SECTION 281300 - ACCESS CONTROL SOFTWARE AND DATABASE MANAGEMENT

PART 1 - GENERAL

1.1 RELATED DOCUMENTS

A. Drawings and general provisions of the Contract, including General and Supplementary Conditions and Division 01 Specification Sections, apply to this Section.

1.2 SUMMARY

A. Section Includes:

1. Security access central-control station.
2. One or more security access networked workstations.
3. Security access operating system and application software.
4. Security access controllers connected to high-speed electronic-data transmission network.

B. Related Requirements:

1. Section 281500 "Access Control System Hardware Devices" for access control system hardware, such as keypads, card readers, and biometric identity devices.

1.3 DEFINITIONS

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

B. DTS: Digital Termination Service. A microwave-based, line-of-sight communication provided directly to the end user.

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

D. Location: A Location on the network having a workstation-to-controller communications link, with additional controllers at the Location connected to the workstation-to-controller link with a TIA 485-A communications loop. Where this term is presented with an initial capital letter, this definition applies.

E. Workstation: Personal computer. Applies to the central station, workstations, and file servers.

F. RAS: Remote access services.

G. RF: Radio frequency.

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

I. TCP/IP: Transport control protocol/Internet protocol.

J. TWAIN: Technology without an Interesting Name. A programming interface that lets a graphics application, such as an image editing program or desktop publishing program, activate a scanner, frame grabber, or other image-capturing device.

K. WMP: Windows media player.

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

M. WYSIWYG: What You See Is What You Get. Text and graphics appear on the screen the same as they will in print.

1.4 ACTION SUBMITTALS

A. Product Data: For each type of product indicated. Include rated capacities, operating characteristics, and furnished specialties and accessories. Reference each product to a location on Drawings. Test and evaluation data presented in Product Data shall comply with SIA BIO-01.

B. Shop Drawings: Include plans, elevations, sections, details, and attachments to other work.

1. Diagrams for cable management system.
2. System labeling schedules, including electronic copy of labeling schedules that are part of the cable and asset identification system of the software specified in Parts 2 and 3.
3. Wiring Diagrams. For power, signal, and control wiring. Show typical wiring schematics.
4. Cable Administration Drawings: As specified in "Identification" Article.
5. Battery and charger calculations for central station, workstations, and controllers.

C. Product Schedules.

1.5 INFORMATIONAL SUBMITTALS

A. Field quality-control reports.

1.6 CLOSEOUT SUBMITTALS

A. Operation and Maintenance Data: For security system to include in emergency, operation, and maintenance manuals. In addition to items specified in Section 017823 "Operation and Maintenance Data," include the following:

1. Workstation operating system documentation.
2. Workstation installation and operating documentation, manuals, and software for the workstation and all installed peripherals. Software shall include system restore, emergency boot diskettes, and drivers for all installed hardware. Provide separately for each workstation.
3. Hard copies of manufacturer's specification sheets, operating specifications, design guides, user's guides for software and hardware, and PDF files on [**USB**] [**cloud**] media of the hard-copy submittal.
4. System installation and setup guides with data forms to plan and record options and setup decisions.

1.7 QUALITY ASSURANCE

A. Installer Qualifications: An employer of workers trained and approved by manufacturer.

B. Source Limitations: Obtain central station, workstations, controllers, Identifier readers, and all software through one source from single manufacturer.

1.8 DELIVERY, STORAGE, AND HANDLING

A. Central Station, Workstations, and Controllers:

1. Store in temperature- and humidity-controlled environment in original manufacturer's sealed containers. Maintain ambient temperature between 50 and 85 deg F (10 and 30 deg C), and not more than 80 percent relative humidity, noncondensing.
2. Open each container; verify contents against packing list; and file copy of packing list, complete with container identification, for inclusion in operation and maintenance data.
3. Mark packing list with the same designations assigned to materials and equipment for recording in the system labeling schedules that are generated by software specified in "Cable and Asset Management Software" Article.
4. Save original manufacturer's containers and packing materials and deliver as directed under provisions covering extra materials.

PART 2 - PRODUCTS

2.1 ACCESS CONTROL SOFTWARE

A. Manufacturers:
1. PDK – ProdataKey
2. MOTOROLA - Avigilon

2.2 DESCRIPTION

A. Security Access System: Workstation-based central station, one or more networked workstation-based workstations, and field-installed controllers, connected by a high-speed electronic-data transmission network.

B. System Software: Based on 128-bit encrypted cloud-based operating system and application software. Software shall have the following capabilities:

1. Multiuser and multitasking to allow for independent activities and monitoring to occur simultaneously at different workstations.
2. Graphical user interface to show pull-down menus and a menu-tree format that complies with interface guidelines of the operating system.
3. System license for the entire system including capability for future additions that are within the indicated system size limits specified in this Section.
4. Open-architecture system that allows importing and exporting of data and interfacing with other systems that are compatible with operating system.
5. Password-protected operator login and access.
6. Open-database-connectivity compliant.

C. Network connecting the central station and workstations shall be a LAN using TCP/IP with a capacity of connecting up to 99 workstations. System shall be portable across multiple communication platforms without changing system software.

D. Network(s) connecting workstations and controllers shall consist of one or more of the following:

1. Local area, IEEE 802.3 Fast Ethernet Gigabit-Ethernet, star topology network based on TCP/IP.
2. Local area, IEEE 802.11 compatible wireless mesh network, based on TCP/IP.
3. Direct-connected, RS-232 cable from the COM port of the central station to the first controller, then RS-485 cable to interconnect the remaining controllers at that Location.

