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 expansion and modification consisting of a operating system and application software update, 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.
   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. Monitoring of field-installed devices.
   i. Interface with fire alarm and video surveillance systems.
   j. Reporting.
2. Security:
   a. Video and camera control.

C. System Architecture:

1. Criticality, operational requirements, and/or limiting points of failure may dictate the development of an enterprise and regional server architecture as opposed to system capacity.

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

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

1. Field installed controllers.
2. PIV Middelware.
3. Card readers.
4. PIV cards.
5. Supportive information system.

6. Door locks and sensors.
7. Power supplies.
8. Interfaces with:
    a. Video Surveillance and Assessment System.
    b. Automatic door operators.
    c. Intrusion Detection System.
    d. Fire Protection System.
    e. HVAC.

F. 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).

G. 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.

H. For locations where secure side processing is not applicable the tamper switches and certified cryptographic processing shall be provided per FIPS-140-2.

I. System Software: Based on Tyco CCure 9000 series central-station, workstation operating system, server operating system, and application software.

J. Software and controllers shall be capable of matching full 56 bit FASC-N plus minimum of 32 bits of public key certificate data.

K. Systems Networks:
    1. A standalone system network shall interconnect all components of the system.

1.2 RELATED WORK

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

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

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

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

E. Section 26 05 11 - REQUIREMENTS FOR ELECTRICAL INSTALLATIONS. Requirements for connection of high voltage.

F. Section 26 05 19 - LOW VOLTAGE ELECTRICAL POWER CONDUCTORS AND CABLES. Requirements for power cables.

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

H. 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.

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

J. Section 27 05 26 - GROUNDING AND BONDING FOR COMMUNICATIONS SYSTEMS. Requirements for grounding of equipment.

K. Section 27 05 33 - RACEWAYS AND BOXES FOR COMMUNICATIONS SYSTEMS. Requirements for infrastructure.

L. Section 28 08 00 - COMMISIONING OF ELECTRONIC SAFETY AND SECURITY SYSTEMS. For requirements for commissioning, systems readiness checklists, and training.

M. Section 28 16 00 - INTRUSION DETECTION SYSTEM (IDS). Requirements for alarm systems.

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

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

1.3 QUALITY ASSURANCE

A. Refer to 28 05 00 COMMON WORK RESULTS FOR ELECTRONIC SAFETY AND SECURITY, Part 1.

1.4 SUBMITTALS

A. Refer to 28 05 00 COMMON WORK RESULTS FOR ELECTRONIC SAFETY AND SECURITY, Part 1.

1.5 APPLICABLE PUBLICATIONS

A. Refer to 28 05 00 COMMON WORK RESULTS FOR ELECTRONIC SAFETY AND SECURITY, Part 1.

1.6 DEFINITIONS

A. Refer to 28 05 00 COMMON WORK RESULTS FOR ELECTRONIC SAFETY AND SECURITY, Part 1.

1.7 COORDINATION

A. Refer to 28 05 00 COMMON WORK RESULTS FOR ELECTRONIC SAFETY AND SECURITY, Part 1.

1.8 MAINTENANCE & SERVICE

A. Refer to 28 05 00 COMMON WORK RESULTS FOR ELECTRONIC SAFETY AND SECURITY, Part 1.

1.9 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 must 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. 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.

F. System Response to Alarms: Field device network shall provide a system end-to-end response time of 1 second(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. This response time shall be maintained during system heavy load.

G. 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.

H. References to industry and trade association standards and codes are minimum installation requirement standards.

I. Drawings and other specification sections shall govern in those instances where requirements are greater than those specified in the above standards.

1.10 EQUIPMENT AND MATERIALS

A. Refer to 28 05 00 COMMON WORK RESULTS FOR ELECTRONIC SAFETY AND SECURITY, Part 1.

1.11 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.

1.12 GENERAL REQUIREMENTS

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

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 will be compatible to ensure correct operation as outlined in FIPS 201, March 2006 and HSPD-12.

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

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

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

1. Physical Access Control System,
2. Surge and Tamper Protection,
3. Controllers (Data Gathering Panel),
4. Keypads,
5. Card Readers,
6. Credential Cards,
7. System Sensors and Related Equipment,
8. Push Button Switches,
9. Interfaces,
10. Door and Gate Hardware interface,
11. RS-232 ASCII Interface,
12. Video and Camera Control,
13. Cables,
14. Transformers.

