

**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 system server, operating system and application software, and field-installed Controllers connected by a high-speed electronic data transmission network. The PACS shall have the following:
  - 1. Physical Access Control:
    - a. Regulating access through doors.
    - b. Credential cards and readers
    - c. RS-232 ASCII interface
    - d. Monitoring of field-installed devices
    - e. Reporting
  - 2. Security:
    - a. Time and attendance.
    - b. Key tracking.
    - c. Video and camera control.
    - d. Time and attendance
- 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. 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. Head-End equipment server,
  - 2. One or more networked PC-based workstations,
  - 3. Physical Access Control System and Database Management Software,
  - 4. Credential validation software/hardware,
  - 5. Field installed controllers,

6. PIV Middleware,
7. Card readers,
8. Biometric identification devices,
9. PIV cards.
10. Supportive information system,
11. Door locks and sensors,
12. Power supplies,
13. Interfaces with:
  - a. Video Surveillance and Assessment System,
  - b. Gate, turnstile, and traffic arm controls,
  - c. Automatic door operators,
  - d. Intrusion Detection System,
  - e. Intercommunication System
  - f. Fire Protection System,
  - g. HVAC,
  - h. Building Management System,
- F. Head-End equipment server, workstations and controllers shall be connected by a high-speed electronic data transmission network.
- G. Information system supporting PACS , Head-End equipment server, workstations, network switches, routers and controllers shall comply with FIPS 200 requirements (Minimum Security Requirements for Federal Information and Information Systems)and NIST Special Publication 800-53 (Recommended Security Controls for Federal Information Systems).
- H. PACS system shall support:
  1. Multiple credential authentication modes,
  2. Bidirectional communication with the reader,
  3. 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.
  4. Visitor management,
- 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: System to be Lenel 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 existing 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. Console Network:

1. Console network, if required, shall provide communication between a central station and any subordinate or separate stations of the system. Where redundant central or parallel stations are required, the console network shall allow the configuration of stations as master and slave. The console network may be a part of the field device network or may be separate depending upon the manufacturer's system configuration.

R. 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 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.

S. The contractor shall retain Lenel to provide the PACS systems for this project. The contractor shall furnish, install and connect all door

hardware devices to the system as directed by Lenel. Retain Lenel to program 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 26 05 11 - REQUIREMENTS FOR ELECTRICAL INSTALLATIONS. Requirements for connection of high voltage.
- E. Section 26 05 21 - LOW VOLTAGE ELECTRICAL POWER CONDUCTORS AND CABLES (600 VOLTS AND BELOW). Requirements for power cables.
- F. Section 26 05 33 - RACEWAYS AND BOXES FOR ELECTRICAL SYSTEMS. Requirements for infrastructure.
- G. Section 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.
- H. Section 28 05 13 - CONDUCTORS AND CABLES FOR ELECTRONIC SAFETY AND SECURITY. Requirements for conductors and cables.
- I. Section 28 05 26 - GROUNDING AND BONDING FOR ELECTRONIC SAFETY AND SECURITY. Requirements for grounding of equipment.
- J. Section 28 05 28.33 - CONDUITS AND BOXES FOR ELECTRONIC SAFETY AND SECURITY. Requirements for infrastructure.
- K. 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**

- 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. 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 MUST 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 may 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 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.

- 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 will 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.

#### **1.10 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, 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 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. Application Software
  - 3. System Database
  - 4. Surge and Tamper Protection
  - 5. Standard Workstation Hardware
  - 6. Communications Workstation
  - 7. Controllers (Data Gathering Panel)
  - 8. Secondary Alarm Annunciator
  - 9. Keypads
  - 10. Card Readers
  - 11. Credential Cards
  - 12. System Sensors and Related Equipment
  - 13. Push Button Switches
  - 14. Interfaces
  - 15. Door and Gate Hardware interface
  - 16. RS-232 ASCII Interface
  - 17. Video and Camera Control
  - 18. Cables
  - 19. Transformers

## **2.2 SECURITY MANAGEMENT SYSTEM (SMS)**

- A. Shall allow the configuration of an enrollment and badging, alarm monitoring, administrative, asset management, digital video management, intrusion detection, visitor enrollment, remote access level management, and integrated client workstations or any combination of all or some.
- B. Shall be expandable to support an unlimited number of individual module or integrated client workstations. All access control field hardware, including Data Gathering Panels(DGP), shall be connected to all physical access control system workstation on the network.

- C. Shall have the ability to compose, file, maintain, update, and print reports for either individuals or the system as follows.
  - 1. Individual reports that consist of an employee's name, office location, phone number or direct extension, and normal hours of operation. The report shall provide a detail listing of the employee's daily events in relation to accessing points within a facility.
  - 2. System reports shall be able to produce information on a daily/weekly/monthly basis for all events, alarms, and any other activity associated with a system user.
- D. All reports shall be in a date/time format and all information shall be clearly presented. Shall be designed to allow it to work with any industry standard network protocol and topology listed below:
  - 1. Transmission Control Protocol (TCP)/IP
  - 2. Novell Netware (IPX/SPX)
  - 3. Banyan VINES
  - 4. IBM LAN Server (NetBEUI)
  - 5. Microsoft LAN Manager (NetBEUI)
  - 6. Network File System (NFS) Networks
  - 7. Remote Access Service (RAS) via ISDN, x.25, and standard phone lines.
- E. Shall provide full interface and control of the PACS to include the following subsystems within the PACS:
  - 1. Public Key Infrastructure
  - 2. Card Management
  - 3. Identity and Access Management
  - 4. Personal Identity Verification
- F. Shall have the following features or compatibilities:
  - 1. The ability to be operated locally or remotely via a LAN, WAN, internet, or intranet.
  - 2. Event and Alarm Monitoring
  - 3. Database Partitioning
  - 4. Ability to fully integrate with all other security subsystems
  - 5. Enhanced Monitoring Station with Split Screen Views
  - 6. Alternate and Extended Shunt by Door
  - 7. Escort Management
  - 8. Enhanced IT-based Password Protection

10. N-man Rule and Occupancy Restrictions
11. Open Journal Data Format for Enhanced Reporting
12. Automated Personnel Import
13. ODBC Support
14. Windows 2000 Professional, Windows Server 2003, Windows XP  
Professionals for Servers, Windows 7
15. Field-Level Audit Trail
16. Cardholder Access Events

