

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 a 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 gates] other access-control devices.
 - b. Anti-passback
 - c. Surge and tamper protection
 - d. Secondary alarm annunciator
 - e. Credential cards and readers
 - f. Push-button switches
 - g. RS-232 ASCII interface
 - h. Credential creation and credential holder database and management
 - i. Monitoring of field-installed devices
 - j. Interface with elevator control systems.
 - k. Reporting
 - 2. Security:
 - a. Video and camera control.
 - b. Time and attendance
- C. System Architecture:
 - 1. Criticality, operational requirements, and/or limiting points of failure shall dictate the development of an enterprise and regional server architecture as opposed to system capacity. Provide server and workstation configurations with all necessary connectors, interfaces and accessories as shown.
- 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. Physical Access Control System and Database Management Software,
2. Credential validation software/hardware,
3. Field installed controllers,
4. PIV Middleware,
5. Card readers,
6. Supportive information system,
7. Door locks and sensors,
8. Power supplies,
9. Interfaces with:
 - a. Video Surveillance and Assessment System,
 - b. Traffic arm controls,
 - c. Automatic door operators,
 - d. Fire Protection System,
 - e. Elevator Controls,
- F. Controllers shall be connected by a high-speed electronic data transmission network to the existing Johnson Control system.
- G. Information system supporting PACS, 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).
- H. PACS system shall support:
 1. Multiple credential authentication modes,
 2. Incident response policy implementation capability; system shall have capability to automatically change access privileges for certain user groups to high security areas in case of incident/emergency.
- I. All security relevant decisions shall be made on "secure side of the door". Secure side processing shall include:
 1. Challenge/response management,
 2. PKI path discovery and validation,
 3. Credential identifier processing,
 4. Authorization decisions.
- J. For locations where secure side processing is not applicable the tamper switches and certified cryptographic processing shall be provided per FIPS-140-2.
- K. System Software: Based on Johnson Control central-station, workstation operating system, server operating system, and application software.

- L. Software and controllers shall be capable of matching full 56 bit FASC-N plus minimum of 32 bits of public key certificate data.
- M. Software shall have the following capabilities:
 - 1. Multiuser multitasking to allow for independent activities and monitoring to occur simultaneously at different workstations.
 - 2. Support authentication and enrolment;
 - a. PIV verification,
 - b. Expiration date check,
 - c. Biometric check,
 - d. Digital photo display/check,
 - e. Validate digital signatures of data objects (Objects are signed by the Trusted Authority
 - f. Private key challenge (CAK & PAK to verify private key public key pairs exist and card is not a clone)
 - 3. Support CRL validation via OCSP or SCVP on a scheduled basis and automatically deny access to any revoked credential in the system.
 - 4. Graphical user interface to show pull-down menus and a menu tree format that complies with interface guidelines of Microsoft Windows operating system.
 - 5. System license shall be for the entire system and shall include capability for future additions that are within the indicated system size limits specified in this Section.
 - 6. System shall have open architecture that allows importing and exporting of data and interfacing with other systems that are compatible with operating system.
 - 7. Operator login and access shall be utilized via integrated smart card reader and password protection.
- N. Systems Networks:
 - 1. A standalone system network shall interconnect all components of the system. This network shall include communications between a central station and any peer or subordinate workstations, enrollment stations, local annunciation stations, portal control stations or redundant central stations.
- O. Security Management System Server Redundancy:
 - 1. The SMS shall support multiple levels of fault tolerance and SMS redundancy listed and described below:
 - a. Hot Standby Servers

- b. Clustering
 - c. Disk Mirroring
 - d. RAID Level 10
 - e. Distributed Intelligence
- P. Number of points:
- 1. PACS shall support multiple autonomous regional servers that can connect to a master command and controller server.
 - 2. Unlimited number of access control readers, unlimited number of inputs or outputs, unlimited number of client workstations, unlimited number of cardholders.
 - 3. Total system solution to enable enterprise-wide, networked, multi-user access to all system resources via a wide range of options for connectivity with the customer's existing LAN and WAN.
- Q. Network(s) connecting PCs and Controllers shall comply with NIST Special Publication 800-53 (Recommended Security Controls for Federal Information Systems) and consist of one or more of the following:
- 1. Local area, IEEE 802.3 Fast Ethernet 100/1000 BASE-TX, star topology network based on TCP/IP.
 - 2. Direct-connected, RS-232 cable from the COM port of the Central Station to the first Controller, then RS-485 to interconnect the remainder of the Controllers at that Location.

1.2 RELATED WORK

- A. Section 01 00 00 - GENERAL REQUIREMENTS. For General Requirements.
- B. Section 07 84 00 - FIRESTOPPING. Requirements for fire stopping 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 14 24 01 - HOLES HYDRAULIC ELEVATORS. Requirements for elevators.
- F. Section 26 05 11 - REQUIREMENTS FOR ELECTRICAL INSTALLATIONS. Requirements for connection of high voltage.
- G. Section 26 05 19 - LOW VOLTAGE ELECTRICAL POWER CONDUCTORS AND CABLES (600 VOLTS AND BELOW). Requirements for power cables.
- H. Section 26 05 33 - RACEWAYS AND BOXES FOR ELECTRICAL SYSTEMS. Requirements for infrastructure.
- I. Section 26 05 41 - UNDERGROUND ELECTRICAL CONSTRUCTION. Requirements for underground installation of wiring.

- J. Section 26 56 00 - EXTERIOR LIGHTING. Requirements for perimeter lighting.
- K. 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.
- L. Section 28 05 13 - CONDUCTORS AND CABLES FOR ELECTRONIC SAFETY AND SECURITY. Requirements for conductors and cables.
- M. Section 28 05 26 - GROUNDING AND BONDING FOR ELECTRONIC SAFETY AND SECURITY. Requirements for grounding of equipment.
- N. Section 28 05 28.33 - CONDUITS AND BOXES FOR ELECTRONIC SAFETY AND SECURITY. Requirements for infrastructure.
- O. 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 shall 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 three (3) 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 shall 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 three (3) continuous years of technical experience in electronic security systems. The Contractor shall have a local service facility. The facility shall be located within 4 hours 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 Contracting Officer's Representative 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 shall 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 shall 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, and Section 28 05 00 COMMON WORK RESULTS FOR ELECTRONIC SAFETY AND SECURITY.
- B. Provide certificates of compliance with Quality Assurance section.
- 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:
 - 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 shall:
 - 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 shall 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).
 - 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 shall 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).
 - 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 the COR 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.
- H. General: Submittals shall be in full compliance of the Contract Documents. All submittals shall be provided in accordance with this section. Submittals lacking the breath or depth these requirements shall 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 23 - SHOP DRAWINGS, PRODUCT DATA, and SAMPLES, which outline basic submittal requirements and coordination. Section 01 33 23 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

