Door Opener and Closer:

1. Shall be low energy operators.
2. Door closing force shall be adjustable to ensure adequate closing control.
3. Shall have an adjustable back-check feature to cushion the door opening speed if opened violently.
4. 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.
5. 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.
6. Door control shall be adjustable to provide compliance with the requirements of the Americans with Disabilities Act (ADA) and ANSI standards A117.1.
7. All automatic door openers and closers shall:
 - a. Meet UL standards.
 - b. Be fire rated.
 - c. Have push and go function to activate power operator or power assist function.
 - d. Have push button controls for setting door close and door open positions.

- e. Have open obstruction detection and close obstruction detection built into the unit.
 - f. 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.
 - g. 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.
 - h. 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.
- H. 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 PUSH BUTTON SWITCHES

- A. Push-Button Switches: Momentary-contact back-lighted push buttons, with stainless-steel switch enclosures.
- 1. Electrical Ratings:
 - a. Minimum continuous current rating of [10] <Insert number> A at 120 V ac or [5] <Insert number> A at 240-V ac.

- b. Contacts that will make 720 VA at [60] <Insert number> A and that will break at 720 VA at [10] <Insert number> A.
- 2. Enclosures: Flush or surface mounting. Push buttons shall be suitable for flush mounting in the switch enclosures.
- 3. Enclosures shall additionally be suitable for installation in the following locations:
 - a. Indoors, controlled environment.
- 4. Power: Push-button switches shall be powered from their associated Controller, using dc control.

2.6 PORTAL CONTROL DEVICES

- A. Shall be used to assist the PACS.
- B. Such devices shall:
 - 1. Provide a means of monitoring the doors status.
 - 2. Allow for exiting a space via either a push button, request to exit, or panic/crash bar.
 - 3. Provide a means of override to the PACS via a keypad or key bypass.
 - 4. Assist door operations utilizing automatic openers and closures.
 - 5. Provide a secondary means of access to a space via a keypad.
- C. Shall be connected to and monitored by the main PACS panel.
- D. 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
- E. Shall provide a secondary means of physical access control within a secure area.
- G. 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 varistor (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. 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.
 - d. 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)

2.7 POWER SUPPLIES

- A. Basis of Design Manufacturer: Altronix Model AL600ULACM.
- B. Converts 120VAC to (8) independently controlled 12VDC or 24VDC fail-safe and/or fail-secure outputs with a total of 6 amp continuous supply current.

2.8 WIRES AND CABLES

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

- B. Comply with manufacturer's recommendations and requirements for all wiring types.
- 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).
- F. 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.
- G. 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.
 - 2. Flame Resistance: UL 1581 Vertical Tray.
 - 2. Flame Resistance: NFPA 262 Flame Test.
- M. 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.
- Q. 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.

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 PREPARATION

- A. Comply with recommendations in SIA CP-01.

- B. Comply with EIA/TIA-606, "Administration Standard for the Telecommunications Infrastructure of Commercial Buildings."
- C. Obtain detailed Project planning forms from manufacturer of access-control system; develop custom forms to suit Project. Fill in all data available from Project plans and specifications and publish as Project planning documents for review and approval.
 - 1. Record setup data for control station and workstations.
 - 2. For each Location, record setup of Controller features and access requirements.
 - 3. Propose start and stop times for time zones and holidays, and match up access levels for doors.
 - 4. Set up groups, linking, and list inputs and outputs for each Controller.
 - 5. Assign action message names and compose messages.
 - 6. Set up alarms. Establish interlocks between alarms, intruder detection, and video surveillance features.
 - 7. Prepare and install alarm graphic maps.
 - 8. Develop user-defined fields.
 - 9. Develop screen layout formats.
 - 10. Propose setups for guard tours and key control.
 - 11. Discuss badge layout options; design badges.
 - 12. Complete system diagnostics and operation verification.
 - 13. Prepare a specific plan for system testing, startup, and demonstration.
 - 14. Develop acceptance test concept and, on approval, develop specifics of the test.
 - 15. Develop cable and asset management system details; input data from construction documents. Include system schematics and Technical Drawings.
- D. In meetings with Architect and Owner, present Project planning documents and review, adjust, and prepare final setup documents. Use final documents to set up system software.

3.5 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."
- D. Wiring Method: Install wiring in raceway 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.

3.6 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:
 - 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).

3.7 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.

3.8 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.
- I. 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.
- J. Existing Equipment:

1. The Contractor shall connect to and utilize existing door equipment, control signal transmission lines, and devices as outlined in the design 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.
- K. 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.

M. 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.

O. 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.

Q. 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.

R. 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).

S. 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.

T. 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.
3. The Commissioning Agent will observe startup and contractor testing of selected equipment. Coordinate the startup and contractor testing schedules with the COR and Commissioning Agent. Provide a minimum of 7 days prior notice.

U. 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.

3.9 SYSTEM SOFTWARE

- A. Install, configure, and test software and databases for the complete and proper operation of systems involved. Assign software license to Owner.

3.10 FIELD QUALITY CONTROL

- A. Manufacturer's Field Service: Engage a factory-authorized service representative to inspect, test, and adjust field-assembled components and equipment installation, including connections, and to assist in field testing]. Report results in writing.

3.12 COMMISSIONING

- A. Provide commissioning documentation in accordance with the requirements of Section 28 08 00 - COMMISSIONING OF ELECTRONIC SAFETY AND SECURITY SYSTEMS for all inspection, start up, and contractor testing required above and required by the System Readiness Checklist provided by the Commissioning Agent.
- B. Components provided under this section of the specification will be tested as part of a larger system. Refer to Section 28 08 00 - COMMISSIONING OF ELECTRONIC SAFETY AND SECURITY SYSTEMS and related sections for contractor responsibilities for system commissioning.

3.13 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-----