### **2.3 APPLICATION SOFTWARE**

- A. System Software: Based on Microsoft Windows central-station and workstation operating system and application software. Software shall have the following features:
  1. Multiuser multitasking to allow independent activities and monitoring to occur simultaneously at different workstations.
  2. Graphical user interface to show pull-down menus and a menu tree format.
  3. Capability for future additions within the indicated system size limits.
  4. Open architecture that allows importing and exporting of data and interfacing with other systems that are compatible with operating system.
  5. Password-protected operator and smart card login and access.
- B. Peer Computer Control Software: Shall detect a failure of a central computer, and shall cause the other central computer to assume control of all system functions without interruption of operation. Drivers shall be provided in both central computers to support this mode of operation.
- C. Application Software: Interface between the alarm annunciation and entry-control Controllers, to monitor sensors[ and DTS links], operate displays, report alarms, generate reports, and help train system operators. Software shall have the following functions:
  1. Resides at the Central Station, workstations, and Controllers as required to perform specified functions.
  2. Operate and manage peripheral devices.
  3. Manage files for disk I/O, including creating, deleting, and copying files; and automatically maintain a directory of all files,

- including size and location of each sequential and random-ordered record.
4. Import custom icons into graphics views to represent alarms and I/O devices.
  5. Globally link I/O so that any I/O can link to any other I/O within the same Location, without requiring interaction with the host PC. This operation shall be at the Controller.
  6. Globally code I/O links so that any access-granted event can link to any I/O with the same Location without requiring interaction with the host PC. This operation shall be at the Controller.
  7. Messages from PC to Controllers and Controllers to Controllers shall be on a polled network that utilizes check summing and acknowledgment of each message. Communication shall be automatically verified, buffered, and retransmitted if message is not acknowledged.
  8. Selectable poll frequency and message time-out settings shall handle bandwidth and latency issues for TCP/IP, RF, and other PC-to-Controller communications methods by changing the polling frequency and the amount of time the system waits for a response.
  9. Automatic and encrypted backups for database and history backups shall be automatically stored at a selected workstation chosen by the VA COTR and encrypted with a nine-character alphanumeric password, which must be used to restore or read data contained in backup.
  10. Operator audit trail for recording and reporting all changes made to database and system software.

D. Workstation Software:

1. Password levels shall be individually customized at each workstation to allow or disallow operator access to program functions for each Location.
2. Workstation event filtering shall allow user to define events and alarms that will be displayed at each workstation. If an alarm is unacknowledged (not handled by another workstation) for a preset amount of time, the alarm will automatically appear on the filtered workstation.

E. Controller Software:

1. Controllers shall operate as an autonomous intelligent processing unit. Controllers shall make decisions about physical access control, alarm monitoring, linking functions, and door locking schedules for its operation, independent of other system components. Controllers shall be part of a fully distributed processing control network. The portion of the database associated with a Controller and consisting of parameters, constraints, and the latest value or status of points connected to that Controller, shall be maintained in the Controller.
2. Functions: The following functions shall be fully implemented and operational within each Controller:
  - a. Monitoring inputs.
  - b. Controlling outputs.
  - c. Automatically reporting alarms to the Central Station.
  - d. Reporting of sensor and output status to Central Station on request.
  - e. Maintaining real time, automatically updated by the Central Station at least once a day.
  - f. Communicating with the Central Station.
  - g. Executing Controller resident programs.
  - h. Diagnosing.
  - i. Downloading and uploading data to and from the Central Station.
3. Controller Operations at a Location:
  - a. Location: Up to 64 Controllers connected to RS-485 communications loop. Globally operating I/O linking and anti-passback functions between Controllers within the same Location without central-station or workstation intervention. Linking and anti-passback shall remain fully functional within the same Location even when the Central Station or workstations are off line.
  - b. In the event of communications failure between the Central Station and a Location, there shall be no degradation in operations at the Controllers at that Location. The Controllers at each Location shall be connected to a memory buffer with a capacity to store up to 10,000 events; there shall be no loss of transactions in system history files until the buffer overflows.

- c. Buffered events shall be handled in a first-in-first-out mode of operation.
- 4. Individual Controller Operation:
  - a. Controllers shall transmit alarms, status changes, and other data to the Central Station when communications circuits are operable. If communications are not available, Controllers shall function in a stand-alone mode and operational data, including the status and alarm data normally transmitted to the Central Station, shall be stored for later transmission to the Central Station. Storage capacity for the latest 1024 events shall be provided at each Controller.
  - b. Card-reader ports of a Controller shall be custom configurable for at least 120 different card-reader or keypad formats. Multiple reader or keypad formats may be used simultaneously at different Controllers or within the same Controller.
  - c. Controllers shall provide a response to card-readers or keypad entries in less than 0.25 seconds, regardless of system size.
  - d. Controllers that are reset, or powered up from a nonpowered state, shall automatically request a parameter download and reboot to its proper working state. This shall happen without any operator intervention.
  - e. Initial Startup: When Controllers are brought on-line, database parameters shall be automatically downloaded to them. After initial download is completed, only database changes shall be downloaded to each Controller.
  - f. Failure Mode: On failure for any reason, Controllers shall perform an orderly shutdown and force Controller outputs to a predetermined failure mode state, consistent with the failure modes shown and the associated control device.
  - g. Startup After Power Failure: After power is restored, startup software shall initiate self-test diagnostic routines, after which Controllers shall resume normal operation.
  - h. Startup After Controller Failure: On failure, if the database and application software are no longer resident, Controllers shall not restart, but shall remain in the failure mode until repaired. If database and application programs are resident,

Controllers shall immediately resume operation. If not, software shall be restored automatically from the Central Station.

5. Communications Monitoring:

- a. System shall monitor and report status of RS-485 communications loop [TCP/IP communication status] of each Location.
- b. Communication status window shall display which Controllers are currently communicating, a total count of missed polls since midnight, and which Controller last missed a poll.
- c. Communication status window shall show the type of CPU, the type of I/O board, and the amount of RAM memory for each Controller.