shall 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, and door hardware) 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 Contracting Officer's Representative 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 SHALL 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 Contracting Officer's Representative 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.
- I. Group 1 Technical Data Package: Group I Technical Data Package shall be one submittal consisting of the following content and organization. Refer to VA Special Conditions Document for drawing format and content requirements. The data package shall include the following:
1. Section I - Drawings:
 - a. General - Drawings shall conform to VA Special Conditions and CAD Standards Documents. All text associated with security details shall be 1/8" tall and meet VA text standard for AutoCAD™ drawings.
 - b. Cover Sheet - Cover sheet shall consist of Project Title and Address, Project Number, Area and Vicinity Maps.
 - c. General Information Sheets - General Information Sheets shall consist of General Notes, Abbreviations, Symbols, Wire and Cable Schedule, Project Phasing, and Sheet Index.
 - d. Floor Plans - Floor plans shall be produced from the Architectural backgrounds issued in the Construction Documents. The contractor shall receive floor plans from the prime A/E to develop these drawing sets. Security devices shall be placed on drawings in scale. All text associated with security details shall be 1/8" tall and meet VA text standard for AutoCAD™ drawings. Floor plans shall identify the following:
 - 1) security devices by symbol,
 - 2) the associated device point number (derived from the loading sheets),
 - 3) wire & cable types and counts
 - 4) conduit sizing and routing
 - 5) conduit riser systems
 - 6) device and area detail call outs
 - e. Architectural details - Architectural details shall be produced for each device mounting type (door details for doors with

physical access control, reader pedestals and mounts, security panel and power supply details).

- f. Riser Diagrams - Contractor shall provide a riser diagram indicating riser architecture and distribution of the physical access control system throughout the facility (or area in scope).
- g. Block Diagrams - Contractor shall provide a block diagram for the entire system architecture and interconnections with SMS subsystems. Block diagram shall identify SMS subsystem (e.g., physical access control, closed circuit television, and other associated subsystems) integration; and data transmission and media conversion methodologies.
- h. Interconnection Diagrams - Contractor shall provide interconnection diagram for each sensor, and device component. Interconnection diagram shall identify termination locations, standard wire detail to include termination schedule. Diagram shall also identify interfaces to other systems such as elevator control, and security management systems.
- i. Security Details:
 - 1) Panel Assembly Detail - For each panel assembly, a panel assembly details shall be provided identifying individual panel component size and content.
 - 2) Panel Details - Provide security panel details identify general arrangement of the security system components, backboard size, wire through size and location, and power circuit requirements.
 - 3) Device Mounting Details - Provide mounting detailed drawing for each security device (physical access control system, video surveillance and assessment) for each type of wall and ceiling configuration in project. Device details shall include device, mounting detail, wiring and conduit routing.
 - 4) Details of connections to power supplies and grounding
 - 5) Details of surge protection device installation
 - 6) Sensor detection patterns - Each system sensor shall have associated detection patterns.
 - 7) Equipment Rack Detail - For each equipment rack, provide a scaled detail of the equipment rack location and rack space utilization. Use of BISCII wire management standards shall be

employed to identify wire management methodology. Transitions between equipment racks shall be shown to include use vertical and horizontal latter rack system.

- 10) Equipment Room - Equipment room details shall provide architectural, electrical, mechanical, plumbing, IT/Data and associated equipment and device placements both vertical and horizontally.
- j. Electrical Panel Schedule - Electrical Panel Details shall be provided for all SMS systems electrical power circuits. Panel details shall be provided identifying panel type (Standard, Emergency Power, Emergency/Uninterrupted Power Source, and Uninterrupted Power Source Only), panel location, circuit number, and circuit amperage rating.
- k. Door Schedule - A door schedule shall be developed for each door equipped with electronic security components. At a minimum, the door schedule shall be coordinated with Division 08 work and include the following information:
 - 1) Item Number
 - 2) Door Number (Derived from A/E Drawings)
 - 3) Floor Plan Sheet Number
 - 4) Standard Detail Number
 - 5) Door Description (Derived from Loading Sheets)
 - 6) Data Gathering Panel Input Number
 - 7) Door Position or Monitoring Device Type & Model Number
 - 8) Lock Type, Model Number & Power Input/Draw (standby/active)
 - 9) Card Reader Type & Model Number
 - 10) Shunting Device Type & Model Number
 - 11) Sounder Type & Model Number
 - 12) Manufacturer
 - 13) Misc. devices as required
 - a) Delayed Egress Type & Model Number
 - b) Intercom
 - c) Camera
 - d) Electric Transfer Hinge
 - e) Electric Pass-through device
 - 14) Remarks column indicating special notes or door configurations

2. Camera Schedule - A camera schedule shall be developed for each camera. Contractors shall coordinate with the Contracting Officer's Representative to determine camera starting numbers and naming conventions. All drawings shall identify wire and cable standardization methodology. Color coding of all wiring conductors and jackets is required and shall be communicated consistently throughout the drawings package submittal. At a minimum, the camera schedule shall include the following information:
 - a. Item Number
 - b. Camera Number
 - c. Naming Conventions
 - d. Description of Camera Coverage
 - e. Camera Location
 - f. Floor Plan Sheet Number
 - g. Camera Type
 - h. Mounting Type
 - i. Standard Detail Reference
 - j. Power Input & Draw
 - k. Power Panel Location
 - l. Remarks Column for Camera
3. Section IV - Manufacturers' Data: The data package shall include manufacturers' data for all materials and equipment, including sensors, local processors and console equipment provided under this specification.
4. Section V - System Description and Analysis: The data package shall include system descriptions, analysis, and calculations used in sizing equipment required by these specifications. Descriptions and calculations shall show how the equipment shall operate as a system to meet the performance requirements of this specification. The data package shall include the following:
 - a. Central processor memory size; communication speed and protocol description; rigid disk system size and configuration; flexible disk system size and configuration; back-up media size and configuration; alarm response time calculations; command response time calculations; start-up operations; expansion capability and method of implementation; sample copy of each report specified; and color photographs representative of typical graphics.

- b. Software Data: The data package shall consist of descriptions of the operation and capability of the system, and application software as specified.
 - c. Overall System Reliability Calculations: The data package shall include all manufacturers' reliability data and calculations required to show compliance with the specified reliability.
5. Section VI - Certifications & References: All specified manufacturer's certifications shall be included with the data package. Contractor shall provide Project references as outlined in "Quality Assurance".
- J. Group II Technical Data Package
- 1. The Contractor shall prepare a report of "Current Site Conditions" and submit a report to the Contracting Officer's Representative documenting changes to the site, particularly those conditions that affect performance of the system to be installed. The Contractor shall provide specification sheets, or written functional requirements to support the findings, and a cost estimate to correct those site changes or conditions which affect the installation of the system or its performance. The Contractor shall not correct any deficiency without written permission from the COR.
 - 2. System Configuration and Functionality: The contractor shall provide the results of the meeting with VA to develop system requirements and functionality:
 - a. Baseline configuration
 - b. Access levels
 - c. Schedules (intrusion detection, physical access control, holidays)
 - d. Badge database
 - e. System monitoring and reporting (unit level and central control)
 - f. Naming conventions and descriptors
- K. Group III Technical Data Package
- 1. Development of Test Procedures: The Contractor shall prepare performance test procedures for the system testing. The test procedures shall follow the format of the VA Testing procedures and be customized to the contract requirements. The Contractor shall deliver the test procedures to the Contracting Officer's

Representative for approval at least 60 calendar days prior to the requested test date.