2.3 OPERATION

A. Security access system shall use a single database for access-control and credential-creation functions.

B. Distributed Processing: A fully distributed processing system.

1. Access-control information, including time, date, valid codes, access levels, and similar data, shall be downloaded to controllers so each controller can make access-control decisions.
2. Intermediate controllers for access control are prohibited.
3. In the event that communications with the central controller are lost, controllers shall automatically buffer event transactions until communications are restored, at which time buffered events shall be uploaded to the central station.

C. Number of Locations:

1. Support at least 1,000 separate Locations using a single workstation with combinations of direct-connect, or TCP/IP LAN connections to each Location.
2. Each Location shall have its own database and history in the central station.
3. Locations may be combined to share a common database.

D. Data Capacity:

1. 130 different card-reader formats.
2. 999 comments.
3. 48 graphic file types for importing maps.

E. Location Capacity:

1. 1024 reader-controlled doors.
2. 50,000 total-access credentials.
   2048 supervised alarm inputs.
3. 2048 programmable outputs.
4. 32,000 custom action messages per Location to instruct operator on action required when alarm is received.

F. System Network Requirements:

1. System components shall be interconnected and shall 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 shall identify the communications 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.

G. 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.

H. Field equipment shall include controllers, sensors, and controls.

1. Controllers shall serve as an interface between the central station and sensors and controls.
2. Data exchange between the central station and the controllers shall include down-line transmission of commands, software, and databases to controllers.
3. 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.
4. Controllers are classified as alarm-annunciation or entry-control type.

I. System Response to Alarms:

1. Field device network shall provide a system end-to-end response time of one second(s) or less for every device connected to the system.
2. Alarms shall be annunciated at the central station within one second of the alarm occurring at a controller or at a device controlled by a local controller, and within 100 ms if the alarm occurs at the central station.
3. Alarm and status changes shall be displayed within 100 ms after receipt of data by the central station.
4. All graphics shall be displayed, including graphics-generated map displays, on the console monitor within five seconds of alarm receipt at the security console.
5. This response time shall be maintained during system heavy load.

J. False-Alarm Reduction: The design of the central station and controllers shall contain features to reduce false alarms. Equipment and software shall comply with SIA CP-01.

K. Error Detection:

1. Use a cyclic code method to detect single- and double-bit errors, burst errors of eight bits or fewer, and at least 99 percent of all other multibit and burst errors between controllers and the central station.
2. Interactive or product error-detection codes alone will not be acceptable.
3. A message shall be in error if one bit is received incorrectly.
4. Retransmit messages with detected errors.
5. Allow for an operator-assigned two-digit decimal number to each communications link representing the number of retransmission attempts.
6. Central station shall print a communication failure alarm message when the number of consecutive retransmission attempts equals the assigned quantity.
7. Monitor the frequency of data transmission failure for display and logging.

L. Data Line Supervision: System shall initiate an alarm in response to opening, closing, shorting, or grounding of data transmission lines.

M. Door Hardware Interface:

1. Comply with requirements in Section 087100 "Door Hardware" and Section 087111 "Door Hardware (Descriptive Specification)" for door hardware required to be monitored or controlled by the security access system.
2. Electrical characteristics of controllers shall match the signal and power requirements of door hardware.

2.4 PERFORMANCE REQUIREMENTS

A. Electrical Components, Devices, and Accessories: Listed and labeled as defined in NFPA 70, by a qualified testing agency, and marked for intended location and application.

B. Comply with NFPA 70, "National Electrical Code."

2.5 APPLICATION SOFTWARE

A. System Software: Based on Microsoft Windows central-station and workstation operating system and application software.

1. Multiuser multitasking shall allow independent activities and monitoring to occur simultaneously at different workstations.
2. Graphical user interface shall 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 login and access.

B. Peer Computer Control Software: Detect a failure of a central computer and cause the other central computer to assume control of all system functions without interruption of operation. Both central computers shall have drivers to support this mode of operation.

C. Application Software: Interface between the alarm annunciation and entry-control controllers to monitor sensors, operate displays, report alarms, generate reports, and help train system operators.

1. Reside 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 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 workstation. 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 workstation. This operation shall be at the controller.
7. Messages from workstation 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 workstation-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 and encrypted with a nine-character alphanumeric password that 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.
11. Support network protocol and topology, TCP/IP, Novel Netware, Digital Pathworks, Banyan Vines, LAN/WAN, and RAS.

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 autonomous, intelligent processing units.

    a. Controllers shall make decisions about access control, alarm monitoring, linking functions, and door-locking schedules for their operation, independent of other system components.
    b. Controllers shall be part of a fully distributed processing-control network.
    c. 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. 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 the 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. Up to 64 controllers connected to TIA 485-A 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 communication failure between the central station and a Location, there shall be no degradation in operations at the controllers at that Location.

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; 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 their 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. 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. After power is restored, following a power failure, startup software shall initiate self-test diagnostic routines, after which controllers shall resume normal operation.

h. After controller 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 TIA 485-A communications loop 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 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. Workstation-to-Controller Communications:

1. Central-station or workstation communications shall use the following:

a. Direct connection using serial ports of the workstation.
b. TCP/IP LAN interface cards.
c. Dial-up or cable modems for connections to Locations.

2. 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. Serial ports shall have adjustable data transmission rates and shall be selectable under program control.
3. Use multiport communications board if more than two serial ports are needed.

a. 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, cable, or satellite communications shall be alike in the monitoring or control of the system except for the connection that must first be made to a dial-up or voice-over IP Location.
5. TCP/IP network interface card (NIV) shall have an option to set the poll-frequency and message-response time-out settings.
6. Workstation-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 in this subparagraph shall be verified and buffered and retransmitted if not acknowledged.