2.2 SECURITY MANAGEMENT SYSTEM (SMS): - NOT USED

2.3 APPLICATION SOFTWARE: - NOT USED

2.4 SURGE AND TAMPER PROTECTION

A. Refer to 28 05 00 COMMON WORK RESULTS FOR ELECTRONIC SAFETY AND SECURITY.

2.5 PACS SERVER HARDWARE: - NOT USED

2.6 STANDARD WORKSTATION HARDWARE: - NOT USED

2.7 COMMUNICATIONS WORKSTATION: - NOT USED

2.8 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 may 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 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.
   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, door strikes, magnetic latches, door operators, and exit push-buttons.
      a. Operate as a stand-alone portal Controller using the downloaded database during periods of communication loss between the Controller and the field-device network.
      b. Accept information generated by the entry-control devices; automatically process this information to determine valid identification of the individual present at the portal:
         1) On authentication of the credentials or information presented, check privileges of the identified individual, allowing only those actions granted as privileges.
         2) Privileges shall include, but not be limited to, time of day control, day of week control, group control, and visitor escort control.

c. Maintain a date-, time-, and Location-stamped record of each transaction. A transaction is defined as any successful or unsuccessful attempt to gain access through a controlled portal by the presentation of credentials or other identifying information.

2. Inputs:
   a. Data from entry-control devices; use this input to change modes between access and secure.
   b. Database downloads and updates from the Central Station that include enrollment and privilege information.
3. Outputs:
   a. Indicate success or failure of attempts to use entry-control devices and make comparisons of presented information with stored identification information.
   b. Grant or deny entry by sending control signals to portal-control devices and mask intrusion alarm annunciation from sensors stimulated by authorized entries.
   c. Maintain a date-, time-, and Location-stamped record of each transaction and transmit transaction records to the Central Station.
   d. Door Prop Alarm: If a portal is held open for longer than 20 seconds, 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 Power Supply Capacity: 5 minutes of battery supply. Submit battery and charger calculations.

c. 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.

2.9 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 to be verified by security personnel using the issuer's certificate authority, SCVP, OCSP responder/repeater, orthe 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.

2.10 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. Will be fully programmable and addressable, locally, and remotely, and hardwired to the system.
G. Shall be individually home run to the main panel.
H. Shall be installed in a manner that they comply with:
   1. The Uniform Federal Accessibility Standards (UFAS),
   2. The Americans with Disabilities Act (ADA,),
   3. The ADA Standards for Accessible Design.
I. Shall support a variety of card readers that must encompass a wide functional range. The PACS may combine any of the card readers described below for installations requiring multiple types of card reader capability (i.e., card only, card and/or PIN, supervised inputs, etc.). These card readers shall be available in the approved technology to meet FIPS 201, and is ISO 14443 A or B, ISO/IEC 7816 compliant. The reader output can be Wiegand, RS-22, 485 or TCP/IP.
J. Shall be housed in an aluminum bezel with a wide lead-in for easy card entry.
K. Shall contain read head electronics, and a sender to encode digital door control signals.
L. LED’s shall be utilized to indicate card reader status and access status.

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

N. Shall provide audible feedback to indicate access granted/denied decisions. Upon a card swipe, two audible tones or beeps shall indicate access granted and three tones or beeps shall indicate access denied. All keypad buttons shall provide tactile audible feedback.

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

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

   1. Entry control keypads shall use a unique combination of alphanumeric and other symbols as an identifier. Keypads shall contain an integral alphanumeric/special symbols keyboard with symbols arranged in ascending ASCII code ordinal sequence. Communications protocol shall be compatible with the local processor.

Q. Shall include a Light Emitting Diode (LED) or other type of visual indicator display and provide visual or visual and audible status indications and user prompts. The display shall indicate power on/off, and whether user passage requests have been accepted or rejected. The design of the keypad display or keypad enclosure shall limit the maximum horizontal and vertical viewing angles of the keypad. The maximum horizontal viewing angle shall be plus and minus five (5) degrees or less off a vertical plane perpendicular to the plane of the face of the keypad display. The maximum vertical viewing angle shall be plus and minus 15 degrees or less off a horizontal plane perpendicular to the plane of the face of the keypad display.