6. Operating systems shall include a real-time clock function that maintains seconds, minutes, hours, day, date, and month. The real-time clock shall be automatically synchronized with the Central Station at least once a day to plus or minus 10 seconds. The time synchronization shall be automatic, without operator action and without requiring system shutdown.

F. PC-to-Controller Communications:

1. Central-station or workstation communications shall use the following:
  - a. Direct connection using serial ports of the PC.
  - b. TCP/IP LAN network interface cards.
  - c. Dial-up modems for connections to Locations.
2. Serial Port Configuration: Each serial port used for communications shall be individually configurable for "direct communications," "modem communications incoming and outgoing," or "modem communications incoming only"; or as an ASCII output port.
3. Multiport Communications Board: Use if more than two serial ports are needed.
  - a. Expandable and modular design. Use a 4-, 8-, or 16-serial port configuration that is expandable to 32 or 64 serial ports.
  - b. Connect the first board to an internal PCI bus adapter card.
4. Direct serial, TCP/IP, and dial-up communications shall be alike in the monitoring or control of system, except for the connection that must first be made to a dial-up Location.
5. TCP/IP network interface card shall have an option to set the poll frequency and message response time-out settings.



6. PC-to-Controller and Controller-to-Controller communications (direct, dial-up, or TCP/IP) shall use a polled-communication protocol that checks sum and acknowledges each message. All communications shall be verified and buffered and retransmitted if not acknowledged.

G. Direct Serial or TCP/IP PC-to-Controller Communications:

1. Communication software on the PC shall supervise the PC-to-Controller communications link.
2. Loss of communications to any Controller shall result in an alarm at all PCs running the communications software.
3. When communications are restored, all buffered events shall automatically upload to the PC, and any database changes shall be automatically sent to the Controller.

H. Dial-up Modem PC-to-Controller Communications:

1. Communication software on the PC shall supervise the PC-to-Controller communications link during dial-up modem connect times.
2. Communication software shall be programmable to routinely poll each of the remote dial-up modem Locations, collecting event logs and verifying phone lines at time intervals that are operator selectable for each Location.
3. System shall be programmable for dialing and connecting to all dial-up modem Locations and for retrieving the accrued history transactions on an automatic basis as often as once every 10 minutes and up to once every 9999 minutes.
4. Failure to communicate to a dial-up Location three times in a row shall result in an alarm at the PC.
5. Time offset capabilities shall be present so that Locations in a different geographical time zone than the host PC will be set to, and maintained at, the proper local time. This feature shall allow for geographical time zones that are ahead of or behind the host PC.
6. The Controller connected to a dial-up modem shall automatically buffer all normal transactions until its buffer reaches 80 percent of capacity. When the transaction buffer reaches 80 percent, the Controller shall automatically initiate a call to the Central Station and upload all transactions.
7. Alarms shall be reported immediately.

8. Dial-up modems shall be provided by manufacturer of the system.  
Modems used at the Controller shall be powered by the Controller.  
Power to the modem shall include battery backup if the Controller is so equipped.

I. Controller-to-Controller Communications:

1. Controller-to-Controller Communications: RS-485, 4-wire, point-to-point, regenerative (repeater) communications network methodology.
2. RS-485 communications signal shall be regenerated at each Controller.

J. Database Downloads:

1. All data transmissions from PCs to a Location, and between Controllers at a Location, shall include a complete database checksum to check the integrity of the transmission. If the data checksum does not match, a full data download shall be automatically retransmitted.
2. If a Controller is reset for any reason, it shall automatically request and receive a database download from the PC. The download shall restore data stored at the Controller to their normal working state and shall take place with no operator intervention.

K. Operator Interface:

1. Inputs in system shall have two icon representations, one for the normal state and one for the abnormal state.
2. When viewing and controlling inputs, displayed icons shall automatically change to the proper icon to display the current system state in real time. Icons shall also display the input's state, whether armed or bypassed, and if the input is in the armed or bypassed state due to a time zone or a manual command.
3. Outputs in system shall have two icon representations, one for the secure (locked) state and one for the open (unlocked) state.
4. Icons displaying status of the I/O points shall be constantly updated to show their current real-time condition without prompting by the operator.
5. The operator shall be able to scroll the list of I/Os and press the appropriate toolbar button, or right click, to command the system to perform the desired function.
6. Graphic maps or drawings containing inputs, outputs, and override groups shall include the following:

- a. Database to import and store full-color maps or drawings and allow for input, output, and override group icons to be placed on maps.
  - b. Maps to provide real-time display animation and allow for control of points assigned to them.
  - c. System to allow inputs, outputs, and override groups to be placed on different maps.
  - d. Software to allow changing the order or priority in which maps will be displayed.
7. Override Groups Containing I/Os:
- a. System shall incorporate override groups that provide the operator with the status and control over user-defined "sets" of I/Os with a single icon.
  - b. Icon shall change automatically to show the live summary status of points in that group.
  - c. Override group icon shall provide a method to manually control or set to time zone points in the group.
  - d. Override group icon shall allow the expanding of the group to show icons representing the live status for each point in the group, individual control over each point, and the ability to compress the individual icons back into one summary icon.
8. Schedule Overrides of I/Os and Override Groups:
- a. To accommodate temporary schedule changes that do not fall within the holiday parameters, the operator shall have the ability to override schedules individually for each input, output, or override group.
  - b. Each schedule shall be composed of a minimum of two dates with separate times for each date.
  - c. The first time and date shall be assigned the override state that the point shall advance to, when the time and date become current.
  - d. The second time and date shall be assigned the state that the point shall return to, when the time and date become current.
9. Copy command in database shall allow for like data to be copied and then edited for specific requirements, to reduce redundant data entry.

L. Operator Access Control:

1. Control operator access to system controls through three password-protected operator levels. System operators and managers with appropriate password clearances shall be able to change operator levels for operators.
2. Three successive attempts by an operator to execute functions beyond their defined level during a 24-hour period shall initiate a software tamper alarm.
3. A minimum of 32 passwords shall be available with the system software. System shall display the operator's name or initials in the console's first field. System shall print the operator's name or initials, action, date, and time on the system printer at login and logoff.
4. The password shall not be displayed or printed.
5. Each password shall be definable and assignable for the following:
  - a. Commands usable.
  - b. Access to system software.
  - c. Access to application software.
  - d. Individual zones that are to be accessed.
  - e. Access to database.

