SECTION 00 90 01

BIDDING AND CONTRACT REQUIREMENTS
ADDENDUM NUMBER (1)
February 22, 2021

Demonica Kemper Architects
125 N. Halsted Street, Suite 301
Chicago, IL 60661
312.496.0000

To: Prospective Bidders

Re: ADDENDUM NUMBER (1) TO THE BIDDING DOCUMENTS:

Illinois Valley Community College
Key Card Access Upgrades
Architect's Project Number: 20-026

This addendum forms a part of the bidding and contract documents and modifies the original bidding documents dated February 01, 2021. Acknowledge receipt of this addendum in the space provided on Bid Form. FAILURE TO DO SO MAY SUBJECT BIDDER TO DISQUALIFICATION.

ADDENDA TO THE PROJECT MANUAL

1. Section 28 10 00 Access Control Specification
    a. PART 2 – Products; 2.1 Manufactures – B. Item# 4 – Alternate manufactures shall be submitted to the architect for review during bidding.
    Suggested Alternate: I would like to seek approval for the use of Schneider Electric – Access Xpert (Version3) as an approved manufacture for the access control system. See attached specification sheet.

        i. **ADDED** Schneider Electric – Access Xpert (Version3) is an approved Alternate.

2. Section 28 10 00 Access Control Specification
    a. 2.1-C – Added item #2 to clarify no ongoing (ie. Annual) maintenance or licensing agreements shall be accepted.
    b. 2.2-B – removed desktop form factor.
    c. 2.2-C – removed this section. System shall be server based.
    d. 2.4-A – removed 1-4. 256+ base card reader system shall be provided.
    e. 2.5 – removed this section. System shall not be a virtual system.
    f. Part 3 – Removed previous Part 3 Execution section in entirety and replaced with updated section

3. **ADDED** Specification 28 13 00 - Access Control Hardware Devices

ADDENDA TO THE DRAWINGS

Electrical Drawings

1. E1-10
    a. Revised tags for (one each) request to exit button and mag lock to RN and EX respectively.

2. E2-10
    a. Building D - Updated location of (one) card reader to match existing back box.
    b. Building D – Added 'NI' and 'EX' tags to one set of door equipment.
    c. Building A – Added 'NI' tag to request to exit button.
    d. Building C – Added note to clarify card access management hardware/software installation location.
    e. Added general note 5 and 5.1.
3. E3-00
    a. Revised duplex outlet to simplex outlet with CAT6 cable.
    b. Updated card access, motion sensor and request to exit button symbols to refer to specifications.
    c. Updated motion sensor symbol to clarify it is a request to exit motion sensor.
    d. Added wiring diagram for BOD product.
    e. Added door strike manufacturer to door strike symbol.

CLARIFICATIONS

Q1: If we're pulling the cable, does it need to be plenum?

A1: Provide plenum in plenum ceilings.

Q2: Are we using cable trays j-hooks or bridle rings?

A2: Utilize existing cable tray where provided, provide j-hooks where cable tray does not exist.

Q3: Can the controllers be installed in the idf or mdf closets?

A3: This would be acceptable pending approval of the exact location by the Owner's IT representative. If the location is not approved, the existing location on the drawings will be required.

Q4: Rack or wall mount?

A4: Wall Mount.

Q5: We only need to provide locks if they are new? All existing locks will stay or be reused?

A5: Existing electronic door strikes/latches and mag locks will be re-used. There are locations called out where new door strikes are required.

Q6: What types of ceilings are they?

A6: Ceiling types vary across the campus. This will need to be verified by the contractor on site.

Q7: Are the door frames filled?

A7: We don't have this information. Frames will need to be field verified.

Q8: How many total doors?

A8: Doors are indicated on the drawings.

Q9: Should the new BID include reusing the old cable or just the alternative?

A9: Refer to the bid documents

Q10: We need to relocate the controller outside the door in the hallway, will this be for the duration of the construction or permanent?

A10: This is permanent for all rooms with mag locks and a controller inside. Quantities and locations can be seen on the drawings.

Q11: Are there door contacts (door status switches) installed on any doors and or in use on any doors, interior or exterior?

A11: There are several doors with contacts. Existing hardware on doors is to be integrated per the drawings.

Q12: Is a dual data drop using Cat6A required at each access control panel location?

A12: Simplex CAT6 data drop can be provided. Refer to upcoming addendum.

Q13: Are all existing access control doors fully functional with the exception of the locations being removed?

A13: Existing access doors are functional with the exception of the locations being removed.

Q14: The demo prints (example listed below Figure-1) show a dotted square as a headend controller for access control. Additionally there are circled 'D' symbols to be removed and noted as door controllers. Can you elaborate as to what the 'D' controller is?

A14: The circled D locations indicate door controllers (typically 2 door) fed from the main head end controller for each building.

Q15: Is all new cable being installed required to be plenum rated?

A15: Plenum cable is only required in plenum ceilings.

Q16: If any panel locations (new or existing) require 120VAC, who will be providing the power?

A16: Contractor is responsible for providing power. Refer to upcoming addendum. All buildings have power existing power available except for building G and the maintenance building.

Q17: Some of the access control hardware will require network connectivity. If the existing network hardware in the MDF/IDF does not have open switch ports, who is required to provide the additional hardware?

A17: There is space in the existing network hardware, but the contractor would be required to provide additional switches.

Q18: Figure-2 shows the card reader seen on site. Is this reader in Figure-2 typical or are there other styles throughout the campus?

A18: These are typical throughout most buildings. The CTC building and portions of building J have mullion style readers. Several satellite buildings have one or two mullion style readers as well.

Q19: Is cable demo required if recabling card access doors?

A19: Yes, cabling demo is required.

Q20: If demo of cable is required, is full demo required or just into the ceiling space?

A20: Full demolition of cable is required.

Attachments

Project Manual:
28 10 00 Access Control
28 15 00 Access Control Hardware Devices

Drawings:
E1.10
E2.10
E3.00

Pre-Bid Sign-in Sheet
Pre-Bid Meeting Minutes

END OF SECTION 00 90 01

SECTION 28 10 00 - ACCESS CONTROL

PART 1 GENERAL

1.1 SECTION INCLUDES:

A. Physical Access Control System (PACS).

B. PACS Appliance.

C. PACS Software.

1.2 ADMINISTRATIVE REQUIREMENTS

A. Coordination:
   1. Coordinate with Owner or Owner's representative regarding network configuration and estimated bandwidth utilization prior to performing network connections.

B. Sequencing / Scheduling: Provide to Owner or Owner's representative a schedule and list of participants required to attend coordination and progress update meetings.
   1. Owner representative(s) for Facilities Management, Information Technology (IT) Services, and Security Management.
   2. General Contractor.
   3. Project Manager.
   4. Manufacturer's Representative.

1.3 INFORMATIONAL SUBMITTALS

A. Product Data: Manufacturer's product information and data sheets for each product specified in this section, including:
   1. Substrate preparation instructions and recommendations
   2. Installation means and methods.
   3. Recommendations and requirements for proper storage and handling.

B. Warranty Information:
   1. Submit confirmation and details of manufacturer's warranty, extended warranty, and replacement policies.

C. System Support Resources:
   1. Submit a list of available manufacturers providing fee based professional services available to the Contractor or Owner, including but not limited to the following:
      a. Training.

b. Installation.
c. Commissioning.
d. Remote diagnostics and integration with 3rd party software and hardware systems.

1.4 CLOSEOUT SUBMITTALS

A. Supply licensing and registration information for all software, hardware, firmware, operational, and administrative licenses.

B. Supply network configuration backup files, restoration application and instructions.

1.5 MAINTENANCE SUBMITTALS

A. Spare Parts: All Spare Parts must be delivered to the owner in their original sealed packaging. Clearly label with "SPARE: DO NOT REMOVE", and include manufacturer part numbers, and date of delivery to Owner. Store all spare parts in an environment and condition recommended by the manufacturer.
1. One spare for each 50 devices.
2. Provide spare components as noted in the coordinating schedule for work listed in this section.

1.6 QUALITY ASSURANCE

A. Qualifications - Manufacturers: Manufacturer(s) suppling products noted in this section must have a minimum of 5 years in business.

B. Qualifications - Installers:
1. Installer must be licensed to install security equipment as required by authority having jurisdiction.
2. Installer must be capable of providing references that will attest to successful completion of projects of similar scope as the work noted in this section.
3. Installer must be certified by the manufacturer and be up to date with all training required to maintain good standing.

C. Mock-Ups: Provide a mock-up for evaluation of installer's workmanship.
1. Do not proceed with remaining Work until workmanship is approved by Architect.
2. Refinish mock-up area as required to produce acceptable work.

1.7 WARRANTY

A. Manufacturer Warranty: Provide manufacturer's warranty covering parts and labor costs to repair or replace part that fail to perform.
1. Warranty Period: Parts and labor warranty for 24 months from date of Substantial Completion or date of purchase, whichever comes first.

2. Service During Warranty: Provide direct support to Owner via phone and email, including access to training and education in the form of documents, videos and other materials via the internet.

PART 2 PRODUCTS

2.1 MANUFACTURERS

A. Basis of Design Manufacturer: Avigilon.

B. Provide products by one of the following:
   1. Avigilon
   2. RS2 Technologies
   3. MonitorCast
   4. Alternate manufacturers shall be submitted to architect for review during bidding.

C. Substitution Limitations:
   1. Single manufacturer will provide, from a single source, a fully integrated
      a. Access Control Software and Database Management.
   2. **Substituted hardware and software shall not include or require an ongoing maintenance or licensing agreement to provide the services included in this specification.**

2.2 ACCESS CONTROL MANAGER (ACM) SYSTEM DESCRIPTION

A. Description: Access Control Manager (ACM) software provides an expandable, role-based system that has the following features:
   1. Compatibility with existing IT systems.
   2. Manages permissions centrally, from a single location.
   3. Integrates with Active Directory, HR databases, and other IT and logical security systems.
   4. Provides browser-based solutions allow full access from other devices, enabling security personnel to respond to an incident immediately.
   5. Integrates with Avigilon Control Center
   6. Does not require installation on multiple workstations.
   7. Supports open field hardware from other manufacturers.
   8. Provides hot-standby or auto-failover through cloud-based server architecture, switching to backup system automatically in the event of a fatal failure.

B. Server Appliance: Linux based server pre-loaded with Avigilon Access Manager Software and optimized to manage an IP-based access control system.
   1. Form Factor: Rack mounted

2. Form Factor: Desktop tower.

C. ~~Virtual Appliance: Bundled as either an on-site, or private cloud solution within the Owner's virtualized environment.~~

D. Products Supported: Provide ACM which supports the following third-party products with the compatible drivers, firmware, and software as required to provide a fully functional system:
   1. Access Hardware:
      a. Mercury Security: Products bearing the "Authentic Mercury" mark.
      b. HID Global: VertX Evo controllers and VerteX Sub Panel.
   2. Reader Hardware:
      a. Refer to symbol list
   3. Power Supplies: Provide one of the following power supplies that are manufacturer prepared to support Mercury Security hardware.
      a. Life Safety Power: Enclosure Kits and Power Supplies.
      b. Elmdene: Power Supplies.
   4. Ellucian Time Management Software

2.3 APPLICATION SUPPORT

A. Supported Browsers: Provide PACS appliance with browser-based access to system applications, without mandated requirement of a dedicated client workstation that supports the following industry standard web browsers:
   1. Mozilla Firefox.
   2. Google Chrome.
   3. Safari.
   4. Internet Explorer.
   5. Microsoft Edge.

B. Supported Third Party Databases: Provide ACM which supports the following third-party data bases:
   1. Lightweight Directory Access Protocol (LDAP).
   2. Microsoft Active Directory.
   3. Structured Query Language (SQL) Server.
   4. Oracle Relational Database Management System (RDBMS).
   5. Comma Separated Value (CSV).
   6. Extensible Markup Language (XML) Event Push).

C. Supported Updates: Provide ACM which automatically updates the following:
   1. Software maintenance of operating system service packs.
   2. Software Licensing.
   3. Operating System Security Vulnerabilities.
   4. Physical Access Control System (PACS) Appliance: Provide a PACS with the following capabilities:

a. Serves as central repository for entire system configuration and activities and is only accessible through a web browser.
b. A database server and separate database server with a unique operating system are not allowed.
c. Compliant with Owner's IT Standard with fully featured physical access control system solution.
d. Utilizes industry standard TCP/IP network infrastructures to communicate including the following:
e. PACS appliances.
f. Intelligent field hardware controllers.
g. Browser based workstation.
h. Secure Data: PACS data secured as follows:
i. Secure Data communicated over the network to/from the PACS appliances and the web browser workstations via SSL 128-bit encryption.
j. Encrypt PACS appliance backups using AES Encryption.
k. Back up PACS appliance to the following:
    1) USB storage device.
    2) Windows shared directory and network shared folder.
    3) Secured SCP servers.
l. Encrypted passwords required to log in to PACS appliance within Open LDAP directory structure.

2.4 ENTERPRISE LEVEL ACCESS CONTROL MANAGER (ACM)

A. Basis of Design Product: Access Control Enterprise Appliance, by Avigilon.
    1. Model: AC-APP-16R-ENT2, with a maximum of 16, upgradable to 400 card readers.
    2. Model: AC-APP-32R-ENT2, with a maximum of 32, upgradable to 400 card readers.
    3. Model: AC-APP-64R-ENT2, with a maximum of 64, upgradable to 400 card readers.
    4. Model: AC-APP-128R-ENT2, with a maximum of 128, upgradable to 400 card readers.
    5. Model: AC-APP-256R-ENT2, with a maximum of 256, upgradable to 400 card readers.

B. Description: Linux based server pre-loaded with Access Control Manager software and optimized to manage an IP-based physical access control. Hardened Linux network appliance using LDAP compliant directory structure with a 1U form factor that can be rack mounted. Factory licensed from the manufacturer.

C. Hardware:

1. Processor: Intel® Xeon® processor E3-1220 v5 3.0GHz, 8M Cache, 4C/4T, Turbo (80W).
2. Memory: 4 GB (1x4GB), 2133MT/s, ECCUDIMM.
3. Hard Drive: TB 7.K RPM SATA 6Gbps 3.5in Cabled Hard Drive.
4. Hard Drive Controller supports RAID 5.
5. Network Adapter Card: Broadcom® 5720.
6. Power supply: Single, non-redundant.
7. Mechanical:
    a. Form Factor: Standard 1U Rack Mount.
    b. Dimensions (L x W x H): 42.8 mm x 482.4 mm x 676.92 mm; (1.68" x 18.99" x 20.8").
    c. Weight: 8.77 kg (19.32 lbs).
8. Power:
    a. Input: 90-264 VAC, 47-63 Hz.
    b. Power Consumption: 250 W.
9. Capacities:
    a. Maximum Controllers: 512.
    b. Maximum Simultaneous Operators: 50.
    c. Maximum Identities: 500,000.
    d. Maximum Stored Events: 150,000,000.