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

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

H. Broadband Workstation-to-Controller Communications:

1. Communication software on the workstation shall supervise the workstation-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 or cable modem Locations, collecting event logs and verifying phone lines at operator-selectable time intervals for each Location.
3. System shall be programmable for dialing and connecting to all dial-up or cable 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 30 minutes.
4. Failure to communicate to a dial-up Location three times in a row shall result in an alarm at the workstation.
5. Time offset capabilities shall be present so that Locations in a different geographical time zone than the host workstation 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 workstation.
6. The controller connected to a dial-up or cable 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 or cable 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. TIA 485-A, four-wire, point-to-point, regenerative (repeater) communications network methodology.
2. TIA 485-A communications signal shall be regenerated at each controller.

J. Database Downloads:

1. All data transmissions from workstations 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 workstation. 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 1024 unique user accounts 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. Selected commands to be 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 one second.
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. Display Graphics: Used to show any graphic displays implemented in the system. Graphic displays shall be completed within 20 seconds from time of operator command.
i. Run system tests.
j. Generate and format reports.
k. 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 application program.

l. 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 two times a day through time-zone programming.
4) Enable or disable cards or codes up to four times a 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, or operator-response plans; unique sound with use of WAV files; and maps or images that graphically represent the point location.
c. Sixty-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.
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 four 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 the authorization level.
c. Maintain a transcript file of the last 5000 commands entered at 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 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 the same manner as burglar alarms, using a TIA 232-F 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.

O. 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 the 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 the same alarm point shall be acknowledged at the 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 the graphic map.
d. Inputs or outputs may be placed on multiple graphic maps. The operator shall be able to toggle to view graphic maps associated with I/Os.
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 the period; and the default printer.
2. Printing on Request: 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 su**ch** as door 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 who are "In" at a selected Location and a 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 data 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 allow 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 workstation.
    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, and 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 the 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 workstation (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 those access levels that have been designated as approved for visitors.
2. Provide an automated log of visitor name, time and doors accessed, and name of person contacted.
3. Allow a visitor designation to be assigned to a credential holder.
4. Security access system shall be able to restrict the access levels that may be assigned to credentials 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. Time and Attendance:

1. Time and attendance reporting shall be provided to match IN and OUT reads and display cumulative time in for each day and cumulative time in for length designated in the report.
2. Shall be provided to match IN and OUT reads and display cumulative time in for each day and cumulative time in for length designated in the report.
3. System software setup shall allow designation of selected access-control readers as time and attendance hardware to gather the clock-in and clock-out times of the users at these readers.

    a. Reports shall show in and out times for each day, total time in for each day, and a total time in for period specified by the user.
    b. Allow the operator to view and print the reports, or save the reports to a file.
    c. Alphabetically sort reports on the person's last name, by Location or location group. Include all credential holders or optionally select individual credential holders for the report.

V. 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.

W. 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 with which data must comply.
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 ASCII File Import Utility: Allows the importing of cardholder data and images.
11. Card Expire Function: Allows readers to be configured to deactivate cards when a card is used at selected devices.

2.6 SYSTEM DATABASE

A. Database and database management software shall define and modify each point in database using operator commands. Definition shall include parameters and constraints associated with each system device.

B. Database Operations:

1. System data management shall be in a hierarchical menu-tree format, with navigation through expandable menu branches and manipulated with use of menus and icons in a main menu and system toolbar.
2. Navigational Aids:

a. Toolbar icons for add, delete, copy, print, capture image, activate, deactivate, and muster report.
b. Point and click feature to facilitate data manipulation.
c. Next and previous command buttons visible when editing database fields to facilitate navigation from one record to the next.
d. Copy command and copy tool in the toolbar to copy data from one record to create a new similar record.

3. Data entry shall be automatically checked for duplicate and illegal data and shall be verified for valid format.
4. System shall generate a memo or note field for each item that is stored in database, allowing the storing of information about any defining characteristics of the item. Memo field is used for noting the purpose for which the item was entered, reasons for changes that were made, and the like.

C. File Management:

1. File management shall include database backup and restoration system, allowing selection of storage media, including 3.5-inch floppy disk, Zip and Jaz drives, and designated network resources.

2. Operations shall be both manual and automatic modes. The number of automatic sequential backups before the oldest backup will be overwritten; FIFO mode shall be operator selectable.
3. Backup program shall provide manual operation from any workstation on the LAN and shall operate while system remains operational.

D. Operator Passwords:

1. Support up to 32,000 individual system operators, each with a unique password.
2. Allow passwords to be case sensitive.
3. Passwords shall not be displayed when entered.
4. Passwords shall have unique and customizable password profile and allow several operators to share a password profile. Include the following features in the password profile:

    a. Predetermine the highest-level password profile for access to all functions and areas of program.
    b. Allow or disallow operator access to any program operation, including the functions of View, Add, Edit, and Delete.
    c. Restrict doors to which an operator can assign access.

5. Operators shall use a username and password to log on to system. This username and password shall be used to access database areas and programs as determined by the associated profile.
6. Make provision to allow the operator to log off without fully exiting program. User may be logged off, but program will remain running while displaying the login window for the next operator.

E. Access Card/Code Operation and Management: Access authorization shall be by card, by a manually entered code (PIN), or by a combination of both (card plus PIN).