L. Group IV Technical Data Package

1. Performance Verification Test

a. Based on the successful completion of the pre-delivery test, the Contractor shall finalize the test procedures and report forms for the performance verification test (PVT) and the endurance test. The PVT shall follow the format, layout and content of the pre-delivery test. The Contractor shall deliver the PVT and endurance test procedures to the Contracting Officer's Representative for approval. The Contractor shall schedule the PVT after receiving written approval of the test procedures. The Contractor shall deliver the final PVT and endurance test reports within 14 calendar days from completion of the tests. Refer to Part 3 of this section for System Testing and Acceptance requirements.

2. Training Documentation

a. New Facilities and Major Renovations: Familiarization training shall be provided for new equipment or systems. Training can include site familiarization training for VA technicians and administrative personnel. Training shall include general information on new system layout including closet locations, turnover of the completed system including all documentation, including manuals, software, key systems, and full system administration rights. Lesson plans and training manuals training shall be oriented to type of training to be provided.

b. New Unit Control Room:

1) Provide the security personnel with training in the use, operation, and maintenance of the entire control room system (Unit Control and Equipment Rooms). The training documentation shall include the operation and maintenance. The first of the training sessions shall take place prior to system turnover and the second immediately after turnover. Coordinate the training sessions with the Owner. Completed classroom sessions shall be witnessed and documented by the Architect/Engineer, and approved by the Contracting Officer's

Representative. Instruction is not to begin until the system is operational as designed.

- 2) The training documents shall cover the operation and the maintenance manuals and the control console operators' manuals and service manuals in detail, stressing all important operational and service diagnostic information necessary for the maintenance and operations personnel to efficiently use and maintain all systems.
- 3) Provide an illustrated control console operator's manual and service manual. The operator's manual shall be written in laymen's language and printed so as to become a permanent reference document for the operators, describing all control panel switch operations, graphic symbol definitions and all indicating functions and a complete explanation of all software.
- 4) The service manual shall be written in laymen's language and printed so as to become a permanent reference document for maintenance personnel, describing how to run internal self diagnostic software programs, troubleshoot head end hardware and field devices with a complete scenario simulation of all possible system malfunctions and the appropriate corrective measures.
- 5) Provide a professional color DVD instructional recording of all the operational procedures described in the operator's manual. All charts used in the training session shall be clearly presented on the video. Any DVD found to be inferior in recording or material content shall be reproduced at no cost until an acceptable DVD is submitted. Provide four copies of the training DVD, one to the architect/engineer and three to the owner.

3. System Configuration and Data Entry:

- a. The contractor is responsible for providing all system configuration and data entry for the SMS and subsystems (e.g., video matrix switch, intercom, digital video recorders, and network video recorders). All data entry shall be performed per VA standards & guidelines. The Contractor is responsible for participating in all meetings with the client to compile the

information needed for data entry. These meetings shall be established at the beginning of the project and incorporated in to the project schedule as a milestone task. The contractor shall be responsible for all data collection, data entry, and system configuration. The contractor shall collect, enter, & program and/or configure the following components:

- 1) Physical Access control system components,
 - 2) Video surveillance, control and recording systems,
 - 3) All other security subsystems shown in the contract documents.
- b. The Contractor is responsible for compiling the card access database for the VA employees, including programming reader configurations, access shifts, schedules, exceptions, card classes and card enrollment databases.
- c. Refer to Part 3 for system programming requirements and planning guidelines.
4. Graphics: Based on CAD as-built drawings developed for the construction project, create all map sets showing locations of all alarms and field devices. Graphical maps of all alarm points installed under this contract including perimeter and exterior alarm points shall be delivered with the system. The Contractor shall create and install all graphics needed to make the system operational. The Contractor shall utilize data from the contract documents, Contractor's field surveys, and all other pertinent information in the Contractor's possession to complete the graphics. The Contractor shall identify and request from the COR, any additional data needed to provide a complete graphics package. Graphics shall have sufficient level of detail for the system operator to assess the alarm. The Contractor shall supply hard copy, color examples at least 203.2 x 254 mm (8 x 10 in) of each type of graphic to be used for the completed Security system. The graphics examples shall be delivered to the Contracting Officer's Representative for review and approval at least 90 calendar days prior to the scheduled date the Contractor requires them.
- M. Group V Technical Data Package: Final copies of the manuals shall be delivered to the Contracting Officer's Representative as part of the acceptance test. The draft copy used during site testing shall be updated with any changes required prior to final delivery of the

manuals. Each manual's contents shall be identified on the cover. The manual shall include names, addresses, and telephone numbers of each sub-contractor installing equipment or systems, as well as the nearest service representatives for each item of equipment for each system. The manuals shall include a table of contents and tab sheets. Tab sheets shall be placed at the beginning of each chapter or section and at the beginning of each appendix. The final copies delivered after completion of the endurance test shall include all modifications made during installation, checkout, and acceptance. Six (6) hard-copies and one (1) soft copy on CD of each item listed below shall be delivered as a part of final systems acceptance.

1. Functional Design Manual: The functional design manual shall identify the operational requirements for the entire system and explain the theory of operation, design philosophy, and specific functions. A description of hardware and software functions, interfaces, and requirements shall be included for all system operating modes. Manufacturer developed literature shall be used; however, shall be produced to match the project requirements.
2. Equipment Manual: A manual describing all equipment furnished including:
 - a. General description and specifications; installation and checkout procedures; equipment electrical schematics and layout drawings; system schematics and layout drawings; alignment and calibration procedures; manufacturer's repair list indicating sources of supply; and interface definition.
3. Software Manual: The software manual shall describe the functions of all software and include all other information necessary to enable proper loading, testing, and operation. The manual shall include:
 - a. Definition of terms and functions; use of system and applications software; procedures for system initialization, start-up, and shutdown; alarm reports; reports generation, database format and data entry requirements; directory of all disk files; and description of all communications protocols including data formats, command characters, and a sample of each type of data transfer.