~~2.5 ACCESS CONTROL MANAGER (ACM) VIRTUAL APPLIANCE~~

A. ~~Basis of Design Product: Access Control Enterprise Appliance, by Avigilon.~~
    1. Model: AC-APP-16R-VM, with a maximum of 16 readers.
    2. Model: AC-APP-32R-VM, with a maximum of 32 readers.
    3. Model: AC-APP-64R-VM, with a maximum of 64 readers.
    4. Model: AC-APP-128R-VM, with a maximum of 128 readers.
    5. Model: AC-APP-256R-VM, with a maximum of 256 readers.
    6. Model: AC-APP-512R-VM, with a maximum of 512 readers.
    7. Model: AC-APP-1024R-VM, with a maximum of 1024 readers.
    8. Model: AC-APP-2048R-VM, with a maximum of 2048 readers.

B. ~~Description: Self-contained virtual appliance is distributed as a digital virtual machine to run within a virtualized computing environment.~~
    1. VMware® vSphere ESX 6.5+.
    2. VMware® Sphere ESXi 6.5+.

C. ~~Owner Provided Minimum Hardware Requirements~~
    1. Processor: Two, with two cores per processor.
    2. Memory: 4 GB Minimum.
    3. Hard Drive: 500GB Minimum
    4. Network: 1 GB Ethernet Port

D. ~~Capacities:~~
   1. Maximum Controllers: 512.
   2. Maximum Simultaneous Operators: 50.
   3. Maximum Identities: 500,000.
   4. Maximum Stored Events: 150,000,000.
   5. Maximum Card Readers: 16.
   6. Maximum Card Readers: 32.
   7. Maximum Card Readers: 64.
   8. Maximum Card Readers: 128.
   9. Maximum Card Readers: 256.
   10. Maximum Card Readers: 512.
   11. Maximum Card Readers: 1024.
   12. Maximum Card Readers: 2048.

2.6 PACS SOFTWARE ALARM CONTROL FUNCTIONALITY

A. Alarm and Event Attributes: Administrator configures and determines how each alarm and event is communicated in Alarm Monitors.
   1. Event Listing Window: Lists alarms and events with their associated event type and source object that is responsible for generating alarm or event.
   2. Upon logging in and accessing Alarm Monitor, queued alarms and events reported into Alarm Monitor for Operator action.

B. Provide Administrators with the following options for each alarm and event in system:
   1. Rename the alarm or event from its factory default.
   2. Rename, where applicable, the Return to Normal state name for the alarm or event.
   3. Assign an event type that sets the default configuration for alarm or event.
   4. Display alarm or event in Alarm Monitor.
   5. Mask alarm or event from displaying in Alarm Monitor.
   6. Display text instructions that guides Operator in responding to alarm.
   7. Automatically send an email message to a recipient.
   8. Have alarm display in priority order based on priority of alarm.
      a. Minimum Number of Priorities Supported: 99.
   9. Set priority of alarm or event, as well as its associated Return to Normal event priority.
   10. For video related alarms or events, automatically launch Video Player to display a live video feed from camera associated with device that generated alarm or event.
   11. Store alarm or event information for later retrieval.
   12. Create distinct schedules that can be assigned to different alarm types.
   13. Create schedule to enable/disable global events, which include the following:
      a. Shunt/un-shunt doors.

b. Mass denial of credentials (lock down).

C. Alarm and Event Logging: As a default, log alarms and events in PACS to the PACS appliance internal data storage logging structure.

D. Off-Line Alarm/Event Queue: Queue alarms and events that occur:
1. While Alarm Monitor is off-line with the rest of the system.
2. When an Operator is not logged in to the Alarm Monitor.

E. Alarm and Event Types: Supports creation of alarm and event types as follows:
1. Creates alarm and event templates as part of the installation.
2. Events contain configuration of parameters including the following:
a. Priority.
b. Text instructions.
c. Masking and masking schedule.
d. Logging.
e. Reporting.
f. Email notifications.
3. Each alarm and event type support multiple alarm and event assignments.

F. Alarm/Event Synchronization: Supports alarm synchronization for alarm and events that report into multiple Alarm Monitors.
1. Clears alarms and events from other Alarm Monitors when alarms or events are acknowledged or cleared by an Alarm Monitor Operator.

G. Alarm Reporting: Supports reporting of alarms to alarm monitors based on schedules.
1. Each alarm in the system to have its own associated schedule.

H. Alarm/Event Instructions: Each alarm and event in the system to have associated text instructions.
1. Maximum instruction character per event: 255.

2.7 PACS SOFTWARE, ACCESS CONTROL FUNCTIONALITY

A. Access Groups: An access group consists of card reader and schedule combinations.
1. Access groups consists of the total number of card readers in the system that are assigned to a single schedule.
2. Any card reader may belong to any access group.
3. Individual card readers may belong to multiple access groups.
4. Credential holder are allowed access to secure areas based on:
a. Card reader.
b. Time.
c. Day.
5. Access Group Support: Provide support of the following minimums:

a. 255 access groups per intelligent enterprise controller.
b. Access groups can be assigned to an individual credential holder per intelligent enterprise controller, and optionally be selectable up to a total of 16.

6. Access groups support conventional names up to 50 alphanumeric characters.

B. Schedules: Provide support for creation of schedules as follows:
1. Schedules serve as templates for application parameters including the following:
a. Access groups.
b. Masking devices.
c. Device modes.
2. Number of Schedules: Minimum of 255 schedules per panel.
a. Each schedule set to one of following 3 operating modes:
1) On: Schedule is active 24 hours per day / seven days per week.
2) Off: Schedule is never active.
3) Scan: Schedule is active during the assigned intervals.
3. Schedule Intervals: Provide ability to assign individual schedules to a predetermined interval as follows:
a. Day(s) of the week.
b. Assigned to function a minimum of 8 holiday types.
c. Supports a minimum of 10 intervals.
4. Download schedules to related intelligent enterprise controllers for local processing and decision making.
5. Schedules support conventional names up to 50 alphanumeric characters.

C. Holidays: Define specific dates and ranges to be defined as a holiday as follows:
1. Number of Holidays: Minimum of 255.
2. Assign a minimum of 8 holiday types.
3. Ability to temporarily alter, adjust or suspend parameters, including the following:
a. Card reader modes.
b. An Identity's access rights.
c. Masking Schedules.
4. Supports an embedded calendar to assist in configuration of holidays.
5. Holidays support conventional names up to 50 alphanumeric characters.

D. Card Reader Options: Defines options for card readers in the system as follows:
1. Specify the card reader is an active card reader.
2. Specify the off-line mode operations should the card reader lose communications with the enterprise intelligent controller or Intelligent Field Controller.

3. Specify Door Forced Filter: Reduces false alarms for doors that "bounced."
    a. No report of Door Forced Open Alarm for door opening within 3 seconds of the door closing.
4. Extended Cardholder Door Held Open Time: Allows a card reader's door held open time to be extended beyond the normal configured time.
    a. Maximum Extended Door Held Open Time: Definable up to 32,767 seconds.
    b. Defines application of this functionality by the following:
        1) Card reader.
        2) Credential holder.
5. Duress Access to a Card Reader: Supports a Duress Mode for a credential holder's entry through a card reader as follows:
    a. When a credential holder is gaining entry under duress, the credential holder must append the number "5" to the end of their PIN code.
        1) Thus, a credential holder with PIN of 9999 would enter 99995 when entering an area under duress.
    b. Make duress access for card readers in the following mode:
        1) Card and PIN mode.
        2) Card or PIN mode.
        3) PIN mode only.
    c. Upon entrance to a card reader under duress, send alarm to Alarm Monitor and logged to the audit database.
    d. Deny if Duress: Able to deny a credential holder access to the card reader during duress, even if that credential holder entered the proper duress code.
    e. Generates an alarm at the Alarm Monitor noting duress access was requested and denied.
6. Specify "Strike Mode" / strike operations allowing Administrators to define, upon a valid access:
    a. Door strike remains active for the entire strike time.
    b. Door strike turns off after the door has closed.
    c. Door strike deactivates as soon as the door is open.
    d. Do Not Pulse Door Strike on REX: Door strike disabled during a valid request to exit.
    e. Allows card reader's strike to be extended beyond the normal strike time for specific individual credential holders as follows:
        1) Definable up to 255 seconds.
        2) Definable by card reader.
        3) Definable by credential holder.

7. Log All Access As Used: In an instance where there is not a door contact at the door to monitor door position, the PACS assumes entry and report an event into the Alarm Monitor.
8. Do not log REX Transactions: Does not log request to exit transactions to the directory structure.
9. Two-Card Control: Requires two valid access requests occur prior to granting access to the door as follows:
    a. Both requests must occur within a 10 second period.
    b. In the event a second valid access has not occurred within 10 seconds of the first valid access request, the card reader will reset and the first credential will have to be presented again.
10. Use Shunt Relay that has ability to shunt a door contact of separate intrusion detection systems:
    a. When the PACS provides an access grant, a dedicated auxiliary output will first trigger and bypass the door contact of the separate intrusion detection system, and then the door locking mechanism will unlock.
    b. Once the door returns to a secure state, the door contact of the separate intrusion detection system will return to its normal state.

E. Pre-Alarm: Supports a Door Held Open pre-alarm capability as follows:
1. When a door has been held open for a pre-determined amount of time after a valid access grant, a local audible annunciation alerts credential holder to close door.
2. Failure to close the door between the pre-alarm annunciation and the configured door held open time generates an alarm at the Alarm Monitor.
3. Pre-Alarm parameters apply to the following:
    a. Door Held Open time.
    b. Pre-alarm time.
    c. Configurable up to 65,534 seconds.
    d. Provide distinct pre-alarm setting for each door.

F. Card Reader Scheduled Mode Overrides: Supports ability for card reader modes to be overridden from standard mode on a scheduled basis.
1. Based on the card reader type, custom modes include the following:
    a. Card only.
    b. Card and PIN.
    c. Card or PIN.
    d. PIN only.
    e. Locked.
    f. Unlocked.
    g. Facility code.

h. At end of scheduled override, card reader returns to its default standard mode.

2. Cipher Mode: Supports Cipher Mode, which emulates presentation of a credential to a card reader with a keypad.
    a. In Cipher Mode, an authorized credential holder attempts access by entering their Credential ID/Card Format at keypad.
        1) The card reader treats the information as a magnetic card format read.
        2) The number sequence must match an existing magnetic card format configured in the system, including facility code.
        3) Correct entry of code will allow access.
        4) Incorrect entry of code will be ignored and deny access to card reader.
        5) Will not send a transaction to Alarm Monitor.
    b. A card reader in Card and PIN Mode and Cipher Mode also requires the credential holder's PIN be entered after original sequence is entered.
    c. Changes in card reader mode will not remove a card reader from Cipher Recent Door Transactions. The PACS will provide a form listing the most recent transaction activity associated with a door, without having to run a report including the following:
        1) Transaction activity.
        2) Time/date.
        3) Identity.
        4) Token related details.
3. Invalid PIN Attempts Counter: Supports an Invalid PIN Attempts Count on a per card reader basis. Invalid PIN Attempts parameters include, but not be limited to, the following:
    a. Unknown PIN entry at a card reader configured as Card or PIN Mode.
    b. Invalid cipher entry at a card reader in Cipher Mode.
    c. Invalid PIN entered for a given card at a card reader configured as Card and PIN Mode.
    d. The Denied PIN Attempts value will be configurable from 0 to 255.
    e. The counter rests to zero if the following events occur:
        1) A specific user defined number of minutes pass without one of the above denial types.
        2) An access grant at the given card reader.
    f. When the current Deny Count reaches the threshold configured for the card reader, a Deny Count Exceeded transaction is reported.

1) This transaction will only be reported when the limit is initially reached.
2) It will not report on subsequent denials.

g. Define the number of Invalid PIN Attempts may be presented before generating an alarm to the Alarm Monitor.

4. Supports Macro/Trigger functionality when the Deny Count Exceeded transaction occurs.
   a. Actions include, but not be limited to, the following:
      1) Lock down the card reader.
      2) Annunciating a local siren.
      3) Configured to execute for a given card reader.
5. Multiple complementary modes can be assigned per reader.

G. Provide buttons in Graphical User Interface (GUI) that are available to control operational state of the door including the following:
   1. Door access.
   2. Door mode.
   3. Forced and Held status.
   4. Door installed status.

H. Door Summary and Status Page: Supports a Door Summary and Status Page that displays a list of doors defined in the system.
   1. For each door in the system, the Door Summary and Status Page will display the following:
      a. Door Name.
      b. Current Door Mode.
      c. Door Status including forced and held states, masking states, including communications and tamper states.
      d. Results displayed are able to be filtered by Door Group or by other searchable criteria.
      e. Door management: Supports adding, updating, and removing doors by the following:
      f. Add Doors button.
      g. Create new doors from Door Template.
      h. Bulk delete doors.
      i. Bulk update doors from Door Template.
      j. Door Scheduled Mode Overrides: Supports ability for door modes to be overridden from standard mode on a scheduled basis.
   2. Supports the following for each override:
      a. Override name.
      b. Door mode.
      c. Start time
      d. End time.

e. Notes.
f. At end of scheduled override, door reader returns to its default standard mode.
g. Supports override indicators for active and scheduled overrides on the following:
h. Door Summary and Status Page.
i. Maps.
j. Overrides listing page.

I. Mask Alarm Filters: Displayed on the workstation GUI.
1. Filter operator views to remove Door Forced Open and Door Held Open alarms to the following:
a. Mask permanently.
b. Mask during a schedule.
2. Distinct Schedules will be able to be assigned to different Alarm Types.

J. Multiple Card Formats: The PACS, enterprise intelligent field controller, and card readers will support a minimum of 16 card formats; including the following:
1. Wiegand.
2. Magnetic Stripe.
3. The PACS will support any industry standard format that uses the following:
a. A card number.
b. A facility code.
c. An issue code combination.
4. The PACS will support the following:
a. A maximum 19 digit card number.
b. Two digit issue codes.

K. Wireless Lock Integration: The PACS will support the following wireless lock integration solutions:
1. Allegion Solution Panel Interface Module (PIM): Schlage wireless locks to communicate with a PIM.
a. Each PIM will allow wireless connection to up to 16 AD-400 wireless locks.
b. There will be RS-485 connection from Mercury controllers to the PIM.
c. There will be automatic linking to remote wireless access points with 10 channel frequencies.
d. The solution will support 125 kHz proximity and 13.56 MHz smart cards.
2. Allegion solution (Engage Gateway): Schlage wireless locks to communicate with the Engage Gateway.
a. Each Gateway will allow wireless connection to up to 10 NDE/LE wireless locks.

b. There will be RS-485 connection from Mercury controllers to the Engage Gateway.
c. The solution will support 125 kHz proximity and 13.56 MHz smart cards.