1. Access authorization shall verify the facility code first, the card or card-and-PIN validation second, and the access level (time of day, day of week, date), anti-passback status, and number of uses last.
2. Use data-entry windows to view, edit, and issue access levels. Access-authorization entry-management system shall maintain and coordinate all access levels to prevent duplication or the incorrect creation of levels.
3. Allow assignment of multiple cards/codes to a cardholder.
4. Allow assignment of up to four access levels for each Location to a cardholder. Each access level may contain any combination of doors.
5. Each door may be assigned four time zones.
6. Access codes may be up to 11 digits in length.
7. Software shall allow the grouping of locations so cardholder data can be shared by all locations in the group.
8. Visitor Access: Issue a visitor badge for data tracking or photo ID purposes without assigning that person a card or code.
9. Cardholder Tracing: Allow for selection of cardholder for tracing. Make a special audible and visible annunciation at control station when a selected card or code is used at a designated code reader. Annunciation shall include an automatic display of the cardholder image.
10. Allow each cardholder to be given either an unlimited number of uses or a number from one to 9999 that regulates the number of times the card can be used before it is automatically deactivated.
11. Provide for cards and codes to be activated and deactivated manually or automatically by date. Provide for multiple deactivate dates to be preprogrammed.

F. Security Access Integration:

1. Photo ID badging and photo verification shall use the same database as the security access and may query data from cardholder, group, and other personal information to build a custom ID badge.
2. Automatic or manual image recall and manual access based on photo verification shall also be a means of access verification and entry.
3. System shall allow sorting of cardholders together by group or other characteristic for a fast and efficient method of reporting on, and enabling or disabling, cards or codes.

G. Key control and tracking shall be an integrated function of cardholder data.

1. Provide the ability to store information about which conventional metal keys are issued and to whom, along with key construction information.
2. Reports shall be designed to list everyone who possesses a specified key.

H. Facility Codes: System shall accommodate up to 2048 facility codes per Location, with the option of allowing facility codes to work at all doors or only at particular doors.

I. Operator Comments:

1. With the press of one appropriate button on the toolbar, the user shall be permitted to enter operator comments into the history at any time.
2. Automatic prompting of operator comment shall occur before the resolution of each alarm.
3. Operator comments shall be recorded by time, date, and operator number.
4. Comments shall be sorted and viewed through reports and history.
5. The operator may enter comments in two ways; either or both may be used:

    a. Manually entered through keyboard data entry (typed), up to 65,000 characters per each alarm.
    b. Predefined and stored in database for retrieval on request.

6. System shall have a minimum of 999 predefined operator comments with up to 30 characters per comment.

J. Group:

1. Group names may be used to sort cardholders into groups that allow the operator to determine the tenant, vendor, contractor, department, division, or any other designation of a group to which the person belongs.
2. System software shall have the capacity to assign one of 32,000 group names to an access authorization.
3. Make provision in software to deactivate and reactivate all access authorizations assigned to a particular group.
4. Allow sorting of history reports and code list printouts by group name.

K. Time Zones:

1. Each zone consists of a start and stop time for seven days of the week and three holiday schedules. A time zone is assigned to inputs, outputs, or access levels to determine when an input shall automatically arm or disarm, when an output automatically opens or secures, or when access authorization assigned to an access level will be denied or granted.
2. Up to four time zones may be assigned to inputs and outputs to allow up to four arm or disarm periods per day or four lock or unlock periods per day; up to three holiday override schedules may be assigned to a time zone.

3. Data-entry window shall display a dynamically linked bar graph showing active and inactive times for each day and holiday, as start and stop times are entered or edited.
4. System shall have the capacity for 2048 time zones for each Location.

L. Holidays:

1. Three different holiday schedules may be assigned to a time zone. Holiday schedule consists of date in format MM/DD/YYYY and a description. When the holiday date matches the current date of the time zone, the holiday schedule replaces the time-zone schedule for that 24-hour period.
2. System shall have the capacity for 32,000 holidays.
3. Three separate holiday schedules may be applied to a time zone.
4. Holidays have an option to be designated as occurring on the designated date each year. These holidays remain in the system and will not be purged.
5. Holidays not designated to occur each year shall be automatically purged from the database after the date expires.

M. Access Levels:

1. System shall allow for the creation of up to 32,000 access levels.
2. One level shall be predefined as the Master Access Level. The Master Access Level shall work at all doors at all times and override any anti-passback.
3. System shall allow for access to be restricted to any area by reader and by time. Access levels shall determine when and where an Identifier is authorized.
4. System shall be able to create multiple door and time-zone combinations under the same access level so that an Identifier may be valid during different time periods at different readers even if the readers are on the same controller.

N. User-Defined Fields:

1. System shall provide a minimum of 99 user-defined fields, each with up to 50 characters, for specific information about each credential holder.
2. System shall accommodate a title for each field; field length shall be 20 characters.
3. A "Required" option may be applied to each user-defined field that, when selected, forces the operator to enter data in the user-defined field before the credential can be saved.
4. A "Unique" option may be applied to each user-defined field that, when selected, will not allow duplicate data from different credential holders to be entered.
5. Data format option may be assigned to each user-defined field that will require the data to be entered with certain character types in specific spots in the field entry window.
6. A user-defined field, if selected, will define the field as a deactivate date. The selection shall automatically cause the data to be formatted with the windows MM/DD/YYYY date format. The credential of the holder will be deactivated on that date.
7. A search function shall allow any one user-defined field or combination of user-defined fields to be searched to find the appropriate cardholder. The search function shall include a search for a character string.
8. System shall have the ability to print cardholders based on and organized by the user-defined fields.

O. Code Tracing:

1. System shall perform code tracing selectable by cardholder and by reader.
2. Any code may be designated as a "traced code" with no limit to how many codes can be traced.
3. Any reader may be designated as a "trace reader" with no limit to which or how many readers can be used for code tracing.

4. When a traced code is used at a trace reader, the access-granted message that usually appears on the monitor window of the central station shall be highlighted with a different color than regular messages. A short singular beep shall occur at the same time the highlighted message is displayed on the window.
5. The traced cardholder image (if image exists) shall appear on workstations when used at a trace reader.