M. Operator Commands:

1. Command Input: Plain-language words and acronyms shall allow operators to use the system without extensive training or data-processing backgrounds. System prompts shall be a word, a phrase, or an acronym.
2. Command inputs shall be acknowledged and processing shall start in not less than 1 second(s).
3. Tasks that are executed by operator's commands shall include the following:
  - a. Acknowledge Alarms: Used to acknowledge that the operator has observed the alarm message.
  - b. Place Zone in Access: Used to remotely disable intrusion alarm circuits emanating from a specific zone. System shall be structured so that console operator cannot disable tamper circuits.
  - c. Place Zone in Secure: Used to remotely activate intrusion alarm circuits emanating from a specific zone.

- d. System Test: Allows the operator to initiate a system-wide operational test.
- e. Zone Test: Allows the operator to initiate an operational test for a specific zone.
- f. Print reports.
- g. Change Operator: Used for changing operators.
- h. Security Lighting Controls: Allows the operator to remotely turn on/off security lights.
- i. Display Graphics: Used to display any graphic displays implemented in the system. Graphic displays shall be completed within 20 seconds from time of operator command.
- j. Run system tests.
- k. Generate and format reports.
- l. Request help with the system operation.
  - 1) Include in main menus.
  - 2) Provide unique, descriptive, context-sensitive help for selections and functions with the press of one function key.
  - 3) Provide navigation to specific topic from within the first help window.
  - 4) Help shall be accessible outside the applications program.
- m. Entry-Control Commands:
  - 1) Lock (secure) or unlock (open) each controlled entry and exit up to four times a day through time-zone programming.
  - 2) Arm or disarm each monitored input up to four times a day through time-zone programming.
  - 3) Enable or disable readers or keypads up to twice a day through time-zone programming.
  - 4) Enable or disable cards or codes up to four times per day per entry point through access-level programming.
- 4. Command Input Errors: Show operator input assistance when a command cannot be executed because of operator input errors. Assistance screen shall use plain-language words and phrases to explain why the command cannot be executed. Error responses that require an operator to look up a code in a manual or other document are not acceptable. Conditions causing operator assistance messages include the following:
  - a. Command entered is incorrect or incomplete.

- b. Operator is restricted from using that command.
  - c. Command addresses a point that is disabled or out of service.
  - d. Command addresses a point that does not exist.
  - e. Command is outside the system's capacity.
- N. Alarms:
- 1. System Setup:
    - a. Assign manual and automatic responses to incoming point status change or alarms.
    - b. Automatically respond to input with a link to other inputs, outputs, operator-response plans, unique sound with use of WAV files, and maps or images that graphically represent the point location.
    - c. 60-character message field for each alarm.
    - d. Operator-response-action messages shall allow message length of at least 65,000 characters, with database storage capacity of up to 32,000 messages. Setup shall assign messages to zone.
    - e. Secondary messages shall be assignable by the operator for printing to provide further information and shall be editable by the operator.
    - f. Allow 25 secondary messages with a field of 4 lines of 60 characters each.
    - g. Store the most recent 1000 alarms for recall by the operator using the report generator.
  - 2. Software Tamper:
    - a. Annunciate a tamper alarm when unauthorized changes to system database files are attempted. Three consecutive unsuccessful attempts to log onto system shall generate a software tamper alarm.
    - b. Annunciate a software tamper alarm when an operator or other individual makes three consecutive unsuccessful attempts to invoke functions beyond their authorization level.
    - c. Maintain a transcript file of the last 5000 commands entered at the each Central Station to serve as an audit trail. System shall not allow write access to system transcript files by any person, regardless of their authorization level.
    - d. Allow only acknowledgment of software tamper alarms.

3. Read access to system transcript files shall be reserved for operators with the highest password authorization level available in system.
4. Animated Response Graphics: Highlight alarms with flashing icons on graphic maps; display and constantly update the current status of alarm inputs and outputs in real time through animated icons.
5. Multimedia Alarm Annunciation: WAV files to be associated with alarm events for audio annunciation or instructions.
6. Alarm Handling: Each input may be configured so that an alarm cannot be cleared unless it has returned to normal, with options of requiring the operator to enter a comment about disposition of alarm. Allow operator to silence alarm sound when alarm is acknowledged.
7. Alarm Automation Interface: High-level interface to Central Station alarm automation software systems. Allows input alarms to be passed to and handled by automation systems in same manner as burglar alarms, using an RS-232 ASCII interface.
8. CCTV Alarm Interface: Allow commands to be sent to CCTV systems during alarms (or input change of state) through serial ports.
9. Camera Control: Provides operator ability to select and control cameras from graphic maps.
0. Alarm Monitoring: Monitor sensors, Controllers, and DTS circuits and notify operators of an alarm condition. Display higher-priority alarms first and, within alarm priorities, display the oldest unacknowledged alarm first. Operator acknowledgment of one alarm shall not be considered acknowledgment of other alarms nor shall it inhibit reporting of subsequent alarms.
  1. Displayed alarm data shall include type of alarm, location of alarm, and secondary alarm messages.
  2. Printed alarm data shall include type of alarm, location of alarm, date and time (to nearest second) of occurrence, and operator responses.
  3. Maps shall automatically display the alarm condition for each input assigned to that map, if that option is selected for that input location.
  4. Alarms initiate a status of "pending" and require the following two handling steps by operators:

- a. First Operator Step: "Acknowledged." This action shall silence sounds associated with the alarm. The alarm remains in the system "Acknowledged" but "Un-Resolved."
  - b. Second Operator Step: Operators enter the resolution or operator comment, giving the disposition of the alarm event. The alarm shall then clear.
5. Each workstation shall display the total pending alarms and total unresolved alarms.
6. Each alarm point shall be programmable to disallow the resolution of alarms until the alarm point has returned to its normal state.
7. Alarms shall transmit to Central Station in real time, except for allowing connection time for dial-up locations.
8. Alarms shall be displayed and managed from a minimum of four different windows.
  - a. Input Status Window: Overlay status icon with a large red blinking icon. Selecting the icon will acknowledge the alarm.
  - b. History Log Transaction Window: Display name, time, and date in red text. Selecting red text will acknowledge the alarm.
  - c. Alarm Log Transaction Window: Display name, time, and date in red. Selecting red text will acknowledge the alarm.
  - d. Graphic Map Display: Display a steady colored icon representing each alarm input location. Change icon to flashing red when the alarm occurs. Change icon from flashing red to steady red when the alarm is acknowledged.
9. Once an alarm is acknowledged, the operator shall be prompted to enter comments about the nature of the alarm and actions taken. Operator's comments may be manually entered or selected from a programmed predefined list, or a combination of both.
10. For locations where there are regular alarm occurrences, provide programmed comments. Selecting that comment shall clear the alarm.
11. The time and name of the operator who acknowledged and resolved the alarm shall be recorded in the database.
12. Identical alarms from same alarm point shall be acknowledged at same time the operator acknowledges the first alarm. Identical alarms shall be resolved when the first alarm is resolved.
13. Alarm functions shall have priority over downloading, retrieving, and updating database from workstations and Controllers.