3. ASSA ABLOY solution: Aperio wireless locks to connect to a Mercury enabled Aperio 8:1 communications hub.
   a. Each hub will connect to up to eight wireless locks.
   b. There will be RS-485 connection from Mercury controllers to the Aperio hub.
   c. The solution will support 125 kHz proximity and 13.56 MHz iClass contactless credentials.
4. SimonsVoss - Smart Intego: SimonsVoss wireless locks to connect to a Smart Intego Gateway Node.
   a. Each Gateway Node will connect to up to 16 wireless locks.
   b. The Gateway Node will communicate the locks via an 868 MHZ wireless solution (RF).
   c. The solution will support 125 kHz proximity and 13.56 MHz iClass contactless credentials.

L. End of Line Resistance Configuration: Allows Administrators to define configurations to be assigned to alarm inputs.
1. Standard End of Line Resistance configurations will include:
   a. Independently define Request to Exit and Door Contacts as Normally Open or Normally Closed.
   b. Independently define Request to Exit and Door Contacts as Supervised or Unsupervised.
2. A minimum of 4 custom End of Line Resistance configurations will be available.
3. Configurations will be given a priority of low, medium or high.
4. Configurations include options for low range and high range resistance thresholds.
5. Configuration options include the following input line statuses:
   a. Inactive.
   b. Active.
   c. Ground Fault.
   d. Open.
   e. Short.
   f. Foreign.
   g. Non-Setting.

M. Elevator Control: Provide elevator control as follows:
1. Using standard access control field hardware.
2. Permits restriction of access to certain floors.

3. Does not restrict access to general admittance floors.
4. Card readers located in elevator cab has the capability to do the following:
    a. Control access for a minimum of one floor.
    b. Integrate to Input and Output Control Modules.
    c. Restrict which floor select buttons are accessible when a credential is swiped based on the Identity's access level.
    d. Permit only one authorized floor to be selected per single card swipe.
    e. Not require a swipe by any passenger to access floors programmed as public access.
5. Independently configure individual floors to allow visitor/general access to different floors during different times of the day.
6. Track which floor was selected by an individual cardholder for auditing and reporting purposes.

N. Anti-Passback (APB):
1. Provide area control features including the following:
    a. Hard Anti-Passback.
    b. Soft Anti-Passback.
    c. Timed Anti-Passback.
    d. Two-Person Control.
    e. Occupancy Count:
        1) Minimum Number of Areas Created: 127 areas per PACS appliance.
2. Hard and Soft APB Common Function: In addition to functions specific to Hard or Soft APB, either function will include the following:
    a. Initially (Time 0), credential holders are reset to Area 0.
    b. Credential holders will be allowed to enter a controlled area any time after Time 0 by presenting a Token to an entry card reader.
    c. Credential holders will not be allowed to exit the controlled area unless they have entered the area presenting a Token to the area entry card reader.
    d. Credential holders will not be allowed to enter the controlled area a second time unless the credential holder has exited that area previously.
    e. Credential holders will be able to enter through any entry card reader and exit through any exit card reader of a single controlled area.
    f. A Forgiveness feature that allows the Administrator to give credential holders One Free Pass to allow the PACS to move them into the next area they enter, regardless of their current APB status.

1) Provide one Free Pass to an individual credential holder, to credential holders in a single enterprise intelligent field controller, and to credential holders in the PACS.

g. Provide an APB exempt option for privileged and VIP credential holders.
   1) Credential holders with this option will not have APB rules applied to them.

h. Provide the ability to disabled/closed areas and not allow access into disabled/closed area.
   1) Exception: Those Tokens with APB privileged status.

3. Hard APB:
   a. Requires a Token be used to enter and exit an area.
      1) Provide entry and exit card readers at controlled area portals.
      2) Confine entry and exist card readers to a single enterprise intelligent field controller.
      3) Logically define areas.
      4) Every card reader in the system is not required to be included within the Area Control.
   b. Operations:
      1) Once in an area, a credential holder must present their Token at an exit card reader of the area they are currently in and wish to leave.
      2) Once access has been granted to leave the area and enter a new area, the credential holder must present their Token at an exit card reader of the new area.
      3) Should a credential holder present their Token at any other card reader involved in Area APB, the credential holder will be denied access and an alarm will be reported.
   c. Nesting: Provide definable, nested control areas (areas inside areas) that include a minimum of 64 entry and exit card readers.
      1) Apply Hard APB rules to individual areas within an area and multiple areas that are independent of each other.

4. Soft APB:
   a. Requires a Token be used to enter and exit an area.
      1) Provide entry and exit card readers at controlled area portals.
      2) Confine entry and exist card readers to a single enterprise intelligent field controller.
      3) Logically define areas.

4) Every card reader in the system is not required to be included within the Area Control.

b. Operations:

1) Once in an area, a credential holder must present their Token at an exit card reader of the area they are currently in and wish to leave.

2) Once access has been granted to leave the area and enter a new area, the credential holder must present their Token at an exit card reader of the new area.

3) Should a credential holder attempt this, the credential holder will be allowed access (provided the credential holder has appropriate access level to access the new area), and an alarm will be reported.

c. Nesting: Provide definable, nested control areas (areas inside areas) that include a minimum of 64 entry and exit card readers.

1) Apply Hard APB rules to individual area within an area and multiple areas that are independent of each other.

5. Timed APB: Allows an Administrator to decide how long after a credential holder has swiped their Token before the same Token will be accepted again at the same card reader.

a. If a credential holder swipes their Token a second time after initial entry and after the delay time has expired, access will be granted and an APB alarm will be reported into the Alarm Monitor.

b. Administrators will be able to set the delay time up to a minimum of 65,535 seconds.

6. Provide Two-Person Control to restrict access to certain areas unless there are 2 credential holders present.

a. When an area is configured for Two-Person Control, apply the following criteria:

1) Card reader will grant access only if 2 valid credential holders (with authorized access privileges) swipe their badges one after the other.

2) In the event that a second authorized badge is not presented within 10 seconds of the first authorized badge, the card reader will reset and the first card will need to be re-swiped.

3) Once 2 people occupy an area, individual access will be granted to other credential holders.

4) Individual exit will be allowed until an area is occupied by only 2 credential holders.

5) For the last 2 credential holders to exit, both must present their cards at exit reader within 10 second of each other and exit together.

O. Mustering: Allow creation of a dashboard and a map view to quickly monitor who as arrived at a predetermined mustering station.
   1. Mustering area will be defined by administrator to add/ delete identities to each mustering area.
   2. Mustering feature will allow a report of people in each area and have ability to filter the report to display specific identities.
   3. The dashboard will contain dynamic text areas that can be customized by size, shape, color and transparency.
   4. Administrator will be able to place dynamic text areas over a map view.
   5. Import maps with the following formats:
      a. BMP.
      b. GIF.
      c. JPG.
      d. PDF.
      e. PNG.
   6. Provide map view with a real time update of the number of people in each area.

P. Occupancy Count / Control: Restricts number of credential holders that are present in an area at any given time.
   1. Administrator will define Occupancy Controlled area.
      a. Occupancy Limit: Maximum 250,000 credential holders in area at any given time.
   2. Once the occupancy limit has been reached, a credential holder must swipe out of the exit card reader before the next credential holder may enter.
   3. Each area where Occupancy Control is enabled will be definable with up to 64 entry/exit card readers.
   4. Able to define Multiple Occupancy Controlled areas.

Q. Custom Device Mappings / Local Alarms: Administrators may assign a unique group of alarm attributes to specific device-alarm combinations to override global settings of generic attributes.

R. Entry / Exit Delay: Administrators may set entry/exit delays for inputs attached to Input Control Modules, Single Reader Interface Modules, and Dual Reader Interface Module using the following settings:
   1. Non-Latched Entry: Administrators may set an input to non-latched entry.
      a. When non-latched entry mode is selected and an entry delay is specified, the following procedure ensues:

1) When an input activates, the alarm will not be reported until the entry delay expires.
2) If the input is active when the entry delay expires, the alarm will be reported.
3) If the input is not active when the entry delay expires, then the alarm will not report.

2. Latched Entry: Administrators may set an input to latched entry.
   a. When latched mode is selected and an entry delay is specified, the following procedure ensues:
      1) When an input activates, the alarm will not be reported until the entry delay expires.
      2) If the alarm has not been masked by the time the entry delay expires, the alarm will be reported.
      3) If the input has been masked when the entry delay expires, then the alarm will not report.
3. Exit Delay: Administrators may set an input to exit delay that activates directly after an input has been unmasked.
   a. When an exit delay is specified, the following procedure ensues:
      1) When an input activates, the alarm will not be reported (operates as if masked) until the exit delay expires.
      2) If the input is still active when the exit delay expires, the alarm will be reported.
      3) If the input is not active when the exit delay expires, the alarm will not be reported.
      4) Administrators will be able to set the entry and exit delay times up to a minimum of 65,535 seconds.

S. Input Control Module Options: Allows the following options to be defined for inputs or outputs in the Input Control Module:
   1. Debounce Time: Allows Administrators to control time that an input state change must remain consistent in order for it to be considered a real change of state.
   2. End of Line Resistance: Administrators may define an Input as Normally Open or Normally Closed and define an input as Supervised or Unsupervised.
   3. Hold Time: Allows Administrators to set the amount of time in seconds to wait to report an input activation as restored when an input goes active and then is restored.
      a. Hold Time Range: From 0 to 15 seconds.
   4. Alarm Masking: Allows input to be masked either all the time or during a defined schedule.
   5. Activate Output: Allows Administrators to configure an output to activate all the time or during a defined schedule.

6. Installed: Defines whether the PACS will consider the input an active component of the on-line system.
7. Logging: Allows Administrators to determine whether to log change of state events or only when the event is not masked.

T. Relay Output Options: Allows the following options to be defined for outputs in the Output Control Module:
1. Installed: Defines whether the PACS will consider the output an active component of the on-line system.
2. Relay Output Mode: Sets default mode of relay output.
3. Pulse Time: Defines how long output will pulse when command is given.
4. Schedule: Defines time the relay output is active.

U. Input / Output / Event Linkages: The PACS will support input/output/event linkage whereby an input/output/event in an enterprise Intelligent field controller can trigger an action within the same enterprise intelligent field controller.
1. Linkage decisions will be made local to the intelligent enterprise controller.
2. Administrators will be able to create macros.
    a. Each macro to consist of a sequence of actions to be performed.
        1) Example: Changing card reader modes and activating outputs.
    b. Maximum Number of Actions: 30 actions per macro.
3. Administrators will then be able to link events to macros so that a defined action will trigger a macro to execute.

V. Global Actions: Allows Operators to define an action to be performed.
1. Action may be scheduled and run manually.
2. Available action types include the following:
    a. Access group install/uninstall.
    b. Action group.
    c. Door grant.
    d. Door install/uninstall.
    e. Door mask.
    f. Door mode.
    g. E-mail.
    h. Exacq soft trigger.
    i. Input.
    j. Intrusion area.
    k. Intrusion output.
    l. Intrusion point.
    m. Output.
    n. Panel install/uninstall.
    o. Panel micro.
    p. Policy install/uninstall.

q. Schedule set mode.

W. Global Linkages: Allows Operators to define linkages relating to the following:
1. Devices, including the following:
a. Doors.
b. Inputs.
c. Intrusion areas.
d. Intrusion outputs.
e. Intrusion panels.
f. Intrusion points.
g. Output.
h. Panel.
i. Sub-panel.
j. Video camera.
k. Video server
2. Events.
3. Tokens.
4. Actions.

X. Inputs include any enterprise intelligent field controller level event, including the following:
1. Enterprise Intelligent Field Controller Events:
a. Cabinet tamper.
b. Power failure.
2. Input Control Module Events:
a. Communication loss.
b. Cabinet tamper.
c. Power failure.
d. Input points.
3. Card Reader Events:
a. Cabinet tamper.
b. Communication loss.
c. Door contact tamper.
d. Door forced open.
e. Door held open.
f. Power failure.
g. Card reader tamper.

Y. Macro actions include, but not be limited to, the following:
1. Activating an Output Control Module Output.
2. Masking/Unmasking an alarm Input.
3. Setting the active mode of a card reader.
4. Activating/deactivating a schedule.

Z. Macros will link to devices and types of inputs will include, but not be limited to, the following:
    1. Enterprise Intelligent Field Controller Events.
        a. Cabinet Tamper, Power Failure:
            1) Secure.
            2) Fault.
            3) Alarm.
    2. Card Reader Events:
        a. Communication Status.
        b. Cabinet tamper, Power failure, Reader Tamper, Forced Open, Held Open, Door Contact tamper, Aux Input #1, Aux Input #2:
            1) Secure.
            2) Fault.
            3) Alarm.
        c. Access Activity:
            1) Access granted.
            2) Access denied.
            3) Duress.
    3. Input Control Module Events:
        a. Communications Status.
        b. Alarms: Cabinet Tamper, Power Failure, Alarm Inputs:
            1) Secure.
            2) Fault.
            3) Alarm.
    4. Intrusion Events:
        a. Points.
        b. Areas.
        c. Panels.
        d. Outputs.
        e. SDI devices.
    5. An input/event may trigger multiple Macros and a Macro will be able to be triggered by multiple inputs/events.
    6. Supports a minimum of 100 Macros per enterprise intelligent field controller.
        a. Maximum Number of Actions: 30 actions per macro.

2.8 PACS SOFTWARE, IDENTITY MANAGEMENT FUNCTIONALITY

A. Identity Management Integration: Offers an integrated Identity Management and Enrollment functionality as part of the core system functionality.
    1. Data Import: Will import Identity records and their associated image in JPEG, BMP and PNG formats.

2. Identity records will be able to be pre-loaded prior to implementation or added at any time after deployment.

B. Provide a pre-configured one-time import utility, using standard Comma Separated Value (.csv) files that allows import of Identity information based on the factory shipped data fields.

C. Identity Enrollment: Allows individual enrollment of identities.
   1. Each Identity allows entry of required and optional fields.
   2. Required fields included the following:
      a. User account.
      b. Account password.
      c. Non-activity timeout.

D. Role Base Permissions:
   1. Assign roles during enrollment.
   2. An identity's role will determine their access groups.
      a. Access groups define the following:
         1) Which card readers they have access to.
         2) Which times access to those card readers is allowed.

E. PACS software allows an identity to have access to specific doors or access groups for a specified time range without requiring a role to be assigned.

F. Create and assign Tokens during enrollment.
   1. For each Token, credentials include, but not be limited to, the following:
      a. A Badge ID.
         1) Support a minimum of a 19 digit Badge IDs.
      b. Embossed number.
      c. Assigned PIN codes
      d. Activation and deactivation date.
      e. Associated settings for Anti-Passback (APB).
   2. Optional credential parameters include, but not be limited to, the following:
      a. Adding a Token to a group during enrollment to create predefined Role and Policy Settings that will drive the configuration of the Identity information.
      b. Expiration of the credential due to non-use within a certain timeframe.
         1) System wide for every credential.
         2) Variable parameters per individual or access level.
         3) Individual or access levels can be exempt from expiration.
         4) Scheduled time for expiration do to non-use will be at least one year from date of activation.