2.7 SURGE AND TAMPER PROTECTION

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

1. Minimum Protection for Power Connections 120 V and More: Auxiliary panel suppressors complying with requirements in Section 264313 "Surge Protection for Low-Voltage Electrical Power Circuits."
2. Minimum Protection for Communication, Signal, Control, and Low-Voltage Power Connections: Comply with requirements in Section 264313 "Surge Protection for Low-Voltage Electrical Power Circuits" as recommended by manufacturer for type of line being protected.

B. Tamper Protection: Tamper switches on enclosures, control units, pull boxes, junction boxes, cabinets, and other system components shall initiate a tamper-alarm signal when unit is opened or partially disassembled. Control-station control-unit alarm display shall identify tamper alarms and indicate locations.

2.8 CENTRAL-STATION HARDWARE

A. Central-Station Computer: Standard workstation of modular design.

B. Redundant Central Computer: One identical redundant central computer, connected in a hot standby, peer configuration. This computer shall automatically maintain its own copies of system software, application software, and data files. System transactions and other activities that alter system data files shall be updated to system files of redundant computer in near real time. If central computer fails, redundant computer shall assume control immediately and automatically.

C. Servers:

1. Web Server:

a. If required to be separate, include Web server hardware and software to match, except backup server is not required.
b. Firewalls between server Web and networks.
c. Password protection for access to server from Web server.
d. Cable installation between the server(s) and building Ethernet network.

2.9 FIXED MAP DISPLAY

A. A fixed map display shall show layout of the protected facilities. Zones corresponding to those monitored by the system shall be highlighted on the display. Status of each zone shall be displayed using digital displays as required within each designated zone. A digital display test switch shall be provided on the map display.

2.10 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, lithium-ion; sized to provide run time during a power outage of 90 minutes, complying with UL 924.

D. Alarm Annunciation Controller:

1. The controller shall automatically restore communication within 10 seconds after an interruption with the field device network**,** with dc line supervision on each of its alarm inputs.

a. Inputs: Monitor dry contacts for changes of state that reflect alarm conditions. Provides at least eight alarm inputs, which are suitable for wiring as normally open or normally closed contacts for alarm conditions.
b. Alarm-Line Supervision:

1) Supervise the alarm lines by monitoring each circuit for changes or disturbances in the signal, and for conditions as described in UL 1076 for line security equipment by monitoring for abnormal open, grounded, or shorted conditions using dc change measurements. System shall initiate an alarm in response to an abnormal current, which is a dc change of 5 percent or more for longer than 500 ms.
2) Transmit alarm-line-supervision alarm to the central station during the next interrogation cycle after the abnormal current condition.

c. Outputs: Managed by central-station software.

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 personnel 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 are not 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.
c. Maintain a date-, time-, and Location-stamped record of each transaction and transmit transaction records to the central station.
d. Door Prop Alarm: If a portal is held open for longer than 20 seconds alarm sounds.

4. With power supplies sufficient to power at voltage and frequency required for field devices and portal-control devices.
5. Data Line Problems: For periods of loss of communication with the central station, or when data transmission is degraded and generating continuous checksum errors, the controller shall continue to control entry by accepting identifying information, making authentication decisions, checking privileges, and controlling portal-control devices.

a. Store up to 1000 transactions during periods of communication loss between the controller and access-control devices for subsequent upload to the central station on restoration of communication.

6. Controller Power: NFPA 70, Class II power-supply transformer, with 12- or 24-V ac secondary, backup battery and charger.

a. Backup Battery: Valve-regulated, recombinant-sealed, lead-calcium battery; spill proof; with a full one-year warranty and a pro rata 3-year warranty. With single-stage, constant-voltage-current, limited battery charger, comply with battery manufacturer's written instructions for battery terminal voltage and charging current recommendations for maximum battery life.
b. Backup Battery: Valve-regulated, recombinant-sealed, lead-acid battery; spill proof. With single-stage, constant-voltage-current, limited battery charger, comply with battery manufacturer's written instructions for battery terminal voltage and charging current recommendations for maximum battery life.
c. Backup Power-Supply Capacity: 90-minutes of battery supply. Submit battery and charger calculations.
d. Power Monitoring: Provide manual, dynamic battery-load test, initiated, and monitored at the control center; with automatic disconnection of the controller when battery voltage drops below controller limits. Report by using local controller-mounted digital displays and by communicating status to central station. Indicate normal power on and battery charger on trickle charge. Indicate and report the following:

1) Trouble Alarm: Normal power-off load assumed by battery.
2) Trouble Alarm: Low battery.

3) Alarm: Power off.

2.11 ENROLLMENT CENTER

A. Equipment for enrolling personnel into, and removing personnel from, system database, using a dedicated desktop workstation

1. Include equipment to enroll selected biometric credentials.

B. Enrollment equipment shall support encoding of credential cards including cryptographic and other internal security checks as required for system.

1. Allow only authorized entry-control enrollment personnel to access the enrollment equipment using passwords.
2. Include enrollment-subsystem configuration controls and electronic diagnostic aids for subsystem setup and troubleshooting with the central station.
3. Enrollment-station records printer shall meet requirements of the report printer.

C. Entry-Control Enrollment Software:

1. Shall include database management functions for the system and shall allow an operator to change and modify the data entered in the system as needed.
2. Software shall not have alarm response or acknowledgment functions as a programmable function.
3. Multiple, password-protected access levels shall be provided at the enrollment station.
4. Database management and modification functions shall require a higher operator-access level than personnel enrollment functions.
5. Software shall provide a means for disabling the enrollment station when it is unattended, to prevent unauthorized use.
6. Software shall provide a method to enter personnel identifying information into the entry-control database files through enrollment stations to include a credential unit in use at the installation.
7. In the case of personnel identity-verification subsystems, this data shall include biometric data.
8. Software shall allow entry of this data into the system database files through the use of simple menu selections and data fields. The data field names shall be customized to suit user and site needs.
9. 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.