14. When a reader-controlled output (relay) is opened, the corresponding alarm point shall be automatically bypassed.
- P. Monitor Display: Display text and graphic maps that include zone status integrated into the display. Colors are used for the various components and current data. Colors shall be uniform throughout the system.
  1. Color Code:
    - a. FLASHING RED: Alerts operator that a zone has gone into an alarm or that primary power has failed.
    - b. STEADY RED: Alerts operator that a zone is in alarm and alarm has been acknowledged.
    - c. YELLOW: Advises operator that a zone is in access.
    - d. GREEN: Indicates that a zone is secure and that power is on.
  2. Graphics:
    - a. Support 32,000 graphic display maps and allow import of maps from a minimum of 16 standard formats from another drawing or graphics program.
    - b. Allow I/O to be placed on graphic maps by the drag-and-drop method.
    - c. Operators shall be able to view the inputs, outputs, and the point's name by moving the mouse cursor over the point on graphic map.
    - d. Inputs or outputs may be placed on multiple graphic maps. The operator shall be able to toggle to view graphic map associated with inputs or outputs.
    - e. Each graphic map shall have a display-order sequence number associated with it to provide a predetermined order when toggled to different views.
    - f. Camera icons shall have the ability to be placed on graphic maps that, when selected by an operator, will open a video window, display the camera associated with that icon, and provide pan-tilt-zoom control.
    - g. Input, output, or camera placed on a map shall allow the ability to arm or bypass an input, open or secure an output, or control the pan-tilt-zoom function of the selected camera.
- Q. System test software enables operators to initiate a test of the entire system or of a particular portion of the system.

1. Test Report: The results of each test shall be stored for future display or printout. The report shall document the operational status of system components.
- R. Report Generator Software: Include commands to generate reports for displaying, printing, and storing on disk and tape. Reports shall be stored by type, date, and time. Report printing shall be the lowest priority activity. Report generation mode shall be operator selectable but set up initially as periodic, automatic, or on request. Include time and date printed and the name of operator generating the report. Report formats may be configured by operators.
  1. Automatic Printing: Setup shall specify, modify, or inhibit the report to be generated; the time the initial report is to be generated; the time interval between reports; the end of period; and the default printer.
  2. Printing on Requests: An operator may request a printout of any report.
  3. Alarm Reports: Reporting shall be automatic as initially set up. Include alarms recorded by system over the selected time and information about the type of alarm, the type of sensor, the location, the time, and the action taken.
  4. Access and Secure Reports: Document zones placed in access, the time placed in access, and the time placed in secure mode.
  5. Custom Reports: Reports tailored to exact requirements of who, what, when, and where. As an option, custom report formats may be stored for future printing.
  6. Automatic History Reports: Named, saved, and scheduled for automatic generation.
  7. Cardholder Reports: Include data, or selected parts of the data, as well as the ability to be sorted by name, card number, imprinted number, or by any of the user-defined fields.
  8. Cardholder by Reader Reports: Based on who has access to a specific reader or group of readers by selecting the readers from a list.
  9. Cardholder by Access-Level Reports: Display everyone that has been assigned to the specified access level.
10. Who Is In (Muster) Report:
  - a. Emergency Muster Report: One click operation on toolbar launches report.

- b. Cardholder Report. Contain a count of persons that are "In" at a selected Location and a count with detailed listing of name, date, and time of last use, sorted by the last reader used or by the group assignment.
- 11. Panel Labels Reports: Printout of control-panel field documentation including the actual location of equipment, programming parameters, and wiring identification. Maintain system installation data within system database so that they are available on-site at all times.
- 12. Activity and Alarm On-Line Printing: Activity printers for use at workstations; prints all events or alarms only.
- 13. History Reports: Custom reports that allows the operator to select any date, time, event type, device, output, input, operator, Location, name, or cardholder to be included or excluded from the report.
  - a. Initially store history on the hard disk of the host PC.
  - b. Permit viewing of the history on workstations or print history to any system printer.
  - c. The report shall be definable by a range of dates and times with the ability to have a daily start and stop time over a given date range.
  - d. Each report shall depict the date, time, event type, event description, device, or I/O name, cardholder group assignment, and cardholder name or code number.
  - e. Each line of a printed report shall be numbered to ensure that the integrity of the report has not been compromised.
  - f. Total number of lines of the report shall be given at the end of the report. If the report is run for a single event such as "Alarms," the total shall reflect how many alarms occurred during that period.
- 14. Reports shall have the following four options:
  - a. View on screen.
  - b. Print to system printer. Include automatic print spooling and "Print To" options if more than one printer is connected to system.
  - c. "Save to File" with full path statement.
  - d. System shall have the ability to produce a report indicating status of system inputs and outputs or of inputs and outputs that

are abnormal, out of time zone, manually overridden, not reporting, or in alarm.

15. Custom Code List Subroutine: Allow the access codes of system to be sorted and printed according to the following criteria:
  - a. Active, inactive, or future activate or deactivate.
  - b. Code number, name, or imprinted card number.
  - c. Group, Location, access levels.
  - d. Start and stop code range.
  - e. Codes that have not been used since a selectable number of days.
  - f. In, out, or either status.
  - g. Codes with trace designation.
16. The reports of system database shall allow options so that every data field may be printed.
17. The reports of system database shall be constructed so that the actual position of the printed data shall closely match the position of the data on the data-entry windows.