G. During Enrollment, the Identity's image will be captured or loaded in JPEG format and a Badge template will be assigned.

H. Federal Information Processing Standard Publication 201 (FIPS-201) Support: Enables FIPS 201 compliant validation and registration of Identities through the following:
   1. Integration with HID pivCLASS devices.
   2. HID pivCLASS Certificate Manager and updating an existing cardholder record or inserting one, if one did not already exist.
   3. Supports importing photographs and fingerprint biometrics from government issued smart card that is compliant with FIPS- 201.

I. Allows credential suspension if card certificate serial number is on a designated list, including the following:
   1. Certificate Revocation List (CRL).
   2. If the FASC-N is on TSA Canceled Card List (CCL).

J. Supports PIV, TWIC, CAC, and FRAC credentials.

K. Credential Re-Issuance:
   1. Operator will be able to deactivate existing credentials by marking them as lost or stolen.
   2. The PACS will be able to use existing Identity information and photos for new credentials.
      a. The process will not require re-enrollment of credential holders.
   3. The re-issuance process will automatically perform the following actions:
      a. Remove access rights from the deactivated Token.
      b. Enable those same rights in the new Token.
      c. Automatically send the appropriate changes to the intelligent enterprise controllers.

L. Identity Database: Each Identity will have a unique record in the Open LDAP directory structure.
   1. LDAP Directory Structure will include the use and definition of User Defined Fields and Forms.

M. Deleting Identities: Highest level administrators will be given the ability to perform the following actions:
   1. Delete individual Identities.
   2. Bulk Delete Identities: The ability to delete a group of identities based on user defined search criteria.

N. Assign Access Groups: Allow Administrators to assign access groups to Roles.
   1. A Role will then be assigned to an Identity during enrollment.

2. Each Identity may have up to 8 access groups assigned to their record per intelligent enterprise controller through assignment of one or more roles to their record.

O. Access group modifications or assignments will be automatically downloaded to the appropriate intelligent enterprise controllers:
   1. Without Operator intervention.
   2. Completed as a push communication immediately after an Identity record is saved. Scheduled, batch updates are not allowed.

P. Supports an Access Group View form that allows Operators to view the following:
   1. Roles that have been assigned to an Identity.
   2. Which access groups are associated with the Role.
   3. What doors an Identity has access to.

Q. Roles: Support a Role Based Permission methodology to be used in conjunction with Identities.
   1. Roles will be assigned to Identities to determine door access as well as access into the system application.
   2. Multiple Roles will be able to be assigned to an Identity.
      a. A Parent/Child relationship can be defined, per Role.
      b. Duplicating Role information for multiple roles will not be required.
   3. Identities will aggregate all Role assigned permissions.
   4. Each Role will have a defined start and stop date.
      a. To allow assignment of Roles on a temporary basis.
      b. Roles can be manually activated or deactivated through the use of a checkbox.
   5. Each Role will consist of any combination of the following components that will determine which Roles an Operator will be able to assign to other Identities during enrollment:
      a. Access groups.
      b. Delegation assignments.
      c. Role assignments.

R. Image Capture Device: Support IP-based cameras for Photo Capture.
   1. The Operator will be able to view a live image on screen of the Identity to move them into a proper pose or position prior to freezing the image.
   2. If the Operator is not satisfied with the captured image, they will be able to revert to a live view and freeze a new image.
   3. Configuration settings for IP cameras, as well as viewing a live and still image of a person will be user-configurable.

S. Photo Capture: The PACS will support Photo Capture through use of an IP-based camera.
   1. The Operator will be able to view a live image on screen of the Identity to move them into a proper pose or position and then be able to freeze the image.
   2. If the Operator is not satisfied with the captured image, they will be able to revert to a live view and freeze a new image.

T. Support the ability to import photos in standard JPEG format from digital cameras or other image capture sources.

U. Allow the captured photo to be cropped via use of the mouse to define the crop window.
   1. Only information inside the crop window will be saved and stored in directory structure.
   2. Images will be associated with the Identity and will be stored in the Open LDAP directory.

V. Token Activation and Deactivation Dates: Supports activation and deactivation dates for Tokens created.
   1. A Token will be able to be configured to activate at a future date from time of creation.
   2. When a Token reaches its deactivation date/time, the PACS will automatically deactivate the access rights associated with the Token.
   3. Access rights of a Token will be eliminated after deactivation date.
   4. Should Identity become authorized for access again, new access rights will be applicable to the same Token.
      a. Re-issue will not be required.
   5. Expiration of Credential Due to Non-Use: Credentials can be set to expire if not used within a timeframe determined by Operator.
      a. Parameters include the following:
         1) System wide for every credential.
         2) Variable parameters per individual or access level.
         3) Individual or access levels can be exempt from expiration.
         4) Scheduled time for expiration do to non-use will be at least one year from date of activation.

W. Token Audit Trail: Keep an on-line record of Tokens issued to an Identity.
   1. For each record, details will be recorded including activation and deactivation dates, Token status, and Token ID.

X. Token Issue Codes: Support a minimum of a 2-digit issue code.

Y. PIN Codes: Support up to 8-digit PIN codes.

1. Each credential holder in the PACS will be able to choose a PIN to be associated with their record.
2. A credential holder's PIN will be able to be changed should the original PIN code be compromised.
3. An Identity will be able to be exempted from PIN requirements within the system.

Z. Credential Options: Support industry standard pre-encoded physical credential options including:
1. Composite Credentials.
    a. Example: PVC cards, mobile credentials.
2. Proximity Credentials including dual PVC technology that includes both proximity and magnetic stripe technology.
3. Contact Smart Credentials.
4. MiFare Credentials.
5. DESFIRE Credentials.
6. HID iClass Credentials.

AA. Last Access Information: A credential holder's last entry point will be indicated as follows:
1. Displays on the main Identity form.
2. Include date/time stamp for when entry occurred.
3. If a credential holder has multiple Tokens, the Tokens' form will also show the last entry point with date/time stamp for each Token in a credential holder's possession.

BB. Last Identity Record Modification: Display date and time of last modification to that Identity record from main Identity form.

CC. Multiple Active Tokens: Allow Identities to have multiple active Tokens associated with their record.
1. Number of Active Tokens: Minimum of 25 active Tokens may be assigned to an Identity.

DD. Dual Sided Credential Printing: Allow for printing on both sides of a credential.

EE. Revoke Credential Access: Allow Operators to revoke access privileges from a credential holder by updating that credential holder's Token status.
1. A Token with Revoked access will immediately stop functioning at card readers.

FF. Search Capabilities: Support search for Identities according to the following parameters:
1. First Name.
2. Last Name.

3. Identity.
4. Token field in the system.

GG. Allow searches using AND / OR logic on filters that include, but not limited to the following fields:
    a. Equals.
    b. Not Equals.
    c. Starts with.
    d. Ends with.
    e. Contains.
    f. Is Empty.
    g. Greater than.
    h. Less than.
    i. Equals.

HH. Pick List Builder: Include a pick list builder that allows Administrators to define Operator selection options that appear in Identity form pick lists.
1. Each pick list will have an unlimited number of pre-defined selections.

II. Support the following standard Identity and Token fields:
1. Last Name.
2. First Name.
3. Middle Name.
4. External System ID.
5. Address.
6. City.
7. State.
8. Zip.
9. Phone.
10. Work Phone.
11. Email Address.
12. Title.
13. Department.
14. Division.
15. Site Location.
16. Building.
17. Last Record Modification.
18. Status.
19. Type.
20. Issue Date.
21. Login.
22. Password.
23. Password Confirmation.
24. Inactivity Timer.

25. Last Door Accessed.
26. Last Time Accessing Last Door.
27. Photo.
28. Embossed Number.
29. Internal Number.
30. PIN.
31. Token Status.
32. Issue Level.
33. Activate Date.
34. Deactivate Date.

JJ. Transaction Activity: Provide a form listing the most recent transaction activity associated with an Identity, without having to run a report.
    1. Information provided will include the following:
        a. Transaction activity.
        b. Time/date.
        c. Related Token.

KK. User-defined Fields: Support the ability to add additional Identity-based forms to support user-defined fields.
    1. Up to 10 user-defined forms will be able to be added.
    2. Each user-defined field will be given a field name/label and be defined as one of the following field types:
        a. String.
        b. Integer.
        c. Boolean.
        d. Date.
        e. Text box.
    3. Up to 300 user-defined fields will be available.

LL. Badge Layout Tool: Support a tool to allow for the custom creation of Identity/Token Badge Layouts.

MM. Support Badge sizes required by Owner and supported by printer used for to create Badges.

NN. Allow multiple objects to be configured for a badge layout including:
    1. Alphanumeric text fields.
    2. Database fields.
    3. Photos.
    4. Identity photos.
    5. Graphics.

OO. Each text and database field added to the layout will be able to employ the following properties:

1. Location of the object.
2. Height and width.
3. Background color.
4. Rotation.
5. Typeface of text.
6. Size of text.
7. Color of text.
8. Horizontal and vertical alignment of text.

PP. Each photo and graphic field added to the layout will be able to employ the following properties:
1. Location of object.
2. Height and width.
3. Maintain aspect ratio.
4. The PACS Badge Layout tool will support a color palette that supports a minimum of 16.7 million colors that can be applied to applicable objects.

2.9 PACS SOFTWARE, ALARM AND EVENT MONITORING

A. System Level Events: Events configured at the system level; for example: Door Forced Event, if configured at System Level will affect all doors in the system.

B. Field Level Events: Events configured at the field controller level and only affect that particular controller. For example: Door Forced Event configured as local event (Field Event), will only affect the door it is configured on, all other doors will follow the System Level Event.

C. Tabbed User Interface: Supports a tabbed view for Monitor User Interface of the following tabs:
1. Event Monitor: Used to monitor system level events.
    a. Example: Operator activity and field level events.
2. Alarm Monitor: Used to monitor field level events.
    a. Example: Identity access activity, input alarms, and door alarms as well as system level events configured as alarms.
3. Swipe and Show Verification: Used to view Identity information in real-time as credential holders access specific doors.
4. Search: Used to search for alarm and event transactions currently stored in the PACS.
5. Hardware Status: Used to view the real-time status of field hardware devices configured in the system, as well as to manipulate/override those devices.

D. Alarm Annunciation: Allows Administrators to configure how alarms and events annunciate into the Alarm Monitor.
1. Support audible notification at workstation when alarms arrive in the system.
    a. Allows Users to adjust the configuration and parameters.

b. Allows Administrators to choose a specific sound to pair with each type of alarm.

E. Provide the following configuration options for alarms and events:
1. Display in Alarm Monitor.
2. Masking from displaying in Alarm Monitor.
3. Allows higher alarms to be displayed on top of Alarm Monitor when an Operator sorts based on alarm priority.
4. Display text instructions that guide Operator in alarm response.
5. Automatically sends an email message to one or more recipients.
6. For video related alarms and events, automatically launches Video Player to display live video feed from camera associated with generating alarm or event.

F. Alarm Management and Handling: Provides a real-time count of alarms and events in Alarm Monitor awaiting Operator action.

G. Supports the following options for handling / responding to alarms and events upon selection:
1. Acknowledge the alarm.
2. Review text instructions on pre-defined alarm response.
3. Enter unlimited notes on reason for alarm and action taken in alarm response.
4. Review the history of the alarm.
5. For alarms and events that include a credential holder, call up the Identity Record of that credential holder.
6. Clear the Alarm: Provide 3 types of alarm clearing as follows:
a. Single Operator Enabled Clearing: Only one Operator is required to clear the alarm from the Monitor.
b. Two-Person Control Clearing: Requires the following sequence of actions:
1) First: One Operator is required to acknowledge the alarm.
2) Second: After alarm has been acknowledged, a different Operator is required to clear the alarm from the Monitor.
c. Role-Based Clearing: Allows System Administrators to assign a Role or Roles to the alarm.
1) Only the Operator assigned one of the Roles assigned to an alarm is allowed to clear the alarm from the Monitor.

H. Bulk Alarm Management and Handling: Supports the ability to manage and handle multiple alarms.
1. Operators may clear or acknowledge all selected alarms in a single action.

I. Alarm Routing: Allows Identity-based alarm routing to specific Identities monitoring the application based on the following:
1. Schedule.

2. Event type.
3. Device.

J. Alarm Masking: Allows masking of specific alarms or alarm types based on pre-defined schedules or via manual overrides.
   1. Masked alarms will not report into the Alarm Monitors.
   2. Logging the transaction database for reporting and audit trail will not be affected by Masked status.
   3. An Operator will be able to mask or unmask any alarm point in the system based on permissions.

K. Alarm Sorting: Allows alarms and events to be sorted in Alarm Monitor by currently configured viewable columns.

L. Alarm Prioritization Color Bars: Provides capability to emphasize alarm priority through use of colored bars within alarm monitor screen.
   1. Each alarm priority has its own unique user-defined color assigned to it.
   2. Color bars may be assigned to individual alarm priorities or to a range of alarm priorities.

M. Column Configuration: Allows Administrators to define which columns are displayed in Alarm Monitor.
   1. Administrators may set column order of the Alarm Monitor and includes the following columns:
      a. Time.
      b. Last Access.
      c. Token Expire Date.
      d. Token Issue Date.
      e. Panel Date.
      f. Priority.
      g. Operator.
      h. Identity First Name.
      i. Identity Middle Initial.
      j. Identity Last Name.
      k. Card Number.
      l. Embossed Number.
      m. Message.
      n. Event Name / Description.
      o. Event Type.
      p. Panel.
      q. Source.
      r. Location.
      s. Alternate Source.
      t. Input Address.

u. Event Address.
v. Source Type.
w. Flags.
x. Status.
y. Issue Level.
z. Role.

N. Email Capabilities: Supports integrated email capabilities.
1. Generates an email message to send to one or more recipients upon a generated alarm or event.
2. Email function interfaces with email servers that uses SMTP protocol.

O. Events Monitoring: Supports an Event Monitoring tab that monitors system level events.
1. An Operator may choose which field columns to display and may place those columns in their order of preference.
2. The Operator may sort events by currently displayed columns in the Event Monitor.
3. Administrators may configure the number of recent events to display in the Event Monitor upon accessing Events tab.

P. Field Hardware Device Status Summary Counter: Supports a real-time Field Hardware Device Status Counter displaying a summary of the total number of doors, input points, intelligent enterprise controllers, and sub panels that are active, masked, and off-line.

Q. Field Hardware Device Status Tab: Supports real-time system status that depicts configured field hardware devices.
1. List the following information in the real-time system status tab:
a. Intelligent enterprise controllers.
b. Input Control Modules.
c. Alarm inputs.
d. Relay outputs.
e. Card readers.
f. Hardware status shows the following real-time status of the devices listed immediately above:
1) On-line versus off-line.
2) Alarms activated.
3) Masking status.