D. System Capacity: Number of badges shall be limited only by hard disk space. Badge templates and images shall be in color, supporting the maximum color capability of workstation operating system.

E. Badge Configuration:

1. Software for badge template creation shall include a template consisting of background and predetermined locations of photographs, text objects and data fields for text, and bar-code and biometric information. Include automatic sizing of data fields placed on a badge to compensate for names, which may otherwise be too large to fit in the area designated.
2. Allow different badge templates to be used for each department, tenant, or visitor.
3. As a setup option, templates shall be automatically selected for the badge, based on the group to which the credential holder is assigned. Allow the operator to override the

automatic template selection and use a template chosen by the operator for creating a badge.

4. Setup shall determine which graphics and credential-holder information will be displayed and where on the card it will be placed. All data in the security access system, such as name, code, group, access level, and any of the 99 user-defined fields, shall be selectable, with the ability to place them anywhere on the card.
5. System shall include an importing, filing, and recall system of stored images and shapes that can be placed on the badge.
6. Allow multiple images on the same badge, including, but not limited to, bar codes, digital photos, and signatures.
7. Support transparent backgrounds so that image is only surrounded by the intended background and not by its immediate background.

F. Photo Imaging: Integral to security access.

1. Import images from bitmap file formats, digital cameras, TWAIN cameras, or scanners. Allow image cropping and editing, WYSIWYG badge-building application, and badge print-preview and printing capabilities.
2. System shall support multiple images stored for each credential holder, including signatures, portrait views, and profile views.

G. Text Objects: Badge configuration shall provide for creation of custom text as an object, allowing font selection, typing, scaling, and formatting of the text object. Formatting options shall include changing font, font size, text flow, and text alignment; bending or curving the text object into a circle or semicircle; applying 3-D effects; and applying predefined effects such as tilt, extrusion, or beveling. Text shall be placed and optionally automatically centered within any region of the badge layout.

H. Badges and Credential Cards:

1. Badges are credential cards that do not contain data to be read by card readers.
2. Credential cards shall store uniquely coded data used by card readers as an Identifier.

    a. Magnetic-Stripe Cards: Comply with ISO/IEC 7810, ISO/IEC 7811-1, ISO/IEC 7811-2, ISO/IEC 7811-6, and ISO/IEC 7811-7. Use single-layer magnetic tape material that is coated with a plastic, slick protective coat and affixed to the back of the credential card near the top.
    b. Wiegand Wire-Effect Cards: Ferromagnetic wires laminated into the credential card using binary digits specified for Wiegand readers to generate a unique credential card identification code.
    c. Proximity Cards: Use proximity detection without physical contact with the reader for proper operation.

3. Allow entry-control card to be modified by lamination or direct print process during the enrollment process for use as a picture and identification badge without reduction of readability. The design shall allow for the addition of at least one slot or hole to accommodate the attachment of a clip for affixing the credential card to the type of badge holder used at the site.

    a. Card Size and Dimensional Stability: Standard size, 2-1/8 by 3-3/8 inches dimensionally stable so that an undamaged card with deformations resulting from normal use shall be readable by the card reader.
    b. Card Material: Abrasion resistant, nonflammable, and nontoxic; and impervious to solar radiation and effects of ultraviolet light.

c. Card Construction: Core and laminate or monolithic construction. Lettering, logos, and other markings shall be hot stamped into the credential material or direct printed.
   1) Furnish equipment for on-site assembly and lamination of credential cards.

d. Card Durability and Maintainability: Designed and constructed to yield a useful lifetime of at least five years or 5000 insertions or swipes, whichever results in a longer period of time. Allow credential cards to be cleaned by wiping with a sponge or cloth wetted with soap and water.

2.12 HARDWARE INTERFACE

A. Exit Device with Alarm: Operation of the exit device shall generate an alarm and annunciate a local alarm. Exit device and alarm contacts are specified in Section 087100 "Door Hardware."

B. Exit Alarm: Operation of a monitored door shall generate an alarm. Exit devices and alarm contacts are specified in Section 087100 "Door Hardware."

C. Electric Door Strikes: Use end-of-line resistors to provide power-line supervision. Signal switches shall transmit data to controller to indicate when the bolt is not engaged and the strike mechanism is unlocked, and they shall report a forced entry. Power and signal shall be from the controller. Electric strikes are specified in Section 087100 "Door Hardware."

D. Electromagnetic Locks: End-of-line resistors shall provide power-line supervision. Lock status sensing signal shall positively indicate door is secure. Power and signal shall be from the controller. Electromagnetic locks are specified in Section 087100 "Door Hardware."

2.13 FIELD-PROCESSING SOFTWARE

A. Operating System:

1. Local processors shall contain an operating system that controls and schedules that local processor's activities in real time.
2. Local processor shall maintain a point database in its memory that includes parameters, constraints, and the latest value or status of all points connected to that local processor.
3. Execution of local processor application programs shall utilize the data in memory resident files.
4. Operating system shall include a real-time clock function that maintains the seconds, minutes, hours, date, and month, including day of the week.
5. Local processor real-time clock shall be automatically synchronized with the central station at least once per day to plus or minus 10 seconds (the time synchronization shall be accomplished automatically, without operator action and without requiring system shutdown).

B. Startup Software:

1. Causes automatic commencement of operation without human intervention, including startup of all connected I/O functions.
2. Local processor restart program based on detection of power failure at the local processor shall be included in the local processor software.
3. Initiates operation of self-test diagnostic routines.
4. Upon failure of the local processor, if the database and application software are no longer resident, the local processor shall not restart, and systems shall remain in the failure mode indicated until the necessary repairs are made.