S. Anti-Passback:

1. System shall have global and local anti-passback features, selectable by Location. System shall support hard and soft anti-passback.
2. Hard Anti-Passback: Once a credential holder is granted access through a reader with one type of designation (IN or OUT), the credential holder may not pass through that type of reader designation until the credential holder passes through a reader of opposite designation.
3. Soft Anti-Passback: Should a violation of the proper IN or OUT sequence occur, access shall be granted, but a unique alarm shall be transmitted to the control station, reporting the credential holder and the door involved in the violation. A separate report may be run on this event.
4. Timed Anti-Passback: A Controller capability that prevents an access code from being used twice at the same device (door) within a user-defined amount of time.
5. Provide four separate zones per Location that can operate without requiring interaction with the host PC (done at Controller). Each reader shall be assignable to one or all four anti-passback zones. In addition, each anti-passback reader can be further designated as

"Hard," "Soft," or "Timed" in each of the four anti-passback zones.

The four anti-passback zones shall operate independently.

6. The anti-passback schemes shall be definable for each individual door.
7. The Master Access Level shall override anti-passback.
8. System shall have the ability to forgive (or reset) an individual credential holder or the entire credential holder population anti-passback status to a neutral status.

T. Visitor Assignment:

1. Provide for and allow an operator to be restricted to only working with visitors. The visitor badging subsystem shall assign credentials and enroll visitors. Allow only access levels that have been designated as approved for visitors.
2. Provide an automated log of visitor name, time and doors accessed, and whom visitor contacted.
3. Allow a visitor designation to be assigned to a credential holder.
4. PACS shall be able to restrict the access levels that may be assigned to credentials that are issued to visitors.
5. Allow operator to recall visitors' credential holder file, once a visitor is enrolled in the system.
6. The operator may designate any reader as one that deactivates the credential after use at that reader. The history log shall show the return of the credential.
7. System shall have the ability to use the visitor designation in searches and reports. Reports shall be able to print all or any visitor activity.

U. Training Software: Enables operators to practice system operation including alarm acknowledgment, alarm assessment, response force deployment, and response force communications. System shall continue normal operation during training exercises and shall terminate exercises when an alarm signal is received at the console.

V. Entry-Control Enrollment Software: Database management functions that allow operators to add, delete, and modify access data as needed.

1. The enrollment station shall not have alarm response or acknowledgment functions.

2. Provide multiple, password-protected access levels. Database management and modification functions shall require a higher operator access level than personnel enrollment functions.
3. The program shall provide means to disable the enrollment station when it is unattended to prevent unauthorized use.
4. The program shall provide a method to enter personnel identifying information into the entry-control database files through enrollment stations. In the case of personnel identity verification subsystems, this shall include biometric data. Allow entry of personnel identifying information into the system database using menu selections and data fields. The data field names shall be customized during setup to suit user and site needs. Personnel identity verification subsystems selected for use with the system shall fully support the enrollment function and shall be compatible with the entry-control database files.
5. Cardholder Data: Provide 99 user-defined fields. System shall have the ability to run searches and reports using any combination of these fields. Each user-defined field shall be configurable, using any combination of the following features:
  - a. MASK: Determines a specific format that data must comply with.
  - b. REQUIRED: Operator is required to enter data into field before saving.
  - c. UNIQUE: Data entered must be unique.
  - d. DEACTIVATE DATE: Data entered will be evaluated as an additional deactivate date for all cards assigned to this cardholder.
  - e. NAME ID: Data entered will be considered a unique ID for the cardholder.
6. Personnel Search Engine: A report generator with capabilities such as search by last name, first name, group, or any predetermined user-defined data field; by codes not used in definable number of days; by skills; or by seven other methods.
7. Multiple Deactivate Dates for Cards: User-defined fields to be configured as additional stop dates to deactivate any cards assigned to the cardholder.
8. Batch card printing.
9. Default card data can be programmed to speed data entry for sites where most card data are similar.

10. Enhanced ACSII File Import Utility: Allows the importing of cardholder data and images.

W. System Redundancy & High Availability: The system shall provide multiple levels of communications redundancy and failover for all PACS hosted controllers, digital video recorders, and client workstations. The PACS shall be capable of automatically re-routing communications to alternate computers across the system without operator intervention.

1. PACS system configuration with a single application/ database server shall provide at a minimum the following redundancy and failover capability:

- a. The PACS shall provide communications redundancy and failover for network-attached devices. Each network attached device shall have one or more alternative communication sever(s) that can provide hosting in case of primary communications server failure.
- b. In case of primary communications server failure, the system shall automatically re-route network-attached devices to their designated backup communications servers to allow continuous system operations without loss of alarm and event transaction processing during failover.
- c. Network-attached devices which transition to backup communications servers, shall be able to be redirected back to their default primary servers, once the primary communications servers have been restored.

#### **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**

A. SMS Server Computer: Standard unmodified PC of modular design. The CPU word size shall be 64 bytes or larger; the CPU operating speed shall be at least 3.4 GHz.

1. Processor family: Intel® Xeon® E5640 (4 core, 2.66 GHz, 12MB L3, 80W).
2. Number of processors: 2
3. Memory: 12 GB RAM , expandable to a minimum of 192 GB without additional chassis or power supplies. Memory protection Mirrored Memory, Online Spare, Advanced ECC, Memory Lock Step Mode.

4. Input/Output: 2 expansions slots, Network Controller (2) 1GbE NC382i Multifunction 4 Ports.
5. Power Supply: Dual - minimum capacity of 460 W hot plug.
6. Real-Time Clock:
  - a. Accuracy: Plus or minus 1 minute per month.
  - b. Time Keeping Format: 24-hour time format including seconds, minutes, hours, date, day, and month; resettable by software.
  - c. Clock shall function for 1 year without power.
  - d. Provide automatic time correction once every 24 hours by synchronizing clock with the Time Service Department of the U.S. Naval Observatory.
7. Serial Ports: Provide two RS-232-F serial ports for general use, with additional ports as required. Data transmission rates shall be selectable under program control.
8. Parallel Port: An enhanced parallel port.
9. The server shall have a 1 GB NIC or greater network card, rated at 100/1000 MB/sec.
10. The server shall have dual 100 GB hard disk drives at 7200 RPM.
11. The server shall have a CD / DVD combo drive.
12. The server operating system shall be either:
  - a. Windows XP Professional Service Pack 2 or later and default services enabled.
13. The Web Server shall be IIS 7.0 or better.
14. The Database shall be SQL Server 2005 (Express, Standard, Data Center, or Enterprise).
15. Sound Card: For playback and recording of digital WAV sound files that are associated with audible warning and alarm functions.
16. Color Monitor: [17"] or larger SVGA (1024 x 768) monitor with true color support.. The server shall have a dedicated 256 MB SVGA accelerated video card with at least 64 MB onboard RAM.
17. Keyboard: With a minimum of 64 characters, standard ASCII character set based on ANSI X3.154.
18. Mouse: Standard, compatible with the installed software.
19. Special function keyboard attachments or special function keys to facilitate data input of the following operator tasks:
  - a. Help.
  - b. Alarm Acknowledge.