R. System status includes the following 3 counters:
1. Active Counter: Counts number of active points.
2. Offline Counter: Counts number of offline devices.
3. Masked Counter: Counts number of masked points.

S. Hardware Status tab displays hardware devices separately in their own row including the following information:
   1. Device Name.
   2. Intelligent Enterprise Controller / Input Control Module / Output Control Module Name.
   3. Current Device Status.

T. Allows Operators to change the access mode of card readers, open doors, mask/unmask alarm inputs, and activate/deactivate/pulse and output from the tab.
   1. Allows Operators to change the access mode of multiple devices with a single action by selecting multiple devices and then performing the command.

U. Supports integration with Life Safety Power's (LSP) N1 network module.
   1. When configured, LSP power supply link appears in Field Hardware Device Status tab.
   2. When link is clicked, the N1 diagnostic and configuration window will appear.

V. History Record Call-Up: Supports the ability to call up the history of an alarm.
   1. History call up window displays associated alarm information including the following:
      a. Time/date stamp.
      b. Acknowledgment actions by Operators.
      c. Entered notes.
   2. Operator will not be required to exit Alarm Monitor to access this information.
      a. This functionality will not prevent additional alarm activity from reporting to Alarm Monitor.

W. Identity Record Call-up: Supports ability to call up Identity form to display Identity Record associated with alarm.
   1. Identity call up window displays Identity's information and photo.
   2. Operator will not be required to exit Alarm Monitor to access this information.
      a. This functionality will not prevent additional alarm activity from reporting to Alarm Monitor.

X. Operator Control of Field Hardware Devices: Allows Operators to manually control the state of field hardware devices and their input/output points from the Alarm Monitor.
   1. Card Readers:
      a. Manually control reader state or based on current schedule:
         1) Unlocked.
         2) Locked.
         3) Facility code.
         4) Card Only.
         5) PIN Only.

6) Card and PIN.
7) Card or PIN.
8) Pulse the Door Open.
9) Mask/Unmask.
10) Door Forced Open/Door Held Open.
11) Disable the Door.
12) Restore the Door to its Correct State.
13) Inputs: mask and unmask input.

2. Outputs:
   a. Manually control reader state or based on current schedule:
      1) Turn on.
      2) Turn off.
      3) Pulse outputs.

Y. Operator will control field hardware devices from Hardware Status tab.

Z. Uses a Last Command Wins methodology.
1. Example: If an output is set to off due to a schedule and an Operator manually turns it on, then the output will remain on until it is manually turned off or until the next scheduled interval occurs.

AA. Manual controls will be recorded in Operator Audit log, including the following information:
1. Time of the change.
2. Operator performing function.
3. Description of activity performed.

BB. Maps: Supports the import of graphic map backgrounds in the following formats:
1. Bitmap (.bmp, .dib).
2. JPEG (.jpg).
3. Portable Network Graphics (.png).
4. TIFF (.tif).
5. Windows Metafile (.wmf, .emf).
6. Encapsulated Post Script (.eps).

CC. Administrator may place system icons for the following hardware devices to indicate their location in facility:
1. Card readers.
2. Input & output points.
3. Video cameras.
4. Other access control field hardware.

DD. Zoom Capabilities: From the Map, operators may zoom in or zoom out on a camera's view and be able to:

1. Acknowledge an alarm.
2. Change the Access Mode of Readers.
3. Mask/Unmask Inputs.
4. Pulse, Set ON/OFF of Relay outputs.
5. Launch a Video "Window".

EE. System Status Indicators: The Alarm Monitor will provide status indicators to display current status of multiple elements of The PACS including the following:
1. Total number of pending Unacknowledged Alarms and Events.
2. Status (including off-line, active, and masked) of the following field hardware devices:
    a. Intelligent System Controllers.
    b. Subpanels.
    c. Card readers.
    d. Inputs.
    e. Outputs.
3. Hardware status tab will show devices that are in alarm, as well as on-line /off-line status, for field hardware devices.

FF. Swipe and Show: Supports Swipe and Show functionality that allows display of credential holder's photo as they swipe their badge through a specified card reader.
1. Up to 4 card readers will be active for swipe and show in each browser window.
2. Swipe and Show: Allows Operators to verify the credential holder to their photo as they enter a portal.

GG. Intrusion Panels: Allows Operators to monitor intrusion panel statuses as well as monitoring and controlling related points, areas and outputs.
1. Intrusion Panel Statuses:
    a. Operators may sort and search/filter the listed statuses.
    b. For each panel indicate the status of the following:
        1) Battery.
        2) Power.
        3) Tamper.
        4) Phone Line.
2. Intrusion Areas:
    a. Areas will be able to be armed using the following options:
        1) Instant Arm.
        2) Delay Arm.
        3) Force Instant Arm.
        4) Force Delay Arm.
        5) Perimeter Instant Arm.
        6) Perimeter Delay Arm.

7) Perimeter Force Instant Arm.
8) Perimeter Force Delay Arm.

b. Operators may easily disarm areas.
c. Operators may silence alarms.
d. Area details will display the following intrusion area statuses:
1) Armed.
2) Ready to Arm.
3) Not Ready to Arm.
4) Partial Arm.
5) Trouble.
6) Alarm.
e. Operators may sort and search/filter the listed statuses.

3. Intrusion Points:
a. Operators may bypass and unbypass points.
b. Point, area and panel details will display the following intrusion point statuses:
1) Normal.
2) Faulted.
3) Bypassed.
4) Trouble.
c. Operators may sort and search/filter the listed statuses.

4. Intrusion Outputs:
a. Operators will be able to activate and deactivate outputs.
b. Output and panel details will display with the following output statuses available:
1) Inactive.
2) Active.
3) Trouble.
c. Operators will be able to sort and search/filter the listed statuses.

2.10 PACS SOFTWARE, SYSTEM CONFIGURATION AND ADMINISTRATION

A. Provide Administrators with a “localization” function that has the ability to utilize separate languages per identity.
1. Languages supported:
a. English.
b. German.
c. Spanish.
d. French.
e. Italian.
f. Brazilian Portuguese.
g. Russian.

h. Simplified Chinese.
i. Arabic

2. Up to 50 operators can be assigned a predefined language.
3. Languages can be changed from the following locations:
    a. Account View.
    b. Identity profile.

B. Alarm and Event Logging: Track and keep a comprehensive log of alarm and event activity, including the following information:
1. Alarm Name.
2. Time and Date Stamp.
3. Where the alarm occurred.
4. Acknowledgment information.
5. Operator actions associated with alarms or events.

C. Administrators may suppress certain alarms from logging during pre-defined scheduled times of the day.

D. Alarm and Event information can be viewed through the PACS reporting engine that lists total number of alarms and events logged in PACS appliance.
1. The number of stored alarms and events will be limited only by the amount of disk space available in The PACS appliance.

E. Operator Session Timeout / Logout: Supports an Auto Logout feature that allows the system to automatically log an Operator out of the system after a period of inactivity.
1. Provide the following auto logout timeout options:
    a. 10 minutes.
    b. 15 minutes.
    c. 30 minutes.
    d. 60 minutes.
    e. One hour.
    f. Indefinite: A selection available to not log out an Operator regardless of inactivity length.

F. Delegations: Protect permission of Major PACS features and functions through use of delegations.
1. Each Operator Account will be assigned a Role, which includes a list of delegations assigned to that Role.
2. Operator access to PACS screens will be controlled though delegations.
    a. Access includes the Operator's ability to view, add, edit, or delete PACS objects.

G. Software Based Licensing: Supports software-based License Enforcement model.

1. A hardware key or dongle for controlling licensed features and functionality is not allowed.

H. Appliance Diagnostic Information: Supports the ability to analyze real-time diagnostic information for each PACS appliance by viewing the About Page for the appliance.
   1. Diagnostic data includes the following:
      a. Number of days online.
      b. Current load.
      c. Memory.
      d. Disk space usage.
      e. Network communications data.

I. On-Line, Context Sensitive Help: Supports on-line, context sensitive help to assist system users in the operation of the system.
   1. Once inside the help program, users may navigate the help files, moving to other areas of the documentation without having to go back into the application software.
   2. Help files will have links to the table of contents and will have search capability.

J. Operator Accounts: Supports Operator Accounts.
   1. Operator Accounts will require a unique user name password to access the system.
   2. Operator Accounts will be assigned a Role, which determines the permission level for that account.
   3. Modifications to an Operator Account will be reported to the Event Monitor and logged to the LDAP directory structure for audit and reporting processes.
   4. The PACS supports as many Operator Accounts as configured identities.

K. Password Protection: Operator Accounts will require a unique user name and password that would tie that identity to delegation rights to access the PACS.
   1. This denotes Operator access to the following:
      a. Screens the Operator can access.
      b. Tasks the Operator can perform.
   2. An Operator will be able to change their PACS password at any time.
   3. Strong Password parameters will be supported.
      a. Requiring system users to enter at least eight characters.
      b. Include at least one upper case letter, one lower case letter and one numeral.

L. Duplicate PINs: Support the use of duplicate PINs.
   1. When enabled, this feature restricts available door modes to the following:
      a. Card and PIN.

b. Card only.

M. Policies: Support Policies that will act as templates to be applied to field hardware devices in the system to ease in configuration of similar devices.
1. Each Policy will consist of a template for card readers, inputs, or outputs.
2. The PACS will support an unlimited number of policies.

N. Groups: Support Grouping of parameters for ease of configuration, including, but not be limited to, the following Grouping concepts:
1. Roles.
2. Field Hardware Devices.
3. Policies.

O. System Partitioning: Provide the capability for advanced system partitioning.
1. Each partition will be allowed its own group of identities, field hardware, and parameters.
a. Example: Schedules and access groups.
2. Identities will be allowed to belong to one or multiple partitions.
3. Partitioning will provide a flexible "tenant/landlord" architecture whereby partition users can only view, add, modify, and delete identities, system parameters, and field hardware that belong to their respective partitions.
4. PACS Operators may be assigned to more than one partition.
a. A partition may be assigned to more than one Operator.

P. Operator Activity Logging: Track and keep a comprehensive log of Operator Account activities.
1. Changes that occur in directory structure will be logged including the following:
a. Operator Account Login / Logout Activity.
b. Adding, Deleting, or Changing Identity Records.
c. Change to system configurations including the following:
1) Field hardware.
2) Access Groups.
3) Schedules.
d. Activity performed inside the Alarm and Event Monitor including the following:
1) Acknowledging alarms.
2) Opening doors.
3) Clearing events.

Q. Logged activities include, but not be limited to, the following:
1. Operator Account.
2. Date and time of the activity.
3. Activity that was performed.

4. Original data prior to change, if applicable.
5. New data that was updated.

R. Operator Account activity information can be viewed through PACS reporting engine that lists total number of Operator events that are logged in the PACS appliance.
   1. The number of stored Operator Account events will be limited only by the amount of disk space available in the PACS appliance.

S. System Scheduler Utility: Allow System Administrators to schedule actions the following:
   1. On-demand or single-use.
   2. Recurring basis.
   3. Types of actions include the following:
      a. Running reports.
      b. Updating identity profiles.
      c. Apply door modes.
      d. Running global actions.
   4. Scheduling Utility will satisfy a wide range of scheduling needs, including the following:
      a. Hourly: For example, “Every day on the hour”.
      b. Specific Day, specific time: For example, “every Monday at 8:00 am”.
      c. Monthly: For example, “the first Sunday of every month”.
      d. Specific Recurring Date: For example, “Every February 29th @ noon”.
      e. Specific Date in the future: For example, “December 7, 2017 @ 5pm”.
      f. Recurring activities can be set to the following:
         1) A master start and stop date.
         2) Run indefinitely.

T. The Scheduling Utility will provide a job monitor allowing the System Administrator to observe the following:
   1. Status of currently running tasks.
   2. A chronological list of future scheduled tasks.
   3. A history log of completed tasks.

U. Reports: Support a minimum of 28 standard reports as follows:
   1. Administrators may create Reports in the following formats:
      a. PDF document.
      b. Spreadsheet document.
   2. Once a Report is created, the Administrators may take the following actions with the report:

a. Save Report to a file.
b. Print Report to a local or networked printer.

3. Each report will be able to be customized / filtered on relevant data for that particular report.
4. Standard PACS reports will include the following:
    a. Access Grant via Operator Report: The Access Grant via Operator Report will present information on access grant activity that was manually generated by an Operator and will include the door that was opened, time, and Operator executing the door grant.
    b. Access Group Report: Presents information on defined PACS Access Groups, including the following:
        1) Roles that are assigned to group.
        2) Schedule assigned to group.
        3) Number of doors assigned to group.
        4) List of doors assigned to group.
    c. Action Audit Report: Presents information on system events and includes the following information:
        1) Panel date (and UTC date).
        2) Event name and type.
        3) Panel and source names.
        4) Source location and alternative name.
        5) Name of related Operator.
    d. Alarm Report: Presents information on alarms that occurred in the system including the following information:
        1) Panel Name.
        2) Operator action taken.
        3) Operator responding to alarm.
        4) Operator Notes pertaining to alarm.
    e. Appliance Report: The Gateway Report presents information on each defined PACS appliance, including the following:
        1) PACS appliance type.
        2) DNS name and domain.
        3) Local time zone and Daylight Savings Time settings.
        4) List of field hardware manufacturers are enabled.
        5) List of Intelligent Enterprise Controllers are configured to report to the panel.
    f. Area Identity Report: Presents information on Areas. Each area entry will include the following information:
        1) Area name.
        2) Last and first names of the Identity.
        3) Last accessed door and time.

4) Identity type.
5) Token internal number.

g. Area Report: Presents information on defined Areas. Each area entry will include the following information:
1) Area name.
2) PACS appliance where the area exists.
3) Doors assigned to the area.

h. Audit Log Report: Presents information about each change made to The PACS by an Operator. Each Audit log entry will include the following information:
1) A date/time stamp.
2) Description.
3) Operator who made the change.
4) Type of change.
5) Details of the change.
6) Original information prior to the change.

i. Camera Report: Presents information on each camera configured in the system including Camera Name and its attributes.

j. Collaboration Report: Presents information on defined PACS collaboration scripts, including collaboration type and if the collaboration is active.

k. Delegation Comparison Report: Presents information comparing the delegations assigned to each identified role.

l. Delegation Report: Presents information on defined PACS delegation groups, including which identities have been assigned to the delegation and what permission have been configured for that delegation.

m. Door Configuration Report: Presents information on the complete configuration / settings of each door configured in the PACS.

n. Door/Identities with Access Report: Presents information on credential holder access to each door in the PACS, including the schedule that credential holder can access door.

o. Event Report: Presents information on defined events in the system along with their attributes including the following:
1) Event Name.
2) Assigned Event Type.
3) Priority.
4) Masking Schedule.
5) If the event is configured to always mask and log the event.

p. Event Type Report: Presents information on each defined PACS Event Type, including the following:
1) Suppression Schedule.