5. If the database and application programs are resident, the local processor shall immediately resume operation.

C. Operating Mode:

1. Local processors shall control and monitor inputs and outputs as specified, independent of communications with the central station or designated workstations.
2. Alarms, status changes, and other data shall be transmitted to the central station or designated workstations when communications circuits are operable.
3. If communications are not available, each local processor shall function in a stand-alone mode and operational data, including the status and alarm data normally transmitted to the central station or designated workstations, shall be stored for later transmission to the central station or designated workstations.
4. Storage for the latest 4000 events shall be provided at local processors, as a minimum.
5. Local processors shall accept software downloaded from the central station.
6. Panel shall support flash ROM technology to accomplish firmware downloads from a central location.

D. Failure Mode: Upon failure for any reason, each local processor shall perform an orderly shutdown and force all local processor outputs to a predetermined (failure-mode) state, consistent with the failure modes shown and the associated control device.

E. Functions:

1. Monitoring of inputs.
2. Control of outputs.
3. Reporting of alarms automatically to the central station.
4. Reporting of sensor and output status to central station upon request.
5. Maintenance of real time, automatically updated by the central station at least once a day.
6. Communication with the central station.
7. Execution of local processor resident programs.
8. Diagnostics.
9. Download and upload data to and from the central station.

2.14 FIELD-PROCESSING HARDWARE

A. Alarm Annunciation Local Processor:

1. Respond to interrogations from the field device network, recognize and store alarm status inputs until they are transmitted to the central station, and change outputs based on commands received from the central station.
2. Local processor shall also automatically restore communication within 10 seconds after an interruption with the field device network and provide dc line supervision on each of its alarm inputs.
3. Local processor inputs shall monitor dry contacts for changes of state that reflect alarm conditions.
4. Local processor shall have at least eight alarm inputs which allow wiring contacts as normally open or normally closed for alarm conditions; and shall provide line supervision for each input by monitoring each input for abnormal open, grounded, or shorted conditions using dc current change measurements.
5. Local processor shall report line supervision alarms to the central station.
6. Alarms shall be reported for any condition that remains abnormal at an input for longer than 500 milliseconds.

7. Alarm condition shall be transmitted to the central computer during the next interrogation cycle.
8. Local processor outputs shall reflect the state of commands issued by the central station.
9. Outputs shall be a form C contact and shall include normally open and normally closed contacts.
10. Local processor shall have at least four command outputs.
11. Local processor shall be able to communicate with the central station via RS-485 or TCP/IP as a minimum.

B. Processor Power Supply:

1. Local processor and sensors shall be powered from an uninterruptible power source.
2. Uninterruptible power source shall provide eight hours of battery back-up power in the event of primary power failure and shall automatically fully recharge the batteries within 12 hours after primary power is restored.
3. If the facility is without an emergency generator, the uninterruptible power source shall provide 24 hours of battery backup power.
4. There shall be no equipment malfunctions or perturbations or loss of data during the switch from primary to battery power and vice versa.
5. Batteries shall be sealed, non-outgassing type.
6. Power supply shall be equipped with an indicator for ac input power and an indicator for dc output power.
7. Loss of primary power shall be reported to the central station as an alarm.

C. Auxiliary Equipment Power: A GFI service outlet shall be furnished inside the local processor's enclosure.

D. Entry-Control Local Processor:

1. Entry-control local processor shall respond to interrogations from the field device network, recognize and store alarm status inputs until they are transmitted to the central station, and change outputs based on commands received from the central station.
2. Local processor shall also automatically restore communication within 10 seconds after an interruption with the field device network and provide dc line supervision on each of its alarm inputs.
3. Entry-control local processor shall provide local entry-control functions including communicating with field devices such as card readers, keypads, biometric personnel identity-verification devices, door strikes, magnetic latches, gate and door operators, and exit push buttons.
4. Processor shall also accept data from entry-control field devices as well as database downloads and updates from the central station that include enrollment and privilege information.
5. Processor shall send indications of successful or failed attempts to use entry-control field devices and shall make comparisons of presented information with stored identification information.
6. Processor shall grant or deny entry by sending control signals to portal-control devices and mask intrusion-alarm annunciation from sensors stimulated by authorized entries.
7. Entry-control local processor shall use inputs from entry-control devices to change modes between access and secure.
8. Local processor shall maintain a date-time- and location-stamped record of each transaction and transmit transaction records to the central station.
9. Processor shall operate as a stand-alone portal controller using the downloaded database during periods of communication loss between the local processor and the central station.
10. Processor shall store a minimum of 4000 transactions during periods of communication loss between the local processor and the central station for subsequent upload to the central station upon restoration of communication.

11. Local processor inputs shall monitor dry contacts for changes of state that reflect alarm conditions.
12. Local processor shall have at least eight alarm inputs which allow wiring contacts as normally open or normally closed for alarm conditions; and shall also provide line supervision for each input by monitoring each input for abnormal open, grounded, or shorted conditions using dc current change measurements.
13. Local processor shall report line supervision alarms to the central station.
14. Alarms shall be reported for any condition that remains abnormal at an input for longer than 500 ms.
15. Alarm condition shall be transmitted to the central station during the next interrogation cycle.
16. Entry-control local processor shall include the necessary software drivers to communicate with entry-control field devices. Information generated by the entry-control field devices shall be accepted by the local processor and automatically processed to determine valid identification of the individual present at the portal.
17. Upon authentication of the credentials or information presented, the local processor shall automatically check privileges of the identified individual, allowing only those actions granted as privileges.
18. Privileges shall include, but are not limited to, time of day control, day of week control, group control, and visitor escort control. The local processor shall maintain a date-time- and location-stamped record of each transaction.
19. 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.
20. Local processor outputs shall reflect the state of commands issued by the central station.
21. Outputs shall be a form C contact and shall include normally open and normally closed contacts.
22. Local processor shall have at least four addressable outputs.
23. The entry-control local processor shall also provide control outputs to portal-control devices.
24. Local processor shall be able to communicate with the central station via RS-485 or TCP/IP as a minimum.
25. The system manufacturer shall provide strategies for downloading database information for panel configurations and cardholder data to minimize the required download time when using IP connectivity.