   1. Shall respond to passage requests by generating a signal to the local processor. The response time shall be 800 milliseconds or less from the time the last alphanumeric symbol is entered until a response signal is generated.
   2. Shall be powered from the source as designed and shall not dissipate more than 150 Watts.
   3. Shall be suitable for surface, semi-flush, pedestal, or weatherproof mounting as required.
   4. Shall provide a means for users to indicate a duress situation by entering a special code.

R. Contactless Smart Cards and Readers:

1. Smart card readers shall read credential cards whose characteristics of size and technology meet those defined by ISO/IEC 7816, 14443, 15693.
2. The readers shall have "flash" download capability to accommodate card format changes.
3. The card reader shall have the capability of reading the card data and transmitting the data to the main monitoring panel.
4. The card reader shall be contactless and meet or exceed the following technical characteristics:
   a. Data Output Formats: FIPS 201 low outputs the FASC-N in an assortment of Wiegand bit formats from 40 – 200 bits. FIPS 201 medium outputs a combination FASC-N and HMAC in an assortment of Wiegand bit formats from 32 – 232 bits. All Wiegand formats or the upgradeability from Low to Medium Levels can be field configured with the use of a command card.
   b. FIPS 201 readers shall be able to read, but not be limited to, DESfire and iCLASS cards.
   c. Reader range shall comply with ISO standards 7816, 14443, and 15693, and also take into consideration conditions, are at a minimum 1” to 2” (2.5 – 5 cm).
   d. APDU Support: At a minimum, the contactless interface shall support all card commands for contactless based access specified in Section 7, End-point PIV Card Application Card Command Interface of SP 800-73-1, Interfaces for Personal Identity Verification.
   e. Buffer Size: The reader shall contain a buffer large enough to receive the maximum size frame permitted by ISO/IEC 7816-3, Section 9.4.
   f. ISO 14443 Support: The PIV Reader shall support parts (1 through 4) of ISO/IEC 14443 as amended in the References of this publication.
   g. Type A and B Communication Signal Interfaces: The contactless interface of the reader shall support both the Type A and Type B communication signal interfaces as defined in ISO/IEC 14443-2:2001.
   h. Type A and B Initialization and Anti-Collision The contactless interface of the reader shall support both Type A and Type B

initialization and anti-collision methods as defined in ISO/IEC 14443-3:2001.

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

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

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

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

2.11 BIOMETRIC IDENTITY VERIFICATION EQUIPMENT: - NOT USED

2.11 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 sequencer random scrambled order as required by the campus standard. 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.

2.12 CREDENTIAL CARDS

A. Personal Identity Verification (PIV) credential cards shall comply to Federal Information Processing Standards Publication (FIPS) 201.

B. Visual Card Topography shall be compliant with NIST 800-104.

C. PIV logical credentials shall contain multiple data elements for the purpose of verifying the cardholder's identity at graduated assurance levels. These mandatory data elements shall collectively comprise the data model for PIV logical credentials, and include the following:

1. CHUID
2. PIN
3. PIV authentication data (one asymmetric key pair and corresponding certificate)
4. + Two biometric fingerprints.

D. The credential card (PIV) shall be an ISO 14443 type smart card with contactless interface that operates at 13.56 MHZ.

2.13 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. Delayed Egress (DE)

1. General:

a. The delay egress locking hardware shall provide a method to secure emergency exits and provide an approved delayed emergency exit method. The package shall be Underwriters Laboratories

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

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

unlock and provide free egress. The Contractor shall provide any required fire alarm relays or interface devices.

c. Reset Mode
   1) The delay egress device shall be manually reset by the Delayed Egress controller located at the door via key switch.
   2) The delay egress device shall automatically reset upon fire alarm system reset.
   3) The delayed egress shall be resettable through the SMS.

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

e. Each individual delayed egress door shall have the ability to unlock through a manual action on the SMS.

f. Unless otherwise indicated the Contractor shall provide all of the above reset methods for each door. All signs will meet the latest ADA requirements.

g. Signs
   1) The delay egress package shall be provided with a warning sign complying with local code requirements. The warning sign shall be attached to the interior side of the controlled door. The sign shall be located on the interior side of the door above and within 304 mm (12 in) of the panic bar. The sign shall read:

      EMERGENCY EXIT.
      PUSH UNTIL
      ALARM SOUNDS
      DOOR CAN BE OPENED,
      IN 30 SECONDS.

2) Signs shall be coordinated and comply with the building's existing sign specifications. Signs shall include grade 2 Braille.
3) Signs shall meet the current ADA requirements.
4) In instances of code and specification conflicts, the life safety code requirement shall prevail.
5) The Division 10 Contractor shall provide samples for approval with their submittal package.