2) Priority.
3) Retransmission Time.
4) Retransmission Procedure.
5) Procedure.
6) If the Event Type is set to be masked, logged, and sent to the Alarm Monitor.

q. Group Report: Presents information on defined Groups, including the following information:
1) Group Name.
2) Type.
3) Members' information.

r. Holiday Report: Presents information on each defined holiday, including the following information:
1) Date of the holiday.
2) Number of days the holiday is in effect.
3) Holiday type(s) assigned to the holiday.

s. Identity Photo Gallery Report: Presents information on each defined Identity, including first and last names, role and photo.

t. Identity Summary Report: Presents information on each defined Identity with respect to Identity Status and Type, Token(s) issue and expiration date, and which Roles and Access Groups have been assigned to the Identity.

u. Identity/Doors with Access Report: Presents information on each defined Identity with respect to which doors they have access.
1) Reports include the schedule in which access has been granted to each reader as well as the Access Group and Role assignments that allow access to each reader.

v. Panel Report: Presents information on complete configuration/settings of each Intelligent Enterprise Controller configured in the PACS.

w. Policy Report: Presents information on defined policies in the PACS, including the following information:
1) Policy Name.
2) Active Status.
3) Which hardware components the policy encompasses.

x. Role Report: Presents information on each defined Role, including the following information:
1) Parent information.
2) Activation/deactivation dates.
3) Child Roles.
4) Identities assigned to that Role.

5) Access Groups assigned to that Role.
6) Doors assigned to that Role.

y. Schedule Report: Presents information on each defined Schedule, including its mode and each interval configured, and including the following information:
1) Days of the week.
2) Holiday types.
3) Start and end times of the interval.

z. Token Report: Presents information on tokens in the system including the following information:
1) Token number.
2) Identity to whom the token is assigned.
3) Active / de-active status.

aa. Tokens Pending Expiration Report: Presents information on tokens that expire within a defined period, including the following information:
1) Internal number.
2) First and last name of the cardholder.
3) Embossed number.
4) Expiration date.
5) Days until expiration.

bb. Transaction Report: Presents information on each transaction generated at the field hardware level, including the following transaction log event information:
1) Date/time stamp.
2) Event source.
3) Event name and type.
4) Identity and Token information.

cc. Quick Reports: The PACS will support Quick Reports.
1) Each of the standard reports defined in the "Reports" paragraph of this Section will be able to have relevant data filters applied to them, prior to running, in order to provide a report with more specific information than the generic report. Quick Report settings are designed to run once and will not be saved.
2) Administrators may create Quick reports as delimited spreadsheet data or PDF.

dd. Custom Reports: The PACS will support Custom Reports.
1) Each of the standard reports defined in the Reports section will be able to have relevant data filters applied to them,

prior to running, in order to provide a report with more specific information than the generic report.

2) Custom Reports will be designed to run multiple times and will be saved in the Custom Reports form for fast future execution.

3) Administrators may create Custom reports as delimited spreadsheet data or PDF. Each Custom Report will be given a unique name to identify it in the Custom Reports list.

V. Remote Support: The PACS will have remote support capability to allow Value Added Reseller or Manufacturer to access customer's appliance for the following:
   1. Troubleshooting.
   2. Diagnostics.
   3. Load review.
   4. Assistance with configuration.

W. The PACS will offer the ability to obtain software log data out of the system appliance Logs for further application support.

X. Grid Based Replication: The PACS will support automated grid based replication architecture of the appliance directory structure for customers that deploy multiple appliances.
   1. Replication architecture will be peer-to-peer and not require a dedicated database server to enable replication of identities and configuration data across appliances.
   2. The PACS will support encrypted communications between appliances using SSL Encryption.
   3. Replication will allow the LDAP data of appliances to be synchronized with each of the others in the system, allowing for the PACS appliance to rebuild itself from replicated data found on another appliance found in the system.

Y. Hot Standby Functionality: The PACS will support a hot standby, auto-failover architecture.
   1. For each appliance, a Hot Standby appliance will be configured to monitor the status of its primary partner device.
   2. Should an appliance fail to function, the hot standby appliance will be able to automatically detect a problem and assume control of the system.

Z. Software Updates: The PACS will support updates by download from software manufacturer's web site, or by receiving emailed update files.
   1. No physical interaction with PACS appliance will be required to perform a successful update and upgrade to system software.

AA. System Backups: The PACS will be able to backup and restore the LDAP directory structure.
    1. Backups will run concurrently with the rest of the system and will not require Operators to log out of the PACS.
    2. Backups will include transaction data and system configuration data.
    3. Appliance backups be encrypted using AES Encryption.
    4. Appliance backups to the following:
        a. USB Storage Device.
        b. Windows shared Directory or network shared folder.
        c. Secured SCP servers.
    5. Backups will be performed as follows:
        a. Automatically on a predefined daily schedule.
        b. Manually via the user interface.

BB. Elegant Restart and Shutdown of Appliance: The PACS will support Elegant Restart and Shutdown capabilities of the Appliance.
    1. The PACS User Interface will support both re-start and shutdown of the Appliance.
    2. Rights and access to re-start and shutdown of the Appliance will be denoted by login.

CC. Global Time Display: The PACS will support localized date and time display.

DD. System Data Logs: The PACS will support system data logs to assist with diagnostics and troubleshooting.
    1. Standard logs will include the following:
        a. Web server logs.
        b. Field hardware communication logs.
        c. System software logs.
        d. System transaction logs.
    2. Logs will be viewable in a plain text format.

2.11 PACS SOFTWARE, THIRD PARTY COLLABORATION UTILITY

A. The PACS will support a Collaboration utility that will allow for real-time or scheduled transfer of information, including images and events, between the PACS and third-party IT, Security, and other systems.

B. A user interface will allow for the generation of import and export collaborations.
    1. A Start and Stop date will be applied to run the Collaboration during the scheduled intervals only between certain dates.

C. The PACS will support a minimum of 32 Collaborations per PACS appliance.

D. The PACS will support the following Collaboration Types:

1. Events:
    a. Arcsight CEF.
    b. Generic XML.
    c. Splunk.
2. Identity:
    a. CSV Export.
    b. CSV One-time Long format.
    c. CSV One-time Short format.
    d. CSV Recurring.
    e. LDAP pull.
    f. Oracle RDBMS pull.
    g. SQL Server pull.

E. Identity Pulls: Identity Pull Collaborations will allow Identity, Token, and Role related data to be imported into the system directory structure.
    1. Importing information will occur in the following method:
        a. Add/Modify: If a record in the file exists in the directory structure, it will be replaced according to the layout configuration specified.
        b. Records that don't already exist will be added to the directory structure.

F. Identity Pull Collaborations will support BLOB image file formats to be imported into the Open LDAP directory structure.

G. Ability to encrypt exported Identity information will be available using SSL encryption.

H. Each collaboration will utilize an error log that will report errors that occur during a file import.
    1. Errors can then be viewed from this log and once corrected the import may be run a second time to download the corrected records.

I. As a Collaboration Pull completes, imported changes will be automatically downloaded to Intelligent Enterprise Controllers on a real-time basis as information is being imported into the directory structure.

J. Event Pushes: Event Push Collaborations will allow alarm and events to be exported from the PACS to other third party reporting engines.

K. Each Event Push Collaboration will be defined with specific Event Types to be exported along with the schedule in which they are to be exported.

L. Events will have the option to be exported with detailed alarm response information including Acknowledgments, Clears, and Operator Notes.

M. Data Filters: Collaborations will allow Administrators to select a subset of data for export or import operations.
   1. Filters will be used do define which records would be selected for the import or export.

2.12 MISCELLANEOUS SOFTWARE

A. Reader Software: AC-SW-16RCU, 16 Reader expansion software for increasing the overall count of readers the system is capable of managing.

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 IDENTIFICATION

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 PROTECTION

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

3.7 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.**
   5. **Corporate management.**

3.8 DEVICE CONFIGURATION BACKUP:

A. **Using ACM backup functionality, perform a full system backup at the completion of the initial programming to a USB drive or customer local network shared folder (preferred option). Backup function could also be scheduled to execute system backup periodically.**

B. **Deliver configuration backup files, restoration application and instructions detailing for restoration of back-up configuration.**

3.9 FINE TUNING:

A. **Perform field software changes after initial programming session to "fine tune" operating parameters and sequence of operations based on any revisions to Owner's operating requirements.**

END OF SECTION

SECTION 281500 - ACCESS CONTROL HARDWARE DEVICES

PART 1 - GENERAL

1.1 SUMMARY

A. Section Includes:

1. Card readers, credential cards, and keypads
2. Cables
3. Transformers

1.2 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 PC-to-controller communications link, with additional controllers at the Location connected to the PC-to-controller link with a TIA 485-A communications loop. Where this term is presented with an initial capital letter, this definition applies.

E. PC: 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.

1.3 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 including the following:

    a. Workstation outlets, jacks, and jack assemblies.
    b. Patch cords.
    c. Patch panels.

4. Cable Administration Drawings: As specified in "Identification" Article.
5. Battery and charger calculations for central station, workstations, and controllers.

C. Product Schedules.

D. Samples: For workstation outlets, jacks, jack assemblies, and faceplates. For each exposed product and for each color and texture specified.

1.4 INFORMATIONAL SUBMITTALS

A. Field quality-control reports.

1.5 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. Hard copies of manufacturer's specification sheets, operating specifications, design guides, user's guides for software and hardware, and PDF files on USB media of the hard-copy submittal.

2. System installation and setup guides with data forms to plan and record options and setup decisions.

1.6 QUALITY ASSURANCE

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

1.7 DELIVERY, STORAGE, AND HANDLING

A. Store in temperature- and humidity-controlled environment in original manufacturer's sealed containers.

B. 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.

C. 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.

D. Save original manufacturer's containers and packing materials and deliver as directed under provisions covering extra materials.

1.8 PROJECT CONDITIONS

A. Environmental Conditions: System shall be capable of withstanding the following environmental conditions without mechanical or electrical damage or degradation of operating capability:

1. Control Station: Rated for continuous operation in ambient conditions of 60 to 85 deg F and a relative humidity of 20 to 80 percent, noncondensing.

2. Indoor, Controlled Environment: NEMA 250, Type 1 enclosure. System components, except the central-station control unit, installed in temperature-controlled indoor environments shall be rated for continuous operation in ambient conditions of 36 to 122 deg F dry bulb and 20 to 90 percent relative humidity, noncondensing.

PART 2 - PRODUCTS

2.1 OPERATION

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

2.2 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."

2.3 CARD READERS, CREDENTIAL CARDS, AND KEYPADS

A. Provide HID SE RP40 or mullion style mounted devices (RP10) where existing devices are mullion style.

B. Card-Reader Power: Powered from its associated controller, including its standby power source, and shall not dissipate more than 5 W.

C. Enclosure: Suitable for surface, semi-flush, pedestal, or weatherproof mounting. Mounting types shall additionally be suitable for installation in the following locations:

1. Indoors, controlled environment.

2. Indoors, uncontrolled environment.

3. Outdoors, with built-in heaters or other cold-weather equipment to extend the operating temperature range as needed for operation at the site.

2.4 Card Readers:

1. The card reader shall read cards in a range from direct contact to at least 2 inches from the reader.

B. Communication Protocol: Compatible with local processor.

C. Credential Card Modification: Entry-control cards shall be able to be modified by lamination direct print process during the enrollment process without reduction of readability. The design of the credential cards 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 badge holder used at the site.

2.5 PUSH-BUTTON SWITCHES

A. Camden Door Controls CM-5020RPTE or approved equal

B. Push-Button Switches: Momentary-contact

C. Enclosures: Flush or surface mounting. Push buttons shall be mounted in existing push button enclosures

D. Power: Push-button switches shall be powered from their associated controller

2.6 MOTION SENSORS (Request to Exit)

A. Bosch DS161 Detector mounted in existing back box.

2.7 CABLES

A. General Cable Requirements: Comply with requirements as recommended by system manufacturer for integration requirement.

B. PVC-Jacketed, TIA 485-A Cables:

1. Paired, two pairs, twisted, No. 22 AWG, stranded (7x30) tinned copper conductors.

2. PVC insulation.

3. Unshielded.

4. PVC jacket.

5. Flame Resistance: Comply with UL 1581.

C. Plenum-Rated TIA 485-A Cables:

1. Paired, two pairs, No. 22 AWG, stranded (7x30) tinned copper conductors.

2. Fluorinated ethylene propylene insulation.

3. Unshielded.

4. Fluorinated ethylene propylene jacket.

5. NFPA 70 Type: Type CMP

6. Flame Resistance: NFPA 262, Flame Test.

2.8 TRANSFORMERS

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

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 PCs, controllers, card readers, and other cable-connected devices to verify actual locations of conduit and back boxes before device installation.

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

3.2 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.

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 CABLING

A. Comply with NECA 1, "Good Workmanship in Electrical Construction."

B. Install cables and wiring according to requirements in Section 260519 "Low-Voltage Electrical Power Conductors and Cables."

C. Wiring Method: Install wiring in raceway and cable tray except within consoles, cabinets, desks, and counters and except in accessible ceiling spaces and in gypsum board partitions where unenclosed wiring method may be used. Use NRTL-listed plenum cable in environmental airspaces, including plenum ceilings. Conceal raceway and cables except in unfinished spaces. Conceal wiring within wall from ceiling space to devices.

D. Install LAN cables using techniques, practices, and methods that are consistent with Category 5e rating of components and optical fiber rating of components, and that ensure Category 6 and optical fiber performance of completed and linked signal paths, end to end.

E. Boxes and enclosures containing security-system components or cabling, and which are easily accessible to employees or to the public, shall be provided with a lock. Boxes above ceiling level in occupied areas of the building shall not be considered accessible. Junction boxes and small device enclosures below ceiling level and easily accessible to employees or the public shall be covered with a suitable cover plate and secured with tamperproof screws.

F. Install end-of-line resistors at the field device location and not at the controller or panel location.

3.4 CABLE APPLICATION

A. Comply with TIA 569-D, "Commercial Building Standard for Telecommunications Pathways and Spaces."

B. Cable application requirements are minimum requirements and shall be exceeded if recommended or required by manufacturer of system hardware.

C. TIA 485-A Cabling: Install at a maximum distance of 4000 ft. between terminations.

D. Card Readers and Keypads:

1. Install number of conductor pairs recommended by manufacturer for the functions specified.

2. Unless manufacturer recommends larger conductors, install No. 22 AWG wire if maximum distance from controller to the reader is 250 ft. (75 m), and install No. 20 AWG wire if maximum distance is 500 ft. (150 m).

3. For greater distances, install "extender" or "repeater" modules recommended by manufacturer of the controller.

4. Install minimum No. 18 AWG shielded cable to readers and keypads that draw 50 mA or more.

E. Install minimum No. 16 AWG cable from controller to electrically powered locks. Do not exceed 500 ft. (150 m) between terminations.