2.15 TIA 232-F ASCII INTERFACE SPECIFICATIONS

A. ASCII interface shall allow TIA 232-F connections to be made between the control station operating as the host workstation and any equipment that will accept TIA 232-F ASCII command strings, such as CCTV switches, intercoms, and paging systems.

1. Alarm inputs in system shall allow for individual programming to output up to four unique ASCII character strings through two different COM ports on the host workstation.
2. Inputs shall have the ability to be defined to transmit a unique ASCII string for alarm and one for restore through one COM port, and a unique ASCII string for a nonalarm, abnormal condition and one for a normal condition through the same or different COM port.
3. Predefined ASCII character strings shall have the ability to be up to 420 characters long with full use of all the ASCII control characters, such as return or line feed. Character strings shall be defined in the system database and then assigned to the appropriate inputs.
4. COM ports of the host workstation used to interface with external equipment shall be defined in the setup portion of the software. COM port's baud rate, word length, stop bits, and parity shall be definable in the software to match that of the external equipment.

B. Pager-System Interface: Alarms shall be able to activate a pager system with customized message for each input alarm.

1. TIA 232-F output shall be capable of connection to a pager interface that can be used to call a paging system or service and send a signal to a portable pager. System shall allow an individual alphanumeric message per alarm input to be sent to the paging system. This interface shall support both numeric and alphanumeric pagers.

C. Alarm-System Interface:

1. TIA 232-F output shall be capable of transmitting alarms from other monitoring and alarm systems to central-station automation software.
2. Alternatively, alarms that are received by this access-control system are to be transferred to the alarm automation system as if they were sent through a digital alarm receiver.

a. System shall be able to transmit an individual message from any alarm input to a burglar-alarm automation monitoring system.
b. System shall be able to append to each message a predefined set of character strings as a prefix and a suffix.

2.16 TRANSFORMERS

A. NFPA 70, Class II control transformers, NRTL listed. Transformers for security access-control system shall not be shared with any other system.

2.17 CABLE AND ASSET MANAGEMENT SOFTWARE

A. Computer-based cable and asset management system, with fully integrated database and graphic capabilities, complying with requirements in TIA 606-B.

1. Document physical characteristics by recording the network, asset, user, TIA details, device configurations, and exact connections between equipment and cabling.

a. Manage the physical layer of security system.
b. List device configurations.
c. List and display circuit connections.
d. Record firestopping data.
e. Record grounding and bonding connections and test data.

2. Information shall be presented in database view, schematic plans, or technical drawings.

a. Microsoft Visio Technical Drawing shall be used as drawing and schematic plans software. Drawing symbols, system layout, and design shall comply with SIA/IAPSC AG-01.

3. System shall interface with the following testing and recording devices:

a. Direct-upload tests from circuit testing instrument into the workstation.
b. Direct-download circuit labeling into labeling printer.

B. Software shall be designed of the same version as security access system's central station and workstations and shall be installed on the designated workstation, using a hard drive dedicated only to this management function.

PART 3 - EXECUTION

3.1 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 workstations, 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.

3.2 PREPARATION

A. Comply with recommendations in SIA CP-01.

B. Comply with TIA 606-B, "Administration Standard for Commercial Telecommunications Infrastructure."

C. Product Schedules: Obtain detailed product schedules from manufacturer of access-control system or develop product schedules to suit Project. Fill in all data available from Project plans and specifications and publish as Product Schedules 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, facility codes, 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 Visio Technical Drawings in electronic format.

D. In meetings with Architect and Owner, present Product Schedules and review, adjust, and prepare final setup documents. Use approved, final Product Schedules to set up system software.

3.3 DENTIFICATION

A. In addition to requirements in this article, comply with applicable requirements in Section 270553 "Identification for Communications Systems" and with TIA 606-B.

B. Using software specified in "Cable and Asset Management Software" Article, develop cable administration drawings for system identification, testing, and management. Use unique, alphanumeric designation for each cable, and label cable and jacks, connectors, and terminals to which it connects with the same designation. Use logical and systematic designations for facility's architectural arrangement.

C. Label each terminal strip and screw terminal in each cabinet, rack, or panel.

1. All wiring conductors connected to terminal strips shall be individually numbered, and each cable or wiring group being extended from a panel or cabinet to a building-mounted device shall be identified with the name and number of the particular device as shown.
2. Each wire connected to building-mounted devices is not required to be numbered at the device if the color of the wire is consistent with the associated wire connected and numbered within the panel or cabinet.

D. At completion, cable and asset management software shall reflect as-built conditions.

3.4 SYSTEM SOFTWARE AND HARDWARE

A. Develop, install, and test software and hardware, and perform database tests for the complete and proper operation of systems involved. Assign software license to Owner.

3.5 STARTUP SERVICE

A. Engage a factory-authorized service representative to supervise and assist with startup service.

1. Complete installation and startup checks according to approved procedures that were developed in "Preparation" Article and with manufacturer's written instructions.
2. Enroll and prepare badges and access cards for Owner's operators, management, and security personnel.

3.6 DEMONSTRATION

A. Train Owner's maintenance personnel to adjust, operate, and maintain security access system.

B. 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.

END OF SECTION 281300