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

D. Crash Bar:
   1. Emergency Exit with Alarm (Panic):
      a. Entry control portals shall include panic bar emergency exit hardware as designed.
      b. Panic bar emergency exit hardware shall provide an alarm shunt signal to the PACS and SMS.
      c. The panic bar shall include a conspicuous warning sign with one (1) inch (2.5 cm) high, red lettering notifying personnel that an alarm will be annunciated if the panic bar is operated.
      d. Operation of the panic bar hardware shall generate an intrusion alarm that reports to both the SMS and Intrusion Detection System. The use of a micro switch installed within the panic bar shall be utilized for this.
      e. The panic bar shall utilize a fully mechanical connection only and shall not depend upon electric power for operation.

f. The panic bar shall be compatible with mortise or rim mount door hardware and shall operate by retracting the bolt manually by either pressing the panic bar or with a key by-pass. Refer to Section 2.2.I.9 for key-bypass specifications.

g. Normal Exit:

1) Entry control portals shall include panic bar non-emergency exit hardware as designed.

2) Panic bar non-emergency exit hardware shall be monitored by and report to the SMS.

3) Operation of the panic bar hardware shall not generate a locally audible or an intrusion alarm within the IDS.

4) When exiting, the panic bar shall depend upon a mechanical connection only. The exterior, non-secure side of the door shall be provided with an electrified thumb latch or lever to provide access after the credential I.D. authentication by the SMS.

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

E. 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.

F. Automatic Door Opener and Closer:
   1. Shall be low energy operators.
   2. Door closing force shall be adjustable to ensure adequate closing control.
   3. Shall have an adjustable back-check feature to cushion the door opening speed if opened violently.
   4. Motor assist shall be adjustable from 0 to 30 seconds in five (5) second increments. Motor assist shall restart the time cycle with each new activation of the initiating device.
   5. Unit shall have a three-position selector mode switch that shall permit unit to be switched "ON" to monitor for function activation, switched to "H/O" for indefinite hold open function or switched to "OFF," which shall deactivate all control functions but will allow standard door operation by means of the internal mechanical closer.
   6. Door control shall be adjustable to provide compliance with the requirements of the Americans with Disabilities Act (ADA) and ANSI standards A117.1.
   7. All automatic door openers and closers shall:
      a. Meet UL standards.
      b. Be fire rated.
      c. Have push and go function to activate power operator or power assist function.
      d. Have push button controls for setting door close and door open positions.
      e. Have open obstruction detection and close obstruction detection built into the unit.
      f. Have door closer assembly with adjustable spring size, back-check valve, sweep valve, latch valve, speed control valve and pressure adjustment valve to control door closing.
      g. Have motor start-up delay, vestibule interface delay; electric lock delay and door hold open delay up to 30 seconds. All operators shall close door under full spring power when power is removed.
      h. Are to be hard wired with power input of 120 VAC, 60Hz and connected to a dedicated circuit breaker located on a power panel reserved for security equipment.
G. 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 its 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).

2.14 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 will make 720 VA at 60 A and that will 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.
   4. Power: Push-button switches shall be powered from their associated Controller, using dc control.

2.15 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 are to 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 will 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 number 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 will 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 will indicate to the system if the strike/bolt is not engaged or is unlocked when it should be secured.
   f. Flush mounted within the door frame.
6. Electric Mortise Locks: Shall be installed within the door and an electric transfer hinge shall be utilized to allow the wires to be transferred from the door frame to the lock. If utilized with a double door, then the lock shall be installed inside the active leaf. Electric Mortise Locks shall:
   a. These locks shall be provided and installed by the Division 8 "DOOR HARDWARE" Contractor.
   b. Provide integration of the Electric Mortise Locks with the PACS for:
      1) Lock Power
      2) Request to Exit switch.
7. Electromagnetic Locks:
   a. These locks shall be without mechanical linkage utilizing no moving parts and securing the door to its frame solely on electromagnetic force.
   b. Shall be comprised of two pieces, the mag-lock and the door plate. The electromagnetic locks shall be surface mounted to the door frame and the door plate shall be surface mounted to the door.
   c. Ensure a diode is installed in line with the DC voltage supplying power to the unit in order to prevent back-check on the system when the electromagnetic lock is powered.
   d. Shall utilize a magnetic bonding sensor (MBS) to monitor the door status and report that status to the SMS.