F. Install minimum No. 18 AWG ac power wire from transformer to controller, with a maximum distance of 25 ft. (8 m) between terminations.

3.5 GROUNDING

A. Comply with IEEE 1100, "Recommended Practice for Power and Grounding Electronic Equipment."

B. Ground cable shields, drain conductors, and equipment to eliminate shock hazard and to minimize ground loops, common-mode returns, noise pickup, cross talk, and other impairments.

C. Bond shields and drain conductors to ground at only one point in each circuit.

D. Signal Ground:

1. Terminal: Locate in each equipment room and wiring closet; isolate from power system and equipment grounding.

2. Bus: Mount on wall of main equipment room with standoff insulators.

3. Backbone Cable: Extend from signal ground bus to signal ground terminal in each equipment room and wiring closet.

3.6 INSTALLATION

A. Install card readers, keypads, and push buttons.

3.7 IDENTIFICATION

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.

3.8 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.

3.9 FIELD QUALITY CONTROL

A. Perform tests and inspections.

1. Manufacturer's Field Service: Engage a factory-authorized service representative to inspect components, assemblies, and equipment installations, including connections, and to assist in testing.

B. Tests and Inspections:

1. LAN Cable Procedures: Inspect for physical damage and test each conductor signal path for continuity and shorts. Use tester approved for type and kind of installed cable. Test for faulty connectors, splices, and terminations. Test according to TIA 568-C.1, "Commercial Building Telecommunications Cabling Standards - Part 1: General Requirements." Link performance for balanced twisted-pair cables must comply with minimum criteria in TIA 568-C.1.

2. Test each circuit and component of each system. Tests shall include, but are not limited to, measurements of power-supply output under maximum load, signal loop resistance, and leakage to ground where applicable. System components with battery backup shall be operated on battery power for a period of not less than 10 percent of the calculated battery operating time. Provide special equipment and software if testing requires special or dedicated equipment.

3. Operational Test: After installation of cables and connectors, demonstrate product capability and compliance with requirements. Test each signal path for end-to-end performance from each end of all pairs installed. Remove temporary connections when tests have been satisfactorily completed.

C. Devices and circuits will be considered defective if they do not pass tests and inspections.

D. Prepare test and inspection reports.

3.10 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.

3.11 DEMONSTRATION

A. Train Owner's maintenance personnel to adjust, operate, and maintain security access system. See Section 017900 "Demonstration and Training."

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.

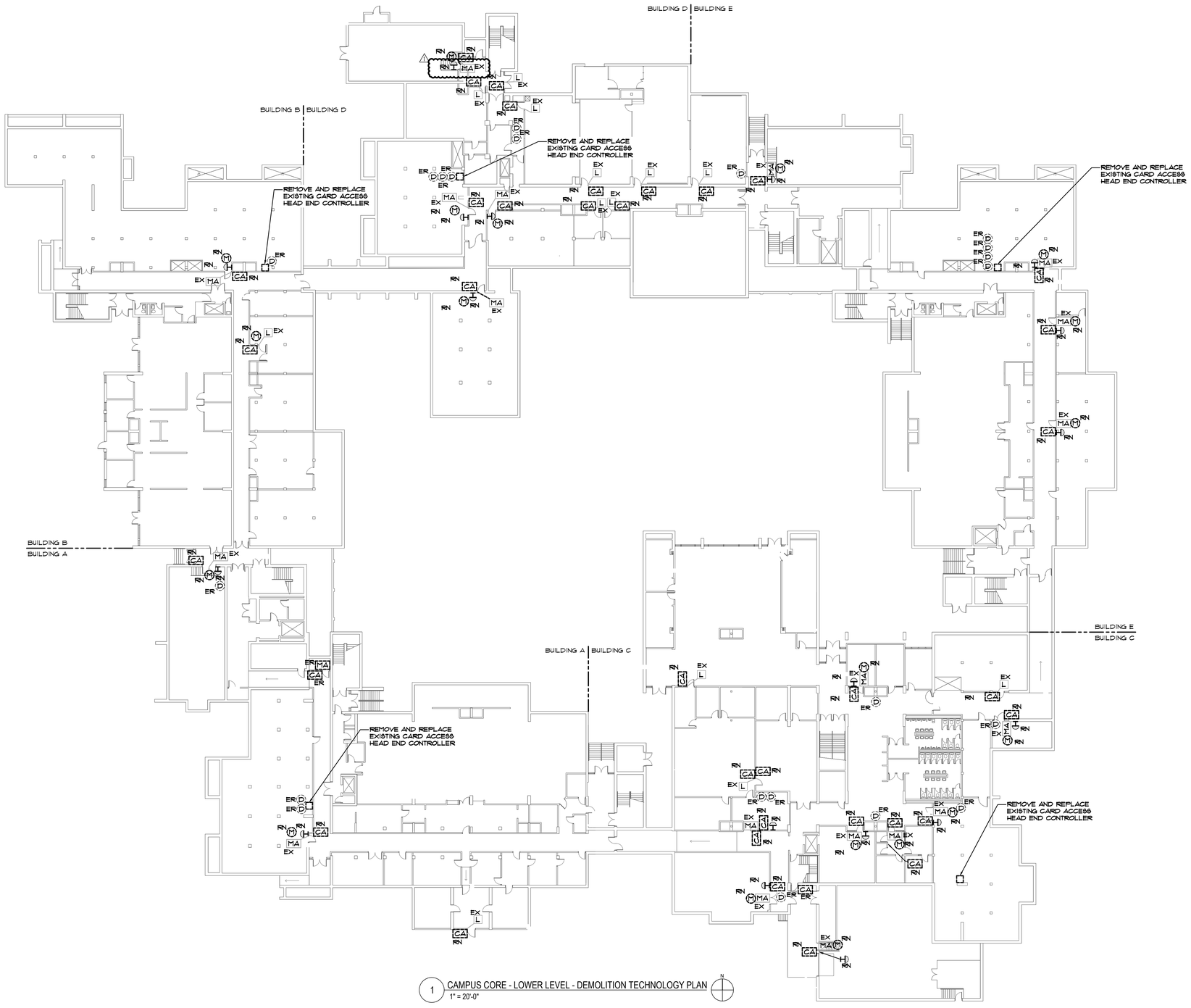
4. Hardware maintenance personnel.

5. Corporate management.

3.12 END OF SECTION 281500

GENERAL NOTES

1. REMOVE ALL EXISTING SERVER EQUIPMENT ASSOCIATED WITH EXISTING DOOR ACCESS CONTROL EQUIPMENT. REMOVE SERVERS, DRIVES, SWITCHES AND ACCESSORIES AS REQUIRED.
2. REMOVE ALL WIRING ASSOCIATED WITH EXISTING DOOR ACCESS HARDWARE BACK TO SOURCE, COMPLETE AS REQUIRED.
   2.1. DEDUCTIVE ALTERNATE - PROVIDE ALTERNATE PRICING FOR THE RE-USE OF EXISTING DOOR ACCESS WIRING IF COMPATIBLE WITH THE NEW CONTROL SYSTEM.
3. PATCH AND REPAIR SURFACE FINISH OF REMOVED DEVICES TO PROVIDE UNIFORM FINISH WITH ADJACENT EXISTING FINISH. WHERE DEVICES ARE BEING REPLACED WITH NEW DEVICES WITH A SMALLER FOOTPRINT, PATCH AND REPAIR SURFACE BEHIND NEW DEVICE AS NOTED ABOVE.
4. REVIEW EXISTING DEVICE CONTROLLERS. ALL DEVICES SHALL BE SERVED BY THE CONTROLLER IN THE SAME BUILDING. SHOULD DEVICES BE SERVED BY A CONTROLLER FROM AN ADJACENT BUILDING, REMOVE EXISTING WIRING AND ROUTE NEW WIRING FROM THE CONTROLLER IN THE BUILDING IN WHICH THE DEVICES ARE LOCATED, COMPLETE AS REQUIRED.



1 CAMPUS CORE - LOWER LEVEL - DEMOLITION TECHNOLOGY PLAN
1" = 20'-0"

ARCHITECT
DEMONICA KEMPER ARCHITECTS
125 N. HALSTED STREET, SUITE 301
CHICAGO, IL 60661
P: 312.496.0000

TECHNOLOGY ENGINEER
MILLIES ENGINEERING GROUP
9711 VALPARAISO DR
MUNSTER, IN 46321
P: 219.595.6500

ILLINOIS VALLEY COMMUNITY COLLEGE
KEY CARD ACCESS UPGRADES

815 N ORLANDO SMITH ST.
OGLESBY, IL 61348
DKA PROJECT NO: 20-026

LICENSED PROFESSIONAL ENGINEER
DAVID G. JANNEY
062-057018
STATE OF ILLINOIS

KEY PLAN:

SHEET STATUS: 02 / 01 / 2021
ISSUED FOR BID

NO:	DESCRIPTION:	DATE:
1	Addendum 1	2/22/2021

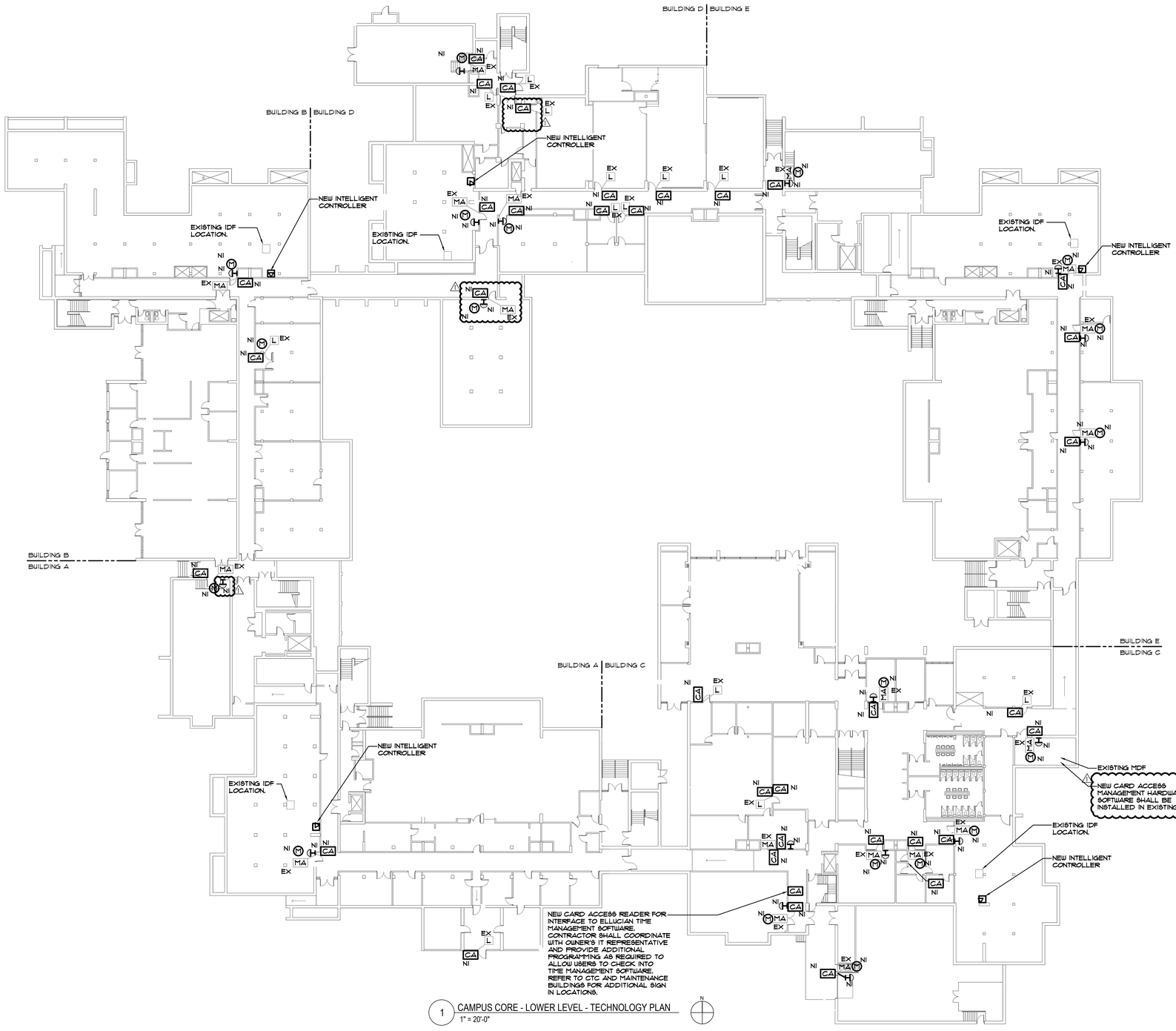
SHEET TITLE:
CAMPUS CORE - LOWER LEVEL - DEMOLITION TECHNOLOGY PLAN

SHEET NUMBER:
E1.10

MILLIES
ENGINEERING GROUP
9711 Valparaiso Drive Munster, Indiana 46321
221 N. LaSalle Street Chicago, Illinois 60601
(219) 924-9400
www.milliesengineeringgroup.com

GENERAL NOTES

1. PROVIDE NEW DOOR HARDWARE CONTROL EQUIPMENT IN EXISTING RACK OR ENCLOSURE. VERIFY CONDITIONS AND REQUIREMENTS IN FIELD, COMPLETE AS REQUIRED.
2. PATCH AND REPAIR SURFACE FINISH OF REMOVED DEVICES TO PROVIDE UNIFORM FINISH WITH ADJACENT EXISTING FINISH. WHERE DEVICES ARE BEING REPLACED WITH NEW DEVICES WITH A SMALLER FOOTPRINT, PATCH AND REPAIR SURFACE BEHIND NEW DEVICE AS NOTED ABOVE.
3. INTERFACE NEW DEVICES WITH EXISTING DOOR OPERATORS AS REQUIRED TO ALLOW EXISTING SYSTEMS TO FUNCTION WITH NEW DOOR ACCESS CONTROLS, COMPLETE AS REQUIRED.
4. ALL NEW DOOR CONTROLLERS IN ROOMS WITH MAGLOCKS SHALL BE LOCATED IN THE HALLWAY OUTSIDE THE ROOM BEING PROTECTED BY THE CARD ACCESS CONTROLLER. LOCATE ABOVE THE CEILING WHERE TILE CEILINGS EXIST.
   - 4.1. FOR DEDUCTIVE ALTERNATE WITH RE-USE OF EXISTING WIRING AND ENCLOSURES, EXISTING ENCLOSURES WITHIN THE ROOM BEING PROTECTED SHALL BE RELOCATED TO THE HALLWAY.
5. WHERE NEW DEVICES ARE TO BE ADDED ON EXISTING WALLS OR DOOR FRAMES, ROUTE NEW WIRING WITHIN WALL TO DOOR MILLION OR BACK BOX.
   - 5.1. ALL NEW CARD ACCESS DEVICES AND ASSOCIATED HARDWARE SHALL BE ROUTED TO THE CARD ACCESS CONTROLLER WITHIN THE SAME BUILDING.