4. Operator's Manual: The operator's manual shall fully explain all procedures and instructions for the operation of the system, including:
 - a. Computers and peripherals; system start-up and shutdown procedures; use of system, command, and applications software; recovery and restart procedures; graphic alarm presentation; use of report generator and generation of reports; data entry; operator commands' alarm messages, and printing formats; and system access requirements.
5. Maintenance Manual: The maintenance manual shall include descriptions of maintenance for all equipment including inspection, recommend schedules, periodic preventive maintenance, fault diagnosis, and repair or replacement of defective components.
6. Spare Parts & Components Data: At the conclusion of the Contractor's work, the Contractor shall submit to the Contracting Officer's Representative a complete list of the manufacturer's recommended spare parts and components required to satisfactorily maintain and service the systems, as well as unit pricing for those parts and components.
7. Operation, Maintenance & Service Manuals: The Contractor shall provide two (2) complete sets of operating and maintenance manuals in the form of an instructional manual for use by the VA Security Guard Force personnel. The manuals shall be organized into suitable sets of manageable size. Where possible, assemble instructions for similar equipment into a single binder. If multiple volumes are required, each volume shall be fully indexed and coordinated.
8. Equipment and Systems Maintenance Manual: The Contractor shall provide the following descriptive information for each piece of equipment, operating system, and electronic system:
 - a. Equipment and/or system function.
 - b. Operating characteristics.
 - c. Limiting conditions.
 - d. Performance curves.
 - e. Engineering data and test.
 - f. Complete nomenclature and number of replacement parts.

- g. Provide operating and maintenance instructions including assembly drawings and diagrams required for maintenance and a list of items recommended to stock as spare parts.
 - h. Provide information detailing essential maintenance procedures including the following: routine operations, trouble shooting guide, disassembly, repair and re-assembly, alignment, adjusting, and checking.
 - i. Provide information on equipment and system operating procedures, including the following; start-up procedures, routine and normal operating instructions, regulation and control procedures, instructions on stopping, shut-down and emergency instructions, required sequences for electric and electronic systems, and special operating instructions.
 - j. Manufacturer equipment and systems maintenance manuals are permissible.
9. Project Redlines: During construction, the Contractor shall maintain an up-to-date set of construction redlines detailing current location and configuration of the project components. The redline documents shall be marked with the words 'Master Redlines' on the cover sheet and be maintained by the Contractor in the project office. The Contractor shall provide access to redline documents anytime during the project for review and inspection by the Contracting Officer's Representative or authorized Office of Protection Services representative. Master redlines shall be neatly maintained throughout the project and secured under lock and key in the contractor's onsite project office. Any project component or assembly that is not installed in strict accordance with the drawings shall be so noted on the drawings. Prior to producing Record Construction Documents, the contractor shall submit the Master Redline document to the Contracting Officer's Representative for review and approval of all changes or modifications to the documents. Each sheet shall have Contracting Officer's Representative initials indicating authorization to produce "As Built" documents. Field drawings shall be used for data gathering & field changes. These changes shall be made to the master redline documents daily. Field drawings shall not be considered "master redlines".

10. Record Specifications: The Contractor shall maintain one (1) copy of the Project Specifications, including addenda and modifications issued, for Project Record Documents. The Contractor shall mark the Specifications to indicate the actual installation where the installation varies substantially from that indicated in the Contract Specifications and modifications issued. (Note related Project Record Drawing information where applicable). The Contractor shall pay particular attention to substitutions, selection of product options, and information on concealed installations that shall be difficult to identify or measure and record later. Upon completion of the mark ups, the Contractor shall submit record Specifications to the COR. As with master relines, Contractor shall maintain record specifications for Contracting Officer's Representative review and inspection at anytime.
11. Record Product Data: The Contractor shall maintain one (1) copy of each Product Data submittal for Project Record Document purposes. The Data shall be marked to indicate the actual product installed where the installation varies substantially from that indicated in the Product Data submitted. Significant changes in the product delivered to the site and changes in manufacturer's instructions and recommendations for installation shall be included. Particular attention shall be given to information on concealed products and installations that cannot be readily identified or recorded later. Note related Change Orders and mark up of Record Construction Documents, where applicable. Upon completion of mark up, submit a complete set of Record Product Data to the COR.
12. Miscellaneous Records: The Contractor shall maintain one (1) copy of miscellaneous records for Project Record Document purposes. Refer to other Specifications for miscellaneous record-keeping requirements and submittals concerning various construction activities. Before substantial completion, complete miscellaneous records and place in good order, properly identified and bound or filed, ready for use and reference. Categories of requirements resulting in miscellaneous records include, a minimum of the following:
 - a. Certificates received instead of labels on bulk products.

- b. Testing and qualification of tradesmen. ("Contractor's Qualifications")
 - c. Documented qualification of installation firms.
 - d. Load and performance testing.
 - e. Inspections and certifications.
 - f. Final inspection and correction procedures.
 - g. Project schedule
13. Record Construction Documents (Record As-Built)
- a. Upon project completion, the contractor shall submit the project master redlines to the Contracting Officer's Representative prior to development of Record construction documents. The Contracting Officer's Representative shall be given a minimum of a thirty (30) day review period to determine the adequacy of the master redlines. If the master redlines are found suitable by the Contracting Officer's Representative, the Contracting Officer's Representative shall initial and date each sheet and turn redlines over to the contractor for as built development.
 - b. The Contractor shall provide the Contracting Officer's Representative a complete set of "as-built" drawings and original master redlined marked "as-built" blue-line in the latest version of AutoCAD drawings unlocked on CD or DVD. The as-built drawing shall include security device number, security closet connection location, data gathering panel number, and input or output number as applicable. All corrective notations made by the Contractor shall be legible when submitted to the COR. If, in the opinion of the COR, any redlined notation is not legible, it shall be returned to the Contractor for re-submission at no extra cost to the Owner. The Contractor shall organize the Record Drawing sheets into manageable sets bound with durable paper cover sheets with suitable titles, dates, and other identifications printed on the cover. The submitted as built shall be in editable formats and the ownership of the drawings shall be fully relinquished to the owner.
 - c. Where feasible, the individual or entity that obtained record data, whether the individual or entity is the installer, sub-contractor, or similar entity, is required to prepare the mark up on Record Drawings. Accurately record the information in a

comprehensive drawing technique. Record the data when possible after it has been obtained. For concealed installations, record and check the mark up before concealment. At the time of substantial completion, submit the Record Construction Documents to the COR. The Contractor shall organize into bound and labeled sets for the COR's continued usage. Provide device, conduit, and cable lengths on the conduit drawings. Exact in-field conduit placement/routings shall be shown. All conduits shall be illustrated in their entire length from termination in security closets; no arrowed conduit runs shall be shown. Pull box and junction box sizes shall be shown if larger than 100mm (4 inch).