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

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

2.16 SECONDARY ALARM ANNUNCIATOR: - NOT USED

2.17 INTERFACES

A. CCTV System Interface

1. An RS232 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. 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 50 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

2.18 FLOOR SELECT ELEVATOR CONTROL: - NOT USED

2.19 AFTER-HOURS HVAC CONTROL: - NOT USED

2.20 REAL TIME GUARD TOUR: - NOT USED

2.21 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 the 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 will 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.

2.22 WIRES AND CABLES

A. Refer to section 28 05 13 "CONDUCTORS AND CABLES FOR ELECTRONIC SAFETY AND SECURITY".

PART 3 - EXECUTION

3.1 GENERAL

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

workmanship, inspection, and testing shall be in accordance with manufacturers' recommendations and as modified herein.

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

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

3.2 CURRENT SITE CONDITIONS

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

3.3 EXAMINATION

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

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

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

3.4 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 may be used. Use NRTL-listed plenum cable in environmental air spaces, including plenum ceilings. Conceal raceway and cables except in unfinished spaces.

E. Install LAN cables using techniques, practices, and methods that are consistent with Category 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 an operable system.

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

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

1. CCTV:
   a. Provide 24 hour coverage of all entry points to the perimeter and agency buildings. As well as all emergency exits utilizing a fixed color camera.
   b. Be able to monitor, control and record cameras on a 24 hours basis.
   c. Be programmed automatically call up a camera when an access point is but into an alarm state.

d. For additional PACS system requirements as they relate to the CCTV, refer to Section 28 23 00, VIDEO SURVEILLANCE.

2. IDS:
   a. Be able monitor door control sensors.
   b. Be able to monitor and control the IDS on a 24 hours basis.
   c. Be programmed to go into an alarm state when an IDS device is put into an alarm state and notify the operator via an audible alarm.
   d. For additional PACS system requirements as they relate to the IDS, refer to Section 28 16 00, INTRUSION DETECTION SYSTEM.

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

J. Existing Equipment:
   1. The Contractor shall connect to and utilize existing door equipment, control signal transmission lines, and devices as outlined in the design package. Door equipment and signal lines that are usable in their original configuration without modification may be reused with COR 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 COR 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 COR 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 will comply with VA Master Specification 07 84 00, Firestopping. The conduit riser shall terminate in a hot-dipped galvanized metal cable terminator. The terminator shall be filled with an approved sealant as recommended by the cable manufacturer and in such a manner that the cable is not damaged.

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 will observe startup and contractor testing of selected equipment. Coordinate the startup and contractor testing schedules with the Contracting Officer's Representative (COR) 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 COR.
2. The Contractor will be present on the job site during the preparatory and initial phases of quality control to provide technical assistance.
3. The Contractor shall also be available on an as needed basis to provide assistance with follow-up phases of quality control.
4. The Contractor shall participate in the testing and validation of the system and shall provide certification that the system installed is fully operational as all construction document requirements have been fulfilled.

3.9 SYSTEM SOFTWARE

A. Update, 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. 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 must comply with minimum criteria in TIA/EIA-568-B.
2. Test each circuit and component of each system. Tests shall include, but are not limited to, measurements of power supply output under maximum load, signal loop resistance, and leakage to ground where applicable. System components with battery backup shall be operated on battery power for a period of not less than 10 percent of the calculated battery operating time. Provide special equipment and software if testing requires special or dedicated equipment.
3. Operational Test: After installation of cables and connectors, demonstrate product capability and compliance with requirements. Test each signal path for end-to-end performance from each end of all pairs installed. Remove temporary connections when tests have been satisfactorily completed.

3.11 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 COMMISSIONING

A. Provide commissioning documentation in accordance with the requirements of Section 28 08 00 – COMMISSIONING OF ELECTRONIC SAFETY AND SECURITY SYSTEMS for all inspection, start up, and contractor testing required above and required by the System Readiness Checklist provided by the Commissioning Agent.

B. Components provided under this section of the specification will be tested as part of a larger system. Refer to Section 28 08 00 – COMMISSIONING OF ELECTRONIC SAFETY AND SECURITY SYSTEMS and related sections for contractor responsibilities for system commissioning.

3.13 DEMONSTRATION AND TRAINING

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

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

C. Develop separate training modules for the following:

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

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

-----END----