- c. Place Zone in Access.
  - d. Place Zone in Secure.
  - e. System Test.
  - f. Print Reports.
  - g. Change Operator.
20. CD-ROM Drive:
- a. Nominal storage capacity of 650 MB.
  - b. Data Transfer Rate: 1.2 Mbps.
  - c. Average Access Time: 150 ms.
  - d. Cache Memory: 256 KB.
  - e. Data Throughput: 1 MB/second, minimum.

## 2.6 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 signals, and for conditions as described in UL 1076 for line security equipment 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, 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.
    - 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 time listed in a schedule, alarm sounds.
4. With power supplies sufficient to power at voltage and frequency required for field devices and portal-control devices.
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.

## **2.7 CARD READERS**

- A. Card readers shall be compatible with hospitals Lenel System.
- B. Power: Card reader shall be powered from its associated Controller, including its standby power source.
- C. 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.
- D. 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.
- E. Display: LED or other type of visual indicator display shall provide visual 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.
- F. 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.
- G. Will be fully programmable and addressable, locally and remotely, and hardwired to the system.
- H. Shall be individually home run to the main panel.
- I. 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
- J. Shall support a variety of card readers that must encompass a wide functional range. The PACS may combine any of the card readers described below for installations requiring multiple types of card reader capability (i.e., card only, card and/or PIN, card and/or biometrics, card and/or pin and/or biometrics, supervised inputs, etc.). These card readers shall be available in the approved technology to meet FIPS 201, and is ISO 14443 A or B, ISO/IEC 7816 compliant. The reader output can be Wiegand, RS-22, 485 or TCP/IP.
- K. Shall be housed in an aluminum bezel with a wide lead-in for easy card entry.
- L. Shall contain read head electronics, and a sender to encode digital door control signals.
- M. LED's shall be utilized to indicate card reader status and access status.
- N. 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.
- O. 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.

- P. Shall have a minimum of two programmable inputs and two programmable outputs.
- Q. 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.
- R. Shall include a Light Emitting Diode (LED) or other type of visual indicator display and provide visual or visual and audible status indications and user prompts. The display shall indicate power on/off, and whether user passage requests have been accepted or rejected. The design of the keypad display or keypad enclosure shall limit the maximum horizontal and vertical viewing angles of the keypad. The maximum horizontal viewing angle shall be plus and minus five (5) degrees or less off a vertical plane perpendicular to the plane of the face of the keypad display. The maximum vertical viewing angle shall be plus and minus 15 degrees or less off a horizontal plane perpendicular to the plane of the face of the keypad display.
  - 1. Shall respond to passage requests by generating a signal to the local processor. The response time shall be 800 milliseconds or less from the time the last alphanumeric symbol is entered until a response signal is generated.
  - 2. Shall be powered from the source as designed and shall not dissipate more than 150 Watts.
  - 3. Shall be suitable for surface, semi-flush, pedestal, or weatherproof mounting as required.
  - 4. Shall provide a means for users to indicate a duress situation by entering a special code.
- S. PIV Contact Card Reader
  - 1. Application Protocol Data Unit (APDU) Support: At a minimum, the contact interface shall support all card commands for contact based access specified in Section 7, End-point PIV Card Application Card

- Command Interface of SP 800-73-1, Interfaces for Personal Identity Verification.
2. Buffer Size: The reader must contain a buffer large enough to receive the maximum size frame permitted by International Organization for Standardization International Electrotechnical Commission (ISO/IEC) 7816-3:1997, Section 9.4.
  3. Programming Voltage: PIV Readers shall not generate a Programming Voltage.
  4. Support for Operating Class: PIV Readers shall support cards with Class A Vccs as defined in ISO/IEC 7816-3:1997 and ISO/IEC 7816-3:1997/Amd 1:2002.
  5. Retrieval Time: Retrieval time 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.
- T. 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

## **2.8 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 ( $\pm 14$ ) 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. Guard tour stations:

1. The guard tour station shall be single gang brushed steel plate flush mounted in a single gang box. The switch shall be a normally open momentary keyed switch.

D. Delayed Egress (DE)

1. General:

- a. The delay egress locking hardware shall provide a method to secure emergency exits and provide an approved delayed emergency exit method. The package shall be Underwriters Laboratories listed as a delay egress-locking device. The delay egress device shall be available to support configurations with both rated and



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

2. The delay-locking device shall include all of the following features:

- a. Delay Egress Mode

- 1) The delayed egress device shall be a SDC 101V Series Exit Check with wall mounted control module. Upon activation of an approved panic bar the delay locking device shall begin a delay sequence of 30 seconds; a flush mounted wall LED panel adjacent to the door will indicate initiation of the countdown time. During the 30 second delay period, a local sounding device shall annunciate a tone activation of the delay cycle and verbal exit instructions. At the end of the delay cycle the locking device shall unlock and allow free egress. The reset of the local sounding device shall be user definable and include options to select either local sound until silenced by reset or local sounder silenced upon opening of the door. Unless otherwise indicated the local delay sounder shall be silenced upon opening of the door. The SDC's device trigger output shall be connected to the SMS DGP alarm panel for pre-activation warning. The contractor shall specify the bond sensor option when ordering the delayed egress hardware; this output shall be wired to the SMS DGP to activate an alarm if the door does not lock. Use of reset panel not top mounted device.

- 2) Delayed egress doors will have bond sensors.

- 3) Delayed egress activation shall also trigger CCTV call -up.