N. FIPS 201 Compliance Certificates

1. Provide Certificates for all software components and device types utilizing credential verification. Provide certificates for:

- a. Fingerprint Capture Station
- b. Card Readers
- c. Facial Image Capturing Camera
- d. PIV Middleware
- e. Template Matcher
- f. Electromagnetically Opaque Sleeve
- g. Certificate Management
 - 1) CAK Authentication System
 - 2) PIV Authentication System
 - 3) Certificate Validator
 - 4) Cryptographic Module

O. Approvals shall be based on complete submission of manuals together with shop drawings.

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

- 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 shall 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:
 - 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. 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 Electro technical 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
- 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 shall 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 PERFORMANCE REQUIREMENTS

- A. PACS shall provide support for multiple authentication modes and bidirectional communication with the reader. PACS shall provide implementation capability for enterprise security policy and incident response.
- B. All processing of authentication information shall occur on the "safe side" of a door
- C. Physical Access Control System shall provide access to following Security Areas:
 - 1. Controlled
 - 2. Limited
 - 3. Exclusion
- D. PACS shall provide:
 - 1. One authentication factor for access to Controlled security areas
 - 2. Two authentication factors for access to Limited security areas
 - 3. Three authentication factors for access to Exclusion security areas

- E. PACS shall provide Credential Validation and Path Validation per NIST 800-116.
- F. The PACS System shall have an Enterprise Path Validation Module (PVM) component that processes X.509 certification paths composed of X.509 v3 certificates and X.509 v2 CRLs. The PVM component SHALL support the following features:
 - 1. Name chaining;
 - 2. Signature chaining;
 - 3. Certificate validity;
 - 4. Key usage, basic constraints, and certificate policies certificate extensions;
 - 5. Full CRLs; and
 - 6. CRLs segmented on names.
- G. Distributed Processing: System shall be a fully distributed processing system so that information, including time, date, valid codes, access levels, and similar data, is downloaded to Controllers so that each Controller makes access-control decisions for that Location. Do not use intermediate Controllers for physical access control. If communications to Central Station are lost, all Controllers shall automatically buffer event transactions until communications are restored, at which time buffered events shall be uploaded to the Central Station.
- H. Data Capacity:
 - 1. 130 different card-reader formats.
 - 2. 999 comments.
 - 3. 16 graphic file types for importing maps.
- I. Location Capacity:
 - 1. 128 reader-controlled doors.
 - 2. 50,000 total access credentials.
 - 3. 2048 supervised alarm inputs.
 - 4. 2048 programmable outputs.
 - 5. 32,000 custom action messages per Location to instruct operator on action required when alarm is received.
- J. System Network Requirements:
 - 1. Interconnect system components and provide automatic communication of status changes, commands, field-initiated interrupts, and other communications required for proper system operation.

2. Communication shall not require operator initiation or response, and shall return to normal after partial or total network interruption such as power loss or transient upset.
 3. System shall automatically annunciate communication failures to the operator and identify the communication link that has experienced a partial or total failure.
 4. Communications Controller shall be used as an interface between the Central Station display systems and the field device network.
Communications Controller shall provide functions required to attain the specified network communications performance.
- K. Central Station shall provide operator interface, interaction, display, control, and dynamic and real-time monitoring. Central Station shall control system networks to interconnect all system components, including workstations and field-installed Controllers.
- L. Field equipment shall include Controllers, sensors, and controls. Controllers shall serve as an interface between the Central Station and sensors and controls. Data exchange between the Central Station and the Controllers shall include down-line transmission of commands, software, and databases to Controllers. The up-line data exchange from the Controller to the Central Station shall include status data such as intrusion alarms, status reports, and entry-control records. Controllers are classified as alarm-annunciation or entry-control type.
- M. System Response to Alarms: Field device network shall provide a system end-to-end response time of 1second(s) or less for every device connected to the system. Alarms shall be annunciated at the Central Station within 1 second of the alarm occurring at a Controller or device controlled by a local Controller, and within 100 ms if the alarm occurs at the Central Station. Alarm and status changes shall be displayed within 100 ms after receipt of data by the Central Station. All graphics shall be displayed, including graphics-generated map displays, on the console monitor within 5 seconds of alarm receipt at the security console.
- N. False Alarm Reduction: The design of Central Station and Controllers shall contain features to reduce false alarms. Equipment and software shall comply with SIA CP-01.
- O. Error Detection: A cyclic code error detection method shall be used between Controllers and the Central Station, which shall detect single-

and double-bit errors, burst errors of eight bits or less, and at least 99 percent of all other multibit and burst error conditions.

Interactive or product error detection codes alone shall not be acceptable. A message shall be in error if one bit is received incorrectly. System shall retransmit messages with detected errors. A two-digit decimal number shall be operator assignable to each communication link representing the number of retransmission attempts. When the number of consecutive retransmission attempts equals the assigned quantity, the Central Station shall print a communication failure alarm message. System shall monitor the frequency of data transmission failure for display and logging.

- P. Data Line Supervision: System shall initiate an alarm in response to opening, closing, shorting, or grounding of data transmission lines.
- Q. Door Hardware Interface: Coordinate with Division 08 Sections that specify door hardware required to be monitored or controlled by the PACS. The Controllers in this Section shall have electrical characteristics that match the signal and power requirements of door hardware. Integrate door hardware specified in Division 08 Sections to function with the controls and PC-based software and hardware in this Section.
- R. References to industry and trade association standards and codes are minimum installation requirement standards.
- S. Drawings and other specification sections shall govern in those instances where requirements are greater than those specified in the above standards.

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 Contracting Officer's Representative 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 Contracting Officer's Representative 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. All equipment and materials for the system shall 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 shall 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's Representative shall approve the acceptance of prior to an installation.
- C. PACS equipment shall meet or exceed all requirements listed below.
- D. A PACS shall be comprised of the following components:
 - 1. Physical Access Control System
 - 2. Application Software
 - 3. System Database
 - 4. Surge and Tamper Protection
 - 5. Controllers (Data Gathering Panel)
 - 6. Keypads
 - 7. Card Readers
 - 8. System Sensors and Related Equipment
 - 9. Push Button Switches
 - 10. Interfaces
 - 11. Door and Gate Hardware interface
 - 12. RS-232 ASCII Interface
 - 13. Floor Select Elevator Control
 - 14. Video and Camera Control
 - 15. Cables
 - 16. Transformers

2.2 SECURITY MANAGEMENT SYSTEM (SMS)) EXISTING JOHNSON CONTROL

2.3 APPLICATION SOFTWARE EXISTING

2.4 SURGE AND TAMPER PROTECTION

- A. Surge Protection: Protect components from voltage surges originating external to equipment housing and entering through power, communication, signal, control, or sensing leads. Include surge protection for external wiring of each conductor-entry connection to components.

1. Minimum Protection for Power Connections 120 V and More: Auxiliary panel suppressors complying with requirements in Division 26 Section "Low-Voltage Electrical Power Conductors and Cables."
 2. Minimum Protection for Communication, Signal, Control, and Low-Voltage Power Connections: Comply with requirements in Division 26 Section "Low-Voltage Electrical Power Conductors and Cables" as recommended by manufacturer for type of line being protected.
- B. Tamper Protection: Tamper switches on enclosures, control units, pull boxes, junction boxes, cabinets, and other system components shall initiate a tamper-alarm signal when unit is opened or partially disassembled. Control-station control-unit alarm display shall identify tamper alarms and indicate locations.

2.5 PACS SERVER HARDWARE

- A. SMS server computer is an existing Johnson Control system.

2.6 STANDARD WORKSTATION HARDWARE

- A. Workstation is existing Johnson Control PACS system.

2.7 REMOTE DOOR CONTROLLERS

- A. 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.
- B. Subject to compliance with requirements in this Article, manufacturers shall use multipurpose Controllers.
- C. Battery Backup: Sealed, lead acid; sized to provide run time during a power outage of 90 minutes, complying with UL 924.
- D. Alarm Annunciation Controller:
1. The Controller shall automatically restore communication within 10 seconds after an interruption with the field device network with dc line supervision on each of its alarm inputs.
 - a. Inputs: Monitor dry contacts for changes of state that reflect alarm conditions. Provides at least eight alarm inputs, which are suitable for wiring as normally open or normally closed contacts for alarm conditions.
 - b. Alarm-Line Supervision:
 - 1) Supervise the alarm lines by monitoring each circuit for changes or disturbances in the signal, and for conditions as described in UL 1076 for line security equipment by monitoring

for abnormal open, grounded, or shorted conditions using dc change measurements. System shall initiate an alarm in response to an abnormal current, which is a dc change of 5 percent or more for longer than 500 ms.

2) Transmit alarm-line-supervision alarm to the Central Station during the next interrogation cycle after the abnormal current condition.

c. Outputs: Managed by Central Station software.

d. Controller shall have Ethernet port for IP connection.

2. Auxiliary Equipment Power: A GFI service outlet inside the Controller enclosure.

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, biometric personal identity verification devices, door strikes, magnetic latches, gate and 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. (Shall have Ethernet port for IP connection)

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 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 alarm sounds.
4. With power supplies sufficient to power at voltage and frequency required for field devices and portal-control devices.
5. Data Line Problems: For periods of loss of communications with Central Station, or when data transmission is degraded and generating continuous checksum errors, the Controller shall continue to control entry by accepting identifying information, making authentication decisions, checking privileges, and controlling portal-control devices.
 - a. Store up to 1000 transactions during periods of communication loss between the Controller and access-control devices for subsequent upload to the Central Station on restoration of communication.
6. Controller Power: NFPA 70, Class II power supply transformer, with 12- or 24-V ac secondary, backup battery and charger.
 - a. Backup Battery: Premium, valve-regulated, recombinant-sealed, lead-calcium battery; spill proof; with a full 1-year warranty and a pro rata 19-year warranty. With single-stage, constant-voltage-current, limited battery charger, comply with battery manufacturer's written instructions for battery terminal voltage and charging current recommendations for maximum battery life.
 - b. Backup Battery: Valve-regulated, recombinant-sealed, lead-acid battery; spill proof. With single-stage, constant-voltage-current, limited battery charger, comply with battery

- manufacturer's written instructions for battery terminal voltage and charging current recommendations for maximum battery life.
- c. Backup Power Supply Capacity: 5 minutes of battery supply.
Submit battery and charger calculations.
 - d. Power Monitoring: Provide manual dynamic battery load test, initiated and monitored at the control center; with automatic disconnection of the Controller when battery voltage drops below Controller limits. Report by using local Controller-mounted LEDs and by communicating status to Central Station. Indicate normal power on and battery charger on trickle charge. Indicate and report the following:
 - 1) Trouble Alarm: Normal power off load assumed by battery.
 - 2) Trouble Alarm: Low battery.
 - 3) Alarm: Power off.

2.8 PIV MIDDLEWARE

- A. PIV Middleware shall provide three-factor authentication, including biometric matching using a fingerprint capture device capable of single fingerprint capture. Unit shall enable digital certificates can to be verified by security personnel using the issuer's certificate authority, SCVP, OCSP responder/repeater, or the TSA hot list for TWIC cardholders. All cards shall be validated using FIPS-201 challenge-response protocol in order to identify forged or cloned cards. PIV Middleware solution shall validate all PIV, TWIC, NG CAC, and FRAC cards. TWIC card FASC-Ns shall also be verified against a live or cached TSA hot list.
- B. PIV Middleware shall have ability to:
 - 1. Verify cardholder identity and validates FIPS 201-compliant PIV-II, next-generation (NG) CAC, TWIC, or FRAC credentials in real-time
 - 2. Perform three-factor authentication of cardholder using PIN, biometrics, and certificate (or serial numbers) detecting forged or cloned cards
 - 3. Enroll FASC-N, photo, and pertinent cardholder information into PACS software
 - 4. Automatically suspend a cardholder's badge if his or her PIV, TWIC, or CAC card certificate serial number is on the Certificate Revocation List (CRL)

5. Upload a cardholder transaction audit trail to central database or exports it to a .csv file for centralized transaction management
 6. Be compatible with biometric mobile terminal for off-site verification and enrollment
 7. Re-validate imported cardholder certificates on a periodic basis via the Internet
 8. Operate with commercial, off-the-shelf (COTS) FIPS 201 PIV-II and ANSI INCITS 378-compliant fingerprint capture devices
 9. Revalidate imported cardholder certificates at regular intervals, ensuring that the credentials used in PACS system are backed by a valid set of digital certificates. Digital certificates are verified against local OCSP repeater/validation authority using the issuer's validation authority, or Microsoft Crypto Application Programming Interface (API) on Windows XP SP3 or Vista.
 10. Certificate Manager shall fully support SCVP and OCSP for fast, online validation.
 11. Provide verification of TWIC credentials against a live TSA hot list.
 12. Support uploading local transactions to a central database for consolidated activity reporting. This application shall support a variety of ODBC- or ADO-compliant databases, including Oracle, SQL Server 2005, Informix, DB2, and Firebird.
 13. Provide user with ability to produce canned transaction log queries as well as creating queries directly from the SQL database.
- C. PIV Middleware PC requirements:
1. PIV Middleware software shall operate on Intel-based PC with minimum 1.8 GHz CPU, 1 GB RAM, 40 GB hard disk, and Microsoft Windows XP SP2 with Microsoft .NET Framework 2.0
 2. Unit shall fingerprint capture devices and smart card reader.
- D. PIV Middleware shall be FIPS 201 approved product.

2.9 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 800ms 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. Shall 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 shall encompass a wide functional range. The PACS shall 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). 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 shall 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 shall contain a buffer large enough to receive the maximum size frame permitted by International Organization for Standardization International Electro technical 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 time¹ 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 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.

1. Readability Range: The reader shall not be able to read PIV card more than 10cm(4inch) from the reader.
- T. Card readers shall be HID 6125CKN0009-G3.0 RDR, RP40, MULTICLASS, PIV II, 64 Bite Reverse BCD to match existing system.

2.10 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. 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.

2.11 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.

C. 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 shall 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. 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. 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.