- b. Fire Alarm Mode

- 1) Upon activation of the facility's fire evacuation and water flow alarm signal the delay locking devices shall immediately

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

c. Reset Mode

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

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

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

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

g. Signs

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

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

- 2) Signs shall be coordinated and comply with the building's existing sign specifications. Signs shall include grade 2 Braille.

- 3) Signs shall meet the current ADA requirements.

- 4) In instances of code and specification conflicts, the life safety code requirement shall prevail.
  - 5) The Division 10 Contractor shall provide samples for approval with their submittal package.
3. Physical Access Control Interface
- a. The delay egress device shall be capable of interface with card access control systems.
  - b. The system shall include a bypass feature that is activated via a dry contact relay output from the physical access control system. This bypass shall allow authorized personnel to pass through the controlled portal without creating an alarm condition or activating the delay egress cycle. The bypass shall include internal electronic shunts or door switches to prevent activation (re-arming) until the door returns to the closed position. An unused access event shall not cause a false alarm and shall automatically rearm the delay egress lock upon expiration of the programmed shunt time. The delay egress physical access control interface shall support extended periods of automated and/or manual lock and unlock cycles.

E. Crash Bar:

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

either pressing the panic bar or with a key by-pass. Refer to Section 2.2.I.9 for key-bypass specifications.

g. Normal Exit:

- 1) Entry control portals shall include panic bar non-emergency exit hardware as designed.
- 2) Panic bar non-emergency exit hardware shall be monitored by and report to the SMS.
- 3) Operation of the panic bar hardware shall not generate a locally audible or an intrusion alarm within the IDS.
- 4) When exiting, the panic bar shall depend upon a mechanical connection only. The exterior, non-secure side of the door shall be provided with an electrified thumb latch or lever to provide access after the credential I.D. authentication by the SMS.
- 5) The panic bar shall be compatible with mortise or rim mount door hardware and shall operate by retracting the bolt manually by either pressing the panic bar or with a key 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.

F. 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.

G. Automatic Door Opener and Closer:

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

2. Door Position Sensor:

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

**2.9 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 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.

## **2.10 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 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.
- D. 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.
- E. Install cables without damaging conductors, shield, or jacket.
- F. 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.
- G. 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 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.
  - 2. EPPS:
    - a. Be programmed to go into an alarm state when an emergency call box or duress alarm/panic device is activated, and notify the Physical Access Control System and Database Management of an alarm event.
    - b. For additional PACS requirements as they relate to the EPPS, refer to Section 28 26 00, ELECTRONIC PERSONAL PROTECTION 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 in the form of a report. The Contractor shall not take any corrective action without written permission received from the Contracting Officer.

J. Existing Equipment:

1. The Contractor shall connect to and utilize existing Lenel System, door equipment, control signal transmission lines, and devices as outlined in the design package. Door equipment and signal lines that are usable in their original configuration without modification may be reused with Contracting Officer approval.
2. The Contractor shall perform a field survey, including testing and inspection of all existing door equipment and signal lines intended to be incorporated into the PACS, and furnish a report to the Contracting Officer as part of the site survey report. For those items considered nonfunctioning, provide (with the report) specification sheets, or written functional requirements to support the findings and the estimated cost to correct the deficiency. As part of the report, the Contractor shall include a schedule for connection to all existing equipment.
3. The Contractor shall make written requests and obtain approval prior to disconnecting any signal lines and equipment, and creating equipment downtime. Such work shall proceed only after receiving Contracting Officer approval of these requests. If any device fails after the Contractor has commenced work on that device, signal or control line, the Contractor shall diagnose the failure and perform any necessary corrections to the equipment.
4. The Contractor shall be held responsible for repair costs due to Contractor negligence, abuse, or improper installation of equipment.
5. The Contracting Officer shall be provided a full list of all equipment that is to be removed or replaced by the Contractor, to include description and serial/manufacturer numbers where possible. The Contractor shall dispose of all equipment that has been removed or replaced based upon approval of the Contracting Officer after reviewing the equipment removal list. In all areas where equipment is removed or replaced the Contractor shall repair those areas to match the current existing conditions.

K. Enclosure Penetrations: All enclosure penetrations shall be from the bottom of the enclosure unless the system design requires penetrations

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

- 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. Biometrics:
  - 1. Connect all signal input and output cables along with all power cables.
  - 2. Program and ensure the device is in operating order.
- Q. Portal Control Devices:
  - 1. Install all signal input and output cables as well as all power cables.
  - 2. Devices shall be surface or flush mounted as per the design package.
  - 3. Program all devices and ensure they are working.

R. Door Status Indicators:

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

S. Entry Control Devices:

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

T. System Start-Up:

1. The Contractor shall not apply power to the PACS until the following items have been completed:
  - a. PACS equipment items and have been set up in accordance with manufacturer's instructions.
  - b. A visual inspection of the PACS has been conducted to ensure that defective equipment items have not been installed and that there are no loose connections.
  - c. System wiring has been tested and verified as correctly connected as indicated.
  - d. All system grounding and transient protection systems have been verified as installed and connected as indicated.
  - e. Power supplies to be connected to the PACS have been verified as the correct voltage, phasing, and frequency as indicated.
2. Satisfaction of the above requirements shall not relieve the Contractor of responsibility for incorrect installation, defective equipment items, or collateral damage as a result of Contractor work efforts.

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

U. Supplemental Contractor Quality Control:

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

**3.9 SYSTEM SOFTWARE**

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

**3.10 FIELD QUALITY CONTROL**

- A. Manufacturer's Field Service: Engage a factory-authorized service representative to inspect field-assembled components and equipment installation, including connections[, and to assist in field testing]. Report results in writing.
- B. Testing Agency: Owner will 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 5 tester. Test for faulty connectors, splices, and terminations. Test according to TIA/EIA-568-1, "Commercial Building Telecommunications Cabling Standards - Part 1

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

### **3.11 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 hours to instruct VA personnel in operation and maintenance of units.
- B. Submit training plans and instructor qualifications.
- 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.



FINAL SUBMISSION  
FOR CONSTRUCTION  
7/11/2012

VAMC WADE PARK CLEVELAND  
Dietetics Admin Space and Storage  
Project No. 541-12-113

-----END-----