D. Key Bypass:

1. Shall be utilized for all doors that have a mortise or rim mounted door hardware.
2. Each door shall be individually keyed with one master key per secured area.
3. Cylinders shall be six (6)-pin and made of brass or equivalent. Keys for the cylinders shall be constructed of solid material and produced and cut by the same distributor. Keys shall not be purchased, cut, and supplied by multiple dealers.
4. All keys shall have a serial number cut into the key. No two serial numbers shall be the same.
5. All keys and cylinders shall be stored in a secure area that is monitored by the Intrusion Detection System.

E. 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 shall 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. Shall 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.
- F. 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).

2.12 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 A at 120 V ac or 5 A at 240-V ac.
 - b. Contacts that shall make 720 VA at 60 A and that shall break at 720 VA at 10 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.
 - b. Indoors, uncontrolled environment.
 - c. Outdoors.
 - 4. Power: Push-button switches shall be powered from their associated Controller, using dc control.

2.13 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.

F. Push-Button Switches:

1. Shall be momentary contact, back lighted push buttons, and stainless steel switch enclosures for each push button as shown. Buttons shall be utilized for secondary means of releasing a locking mechanism.
 - a. In an area where a push button is being utilized for remote access of the locking device then no more than two (2) buttons shall operate one door from within one secure space. Buttons shall not be wired in series with one other.
 - b. In an area where locally stationed guards control entry to multiple secure points via remote switches. An interface board shall be designed and constructed for only the amount of buttons it shall house. These buttons shall be flush mounted and clearly labeled for ease of use. All buttons shall be connected to the PACS and SMS system for monitoring purposes.
 - c. Shall have double-break silver contacts that shall make 720 VA at 60 amperes and break 720 VA at 10 amperes.

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 shall indicate to the system if the strike/bolt is not engaged or is unlocked when it shall 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 new doors receiving physical access control devices.
 - b. Provide integration of the Electric Mortise Locks with the PACS for:
 - 1) Lock Power
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)

8. Turnstiles:
- a. Shall operate at 110 VAC, 60 Hz or 220 VAC, 50 Hz supplied from a dedicated circuit breaker on a security power panel. This device does not require a back-up power source.

- b. Shall be utilized as a means of monitoring and controlling access in a lobby.
- c. Shall meet the following minimum requirements:
 - 1) Be UFAS compliant.
 - 2) Provide either an audible or visual confirmation that access has been granted to a cleared individual.
 - 3) Provide an audible alarm in the event a non-cleared individual is attempting to gain access.
 - 4) Interface with the SMS and utilize a card reader for accessing and exiting a facility, and provide a recorded event of personnel accessing these points.
 - 5) Have a built-in step-down transformer to provide power to a card reader unit.
 - 6) Have built-in signal wiring chassis to allow for plug and play capabilities with the PACS.
 - 7) Have the ability to detect tailgating within one quarter on an inch to prevent unauthorized access to a facility.
- 9. Vehicle Gate Operator: Interface electrical operation of gate with controls of this Section. Vehicle gate operators shall be connected, monitored, and controlled, by the security access Controllers.

2.14 INTERFACES

A. CCTV System Interface

- 1. An RS232 and/or Ethernet interface associated driver, and controller shall be provided for connection of the SMS Central Computer to the CCTV Alarm interface and switcher. The interface shall provide alarm data to the CCTV Alarm interface for automatic camera call-up. If required the Security Contractor shall be responsible for programming the command strings into the SMS Server.

B. Intercom System Interface

- 1. The CCTV call-up from intercom stations shall be through the intercom unit via Ethernet communications interface to the SMS system, then through the matrix switcher.
 - a. Application Software
 - 1) Provides the interface between the Alarm Annunciation System and Operator; all sensors, local processors and data links, drive displays, report alarms, and report generation.

- 2) Software is categorized as System Software and Application Software. System Software shall consist of software to support set-up, operation, hard drive back-ups and maintenance processor. Application Software shall consist of software to provide the completion of Physical Access Control System.

C. Power Supplies:

1. Shall be UL rated and able to adequately power (enter number) entry control devices on a continuous base without failure.
2. Shall meet the following minimum technical characteristics:

INPUT POWER	110 VAC 60 HZ (enter amperage)A
OUTPUT VOLTAGE	12 VDC Nominal (13.8 VDC) 24 VDC Nominal (27.6 VDC) Filtered and Regulated
BATTERY	Dependant on Output Voltage shall provide up to 200 Ah
OUTPUT CURRENT	10 amp max. @ 13.8 VDC 5 amp max. @ 27.6 VDC
PRIMARY FUSE SIZE	6.3 amp (non-removable)
BATTERY FUSE SIZE	12 amp, 3AG
CHARGING CIRCUIT	Built-in standard

2.15 FLOOR SELECT ELEVATOR CONTROL

- A. Elevator access control shall be integral to security access.
1. System shall be capable of providing full elevator security and control through dedicated Controllers without relying on the control-station host PC for elevator control decisions.
 2. Access-control system shall enable and disable car calls on each floor and floor select buttons in each elevator car, restricting passengers' access to the floors where they have been given access.
 3. System setup shall, through programming, automatically secure and unsecure each floor select button of a car individually by time and day. Each floor select button within a car shall be separately controlled so that some floors shall be secure while others remain unsecure.
 4. When a floor select button is secure, it shall require the passenger to use his/her access code and have access to that floor before the

floor select button shall operate. The passenger's credential shall determine which car call and floor select buttons shall be enabled, restricting access to floors unless authorized by system's access code database. Floor select button shall be enabled only in the car where the credential holder is the passenger.

- B. PACS shall record which call button is pressed, along with credential and time information.
 - 1. System Controller shall record elevator access data.
 - 2. The Controller shall reset all additional call buttons that shall have been enabled by the user's credential.
 - 3. The floor select elevator control shall allow for manual override either individually by floor or by cab as a group from a workstation PC.

2.16 VIDEO AND CAMERA CONTROL

- A. Control station or designated workstation displays live video from a CCTV source.
 - 1. Control Buttons: On the display window, with separate control buttons to represent Left, Right, Up, Down, Zoom In, Zoom Out, Scan, and a minimum of two custom command auxiliary controls.
 - 2. Provide at least seven icons to represent different types of cameras, with ability to import custom icons. Provide option for display of icons on graphic maps to represent their physical location.
 - 3. Provide the alarm-handling window with a command button that shall display the camera associated with the alarm point.
- B. Display mouse-selectable icons representing each camera source, to select source to be displayed. For CCTV sources that are connected to a video switcher, control station shall automatically send control commands through a COM port to display the requested camera when the camera icon is selected.
- C. Allow cameras with preset positioning to be defined by displaying a different icon for each of the presets. Provide control with Next and Previous buttons to allow operator to cycle quickly through the preset positions.

2.17 WIRES AND CABLES

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

- B. PVC-Jacketed, RS-232 Cable: Paired, 2 pairs, No. 22 AWG, stranded (7x30) tinned copper conductors, polypropylene insulation, and individual aluminum foil-polyester tape shielded pairs with 100 percent shield coverage; PVC jacket. Pairs are cabled on common axis with No. 24 AWG, stranded (7x32) tinned copper drain wire.
1. NFPA 70, Type CM.
 2. Flame Resistance: UL 1581 Vertical Tray.
- 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. PVC-Jacketed, RS-485 Cable: Paired, 2 pairs, twisted, No. 22 AWG, stranded (7x30) tinned copper conductors, PVC insulation, unshielded, PVC jacket, and NFPA 70, Type CMG.
- 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.
- H. Paired Readers and Wiegand Keypads Cables: Paired, 3 pairs, twisted, No. 22 AWG, stranded (7x30) tinned copper conductors, polypropylene insulation, individual aluminum foil-polyester tape shielded pairs each with No. 22 AWG, stranded tinned copper drain wire, 100 percent shield coverage, and PVC jacket.

1. NFPA 70, Type CM.
 2. Flame Resistance: UL 1581 Vertical Tray.
- I. Paired Readers and Wiegand Keypads Cable: Paired, 3 pairs, twisted, No. 20 AWG, stranded (7x28) tinned copper conductors, polyethylene (polyolefin) insulation, individual aluminum foil-polyester tape shielded pairs each with No. 22 AWG, stranded (19x34) tinned copper drain wire, 100 percent shield coverage, and PVC jacket.
1. NFPA 70, Type CM.
 2. Flame Resistance: UL 1581 Vertical Tray.
- J. 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.
- K. 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.
- L. Paired Lock Cable: 1 pair, twisted, No. 16 AWG, stranded (19x29) tinned copper conductors, PVC insulation, unshielded, and PVC jacket.
1. NFPA 70, Type CMG.
 2. Flame Resistance: UL 1581 Vertical Tray.
- 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.
- N. Paired Lock Cable: 1 pair, twisted, No. 18 AWG, stranded (19x30) tinned copper conductors, PVC insulation, unshielded, and PVC jacket.
1. NFPA 70, Type CMG.
 2. Flame Resistance: UL 1581 Vertical Tray.

- O. 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.
- P. Paired Input Cable: 1 pair, twisted, No. 22 AWG, stranded (7x30) tinned copper conductors, polypropylene insulation, overall aluminum foil-polyester tape shield with No. 22 AWG, stranded (7x30) tinned copper drain wire, 100 percent shield coverage, and PVC jacket.
1. NFPA 70, Type CMR.
 2. Flame Resistance: UL 1666 Riser 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.
- R. Paired AC Transformer Cable: 1 pair, twisted, No. 18 AWG, stranded (7x26) tinned copper conductors, PVC insulation, unshielded, and PVC jacket.
1. NFPA 70, Type CMG.
- S. 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.
- T. Elevator Travel Cable: Steel center core, with shielded, twisted pairs, No. 20 AWG conductor size.
1. Steel Center Core Support: Preformed, flexible, low-torsion, zinc-coated, steel wire rope; insulated with 60 deg C flame-resistant PVC and covered with a nylon or cotton braid.
 2. Shielded Pairs: Insulated copper conductors; color-coded, insulated with 60 deg C flame-resistant PVC; each pair shielded with bare copper braid for 85 percent coverage.
 3. Jute Filler: Electrical grade, dry.
 4. Binder: Helically wound synthetic fiber.
 5. Braid: Rayon or cotton braid applied with 95 percent coverage.

6. Jacket: 60 deg C PVC specifically compounded for flexibility and abrasion resistance. UL VW-1 and CSA FT1 flame rated.

U. 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, 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 shall 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."
- 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 shall 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 5E rating of components and that ensure Category 5E 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 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).

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 shall be designed, engineered, installed, and tested to ensure all components are fully compatible as a system and can be integrated with all associated security subsystems, whether the system is a stand alone or a network.
- E. For integration purposes, the PACS shall be integrated where appropriate with the following associated security subsystems:
 - 1. CCTV:
 - a. Provide 24 hour coverage of all entry points to the perimeter and agency buildings. As well as all emergency exits utilizing a fixed color camera.
 - b. Be able to monitor, control and record cameras on a 24 hours basis.
 - c. Be programmed automatically call up a camera when an access point is but into an alarm state.
 - d. For additional PACS system requirements as they relate to the CCTV, refer to Section 28 23 00, VIDEO SURVEILLANCE.
 - 3. Security Access Detection:
 - a. Be able to monitor all objects that have been screened with an x-ray machine and be able to monitor all data acquired by the bomb detection unit.
 - 4. EPPS:
 - a. Be programmed to go into an alarm state when an emergency call box or duress alarm/panic device is activated, and notify the Physical Access Control System and Database Management of an alarm event.
- F. Integration with these security subsystems shall be achieved by computer programming or the direct hardwiring of the systems.
- G. For programming purposes refer to the manufacturers requirements for correct system operations. Ensure computers being utilized for system integration meet or exceed the minimum system requirements outlined on the systems software packages.
- H. 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 shall affect performance of the system. The Contractor shall not take any corrective action without written permission from the Government.

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 shall affect performance of the system to the Contracting Officer's Representative in the form of a report. The Contractor shall not take any corrective action without written permission received from the Contracting Officer's Representative.

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 shall be reused with Contracting Officer's Representative 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's Representative 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's Representative 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 COR 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 COR 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 shall comply with VA Master Specification 07 84 00, Fire stopping. 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.
- L. 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.
- 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.
- N. 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.
- 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.
- P. 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.

Q. 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).

R. 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.

S. 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 shall observe startup and contractor testing of selected equipment. Coordinate the startup and contractor testing schedules with the Contracting Officer's Representative and Commissioning Agent. Provide a minimum of 7 days prior notice.

T. 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's Representative.
2. The Contractor shall 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.
- B. Testing Agency: Engage a qualified testing and inspecting agency to perform field tests and inspections and prepare test reports:
- C. 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 6 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 shall comply with minimum criteria in TIA/EIA-568-B.
2. Test each circuit and component of each system. Tests shall include 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.

3.11 PROTECTION

- A. Maintain strict security during the installation of equipment and software. Rooms housing the control station, and workstations that have been powered up shall be locked and secured, with an activated burglar alarm and access-control system reporting to a Central Station complying with UL 1610, "Central-Station Burglar-Alarm Units," during periods when a qualified operator in the employ of Contractor is not present.

3.12 DEMONSTRATION AND TRAINING

- A. Provide services of manufacturer's technical representative for four clock hours to instruct VA personnel in operation and maintenance of units.
- B. Submit training plans and instructor qualifications to the COR.
- 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.

Milwaukee VAMC
Parking Structure Lot 7
Milwaukee, WI 53295

April 29, 2015
Bid Set - Amendment 1
Project No. 695-325

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-----