1 CAMPUS CORE - LOWER LEVEL - TECHNOLOGY PLAN
1" = 20'-0"

ARCHITECT
DEMONICA KEMPER ARCHITECTS
125 N. HALSTED STREET, SUITE 301
CHICAGO, IL 60661
P: 312.496.0000

TECHNOLOGY ENGINEER
MILLIES ENGINEERING GROUP
9711 VALPARAISO DR
MUNSTER, IN 46321
P: 219.595.6500

ILLINOIS VALLEY COMMUNITY COLLEGE
KEY CARD ACCESS UPGRADES

815 N ORLANDO SMITH ST.
OGLESBY, IL 61348
DKA PROJECT NO: 20-026

LICENSED PROFESSIONAL ENGINEER
DAVID G. JANNEY
062-057018
STATE OF ILLINOIS

KEY PLAN:

SHEET STATUS: 02 / 01 / 2021
ISSUED FOR BID

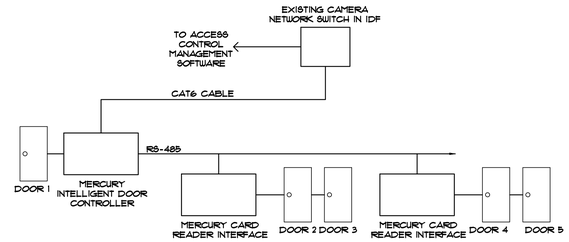
NO:	DESCRIPTION:	DATE:
1	Addendum 1	2/22/2021

SHEET TITLE:
CAMPUS CORE - LOWER LEVEL - TECHNOLOGY PLAN

SHEET NUMBER:
E2.10

MILLIES
ENGINEERING GROUP
9711 Valparaiso Drive Munster, Indiana 46321
221 N. LaSalle Street Chicago, Illinois 60601
(219) 924-8400
www.milliesengineeringgroup.com

WIRING DIAGRAM - BASIS OF DESIGN



ELECTRICAL ABBREVIATIONS

NOTE:
ABBREVIATIONS USED ON DRAWINGS IN GENERAL ARE LISTED BELOW. REFER TO CSI SECTION 01420 FOR ANY ABBREVIATIONS LISTED ON THE DRAWINGS BUT ARE NOT LISTED BELOW.

A	AMPS
AC	AIR CONDITIONING
AFF	ABOVE FINISH FLOOR
AFG	ABOVE FINISH GRADE
BRKR	BREAKER
C	CONDUIT
CH	CABINET HEATER
CKT	CIRCUIT
DISTR	DISTRIBUTION
EF	EXHAUST FAN
ELEC	ELECTRICAL
EM	EMERGENCY
EMT	ELECTRICAL METALLIC TUBING
ER	EXISTING DEVICE TO BE REMOVED
EX	EXISTING DEVICE TO REMAIN
F	FUSE
FS	FUSIBLE SWITCH
G	GROUND
GFI	GROUND FAULT INTERRUPTING PROTECTION
GRC	GALVANIZED RIGID CONDUIT
HP	HORSEPOWER
J	JUNCTION BOX
KVA	KILOVOLT AMPERE
KW	KILOWATTS
MECH	MECHANICAL
MTD	MOUNTED
NE	NEW LOCATION OF EXISTING RELOCATED DEVICE
NIC	NOT IN CONTRACT
NL	NIGHTLIGHT
NTS	NOT TO SCALE
O/C	ON CENTER
P	POLE
PNL	PANEL
PH	PHASE
RR	REMOVE AND RELOCATED EXISTING DEVICE
SW	SWITCH
TYP	TYPICAL
UON	UNLESS OTHERWISE NOTED
V	VOLTS
VIF	VERIFY IN FIELD
W	WATTS
WP	WEATHERPROOF TYPE DEVICE
WG	WIRE GUARD
F4I	FURNISH AND INSTALL

SYMBOL LIST

SIMPLEX DATA OUTLET - WITH ¾" CONDUIT STUBBED INTO ACCESSIBLE CEILING SPACE WITH INSULATED BUSHING - MOUNTED 18" AFF. WHEN MOUNTED ADJACENT TO AN ELECTRICAL RECEPTACLE OR AS NOTED. PROVIDE CAT-6 PLENUM CABLE, FROM EACH JACK, TO NEAREST IDF OR MDF LOCATION INDICATED ON PLANS. TERMINATE WITH RJ-45 JACK. TEST AND LEAVE 10' SLACK LENGTH. PROVIDE 6' PATCH CABLE FOR CONNECTION TO NETWORK SWITCH. COORDINATE CABLE COLOR AND LABELING WITH OWNER'S IT REPRESENTATIVE.

J — JUNCTION BOX - SIZE AND TYPE AS REQUIRED.

CA — CARD ACCESS CONTROLLER - HID SE RP40 - PROVIDE BACK BOX MOUNTED 42" AFF. WITH ¾"C. ROUTED TO THE ACCESSIBLE CEILING SPACE. REFER TO SPECIFICATIONS FOR ADDITIONAL INFORMATION. PROVIDE MULLION STYLE CARD READER WHERE EXISTING MULLION READERS ARE PROVIDED. REFER TO SPECIFICATIONS FOR ADDITIONAL INFORMATION

L — ELECTRIC DOOR STRIKE (HES 5000) - STUB ¾" CONDUIT FROM THE ACCESSIBLE CEILING SPACE TO THE DOOR MULLION FOR WIRING. ROUTE PLENUM RATED RS-485 WIRING FROM THE DOOR STRIKE TO THE DOOR ACCESS SYSTEM FOR A COMPLETE AND PROPERLY OPERATING SYSTEM. PROVIDE 5201 FACEPLATE WITH SATIN STAINLESS STEEL FINISH

MA — ~~ELECTRIC MAGNETIC LOCK (MAG LOCK) - STUB ¾" CONDUIT FROM THE ACCESSIBLE CEILING SPACE~~ TO THE DOOR MULLION FOR WIRING. INTERFACE WIRING TO THE DOOR ACCESS SYSTEM FOR A COMPLETE AND PROPERLY OPERATING SYSTEM.

M — ACCESS CONTROL (REQUEST TO EXIT) MOTION SENSOR - STUB ¾" CONDUIT FROM THE ACCESSIBLE CEILING SPACE TO THE DOOR MULLION AS REQUIRED FOR WIRING. INTERFACE WIRING TO THE DOOR ACCESS SYSTEM FOR A COMPLETE AND PROPERLY OPERATING SYSTEM. REFER TO SPECIFICATIONS FOR ADDITIONAL INFORMATION.

D — EXISTING DOOR CONTROLLER TO BE REMOVED FOR ALTERNATE DEDUCTION. RE-USE EXISTING DOOR CONTROLLER ENCLOSURES IN ROOMS WITH MAG LOCK ACCESS. EXISTING DOOR CONTROLLERS TO BE RE-USED SHALL BE RELOCATED INTO HALLWAY (ABOVE TILE CEILING WHERE APPLICABLE).

REQUEST TO EXIT MOMENTARY CONTACT BUTTON - CARDEN SH-SD0RPTE - STUB ¾ CONDUIT FROM THE ACCESSIBLE CEILING SPACE TO THE DOOR MULLION AS REQUIRED FOR WIRING. INTERFACE WIRING TO THE DOOR ACCESS SYSTEM FOR A COMPLETE AND PROPERLY OPERATING SYSTEM. REFER TO SPECIFICATIONS FOR ADDITIONAL INFORMATION.

RN — ~~REMOVE EXISTING DEVICE AND REQUIRE NEW AS INDICATED~~ IN EXISTING BACK BOX, JUNCTION BOX, ETC. VERIFY EXACT LOCATION AND CONDITIONS IN FIELD. MODIFY EXISTING BACK BOX, JUNCTION BOX, ETC. PROVIDE TRIM PLATES, EXTENSION RINGS, ETC. AS REQUIRED TO MOUNT NEW DEVICE AS INDICATED.

NI — F4I NEW DEVICE AS INDICATED.

EX — EXISTING LIGHTS, RECEPTACLES, SPECIAL SYSTEMS, DEVICE, ETC. TO REMAIN.

ER — EXISTING LIGHTS, RECEPTACLES, SPECIAL SYSTEMS, DEVICE, ETC. TO BE REMOVED COMPLETE IN ITS ENTIRETY. REMOVE ALL ASSOCIATED SURFACE MOUNTED CONDUIT, OUTLETS, ETC. AND BLANK-OFF FLUSH WITH NEW OR EXISTING CONSTRUCTION. SEE GENERAL NOTES AND SPECIFICATIONS FOR ADDITIONAL INFORMATION.

ARCHITECT
DEMONICA KEMPER ARCHITECTS
125 N. HALSTED STREET, SUITE 301
CHICAGO, IL 60661
P: 312.496.0000

TECHNOLOGY ENGINEER
MILLIES ENGINEERING GROUP
9711 VALPARAISO DR
MUNSTER, IN 46321
P: 219.595.6500

ILLINOIS VALLEY COMMUNITY COLLEGE
KEY CARD ACCESS UPGRADES

815 N ORLANDO SMITH ST.
OGLESBY, IL 61348
DKA PROJECT NO: 20-026

LICENSED PROFESSIONAL ENGINEER
DAVID G. JANNEY
062-057018
STATE OF ILLINOIS

KEY PLAN:

SHEET STATUS: 02 / 01 / 2021
ISSUED FOR BID

NO:	DESCRIPTION:	DATE:
1	Addendum 1	2/22/2021

SHEET TITLE:
ELECTRICAL DETAILS

SHEET NUMBER:
E3.00

MILLIES ENGINEERING GROUP
9711 Valparaiso Drive Munster, Indiana 46321
221 N. LaSalle Street Chicago, Illinois 60601
(219) 924-8400
www.milliesengineeringgroup.com

DEMONICA KEMPER ARCHITECTS
125 North Halsted Street, Suite 301 Chicago, Illinois 60661 T 312.496.0000 | F 312.496.0001
www.dka-design.com

Illinois Valley Community College
Key Card Access Upgrades
Pre-Bid Meeting Minutes

February 10, 2021 at 10:00 am at Illinois Valley Community College:
815 North Orlando Smith Road
Oglesby, IL 61348
Room: Fireplace Lounge

Plans and Project Manual available from Cross Rhodes Repro, 30 Eisenhower Lane North, Lombard, IL 60148
Phone 630.963.4700: Fax: 630.598.0317

Bidding Documents may also be examined at the following locations: the office of the Architect; Greater Peoria Contractors & Supplier Association, 1811 West Altorfer Drive, Peoria, IL; Illinois Valley Contractor's Association, 1120 First St., LaSalle, IL; Contractors Association of Will & Grundy Counties, 233 north Springfield Ave, Joliet, IL; www.dodge.construction.com; and www.reedplans.com.

1. Bidders assume all responsibility for their choice of carrier if they choose to have their bids delivered to the College.

2. Bids are due to IVCC, on **February 25, 2021 at 2:00 pm**. Any bids received by IVCC after this time will be returned to the bidder unopened.

   Bids shall be submitted on or before the specified closing time in a sealed envelope addressed to: Michelle Carboni, Director of Purchasing, Room C343, Third Floor of Building C, Illinois Valley Community College.

   a. Submit the bid in an **opaque sealed envelope**. On the envelope include the following:
      i. Bidder name and address, Bid title, Bid opening time and date.
   b. Fax and email copies of bids **WILL NOT** be accepted.
   c. **Three copies** of the bid shall be submitted (one original, two copies). Refer to the specifications for all the information required to be submitted.
   d. The following documents must be fully completed and shall be submitted with the bid.
      i. Document 00 41 13 – Bid Form
      ii. Document 00 43 13 – Bid Bond
      iii. Document 00 43 25 - Substitution Sheet
      iv. Document 00 45 19 - Bidder Eligibility and Non-Collusion Affidavit

3. **A bid bond in the amount of 10%** of the bid shall be submitted with the bid, made payable to Illinois Valley Community College.

4. The last day for submittal of questions regarding the Bidding Documents is **Wednesday, February 17th, 2021 at 5:00 pm.** The last addendum will be issued on **Monday, February 22nd, 2021** to address any questions raised by bidders. A copy of the minutes from this Pre-Bid Conference will be issued along with the addendum.

5. Proposals shall be publicly opened and read aloud in Room C326 immediately after the deadline for submittal.

6. **Bids will be required to be held for 90 days after the due date**.

7. **General contractors will be required to identify their subcontractors prior to award of the contract**.

8. All contractors and subcontractors are required to **pay prevailing wages** in accordance with the specifications and the Illinois Department of Labor.

9. **AIA Document A201** – General Conditions of the Contract for Construction for this project is included in the specifications.

10. **Two (2) alternate bids** are requested on the Bid Form and are described in the specifications.
    Alt Bid #1: For eliminating the liquidated damages clause from the contract ($500 per day)
    Alt Bid #2: For re-using existing door controller cabinets and existing wiring within the campus core (excluding the CTC and Satellite Buildings)

11. **A performance bond and labor and material payment bond in the amount of 100%** of the bid amount will be required to be submitted by the successful bidder upon award of the contract.

12. The apparent low bidder will be asked to produce a copy of **AIA Document 305 – Qualification Statement Form** immediately after the bid opening in order for a recommendation to be made to the Illinois Valley Community College Board of Trustees.

13. It is planned that a contract will be awarded to the successful bidder at the **March 11th Board Meeting.**

14. **Commencement** of work on-site is **March 15th, 2021**.

15. **Substantial Completion** is **July 2nd, 2021**.

16. It is mandatory that all Bidders examine the project site before submitting a bid. A visit to the project site may be arranged for Bidders by contacting Mr. Scott Curley, Director of Facilities; 1-815-224-0301.

17. **Project Description**

    a. This project consists of the campus-wide upgrades to security access control systems, including replacement of existing access control panels, access controllers, door controllers, card readers, and associated cabling.

18. Questions regarding the bidding documents or bidding procedures shall be directed to **Frank Carello at Demonica Kemper Architects**. Email: fcarello@dka-design.com; phone: 312.994.9972.

    a. **All questions must be submitted in writing via EMAIL, no phone conversations questions will be accepted.**

19. Walk through of Project Work Areas.

DEMONICA KEMPER ARCHITECTS
125 North Halsted Street, Suite 301 Chicago, Illinois 60661 T 312.496.0000 | F 312.496.0001
www.dka-design.com

Pre-Bid Conference Sign-In Sheet

Client: IVCC **Project:** Key Card Access Upgrades **Project No.:** 20-026

Date: February 10, 2021

	Name	Company	Trade	Contact (tel or e-mail)
1	Chris Cooper	Tri-Electronics		Chris@Tri-E.com
2	Mike Thompsin	Total Automation Concepts		MThompson@ta-concepts.com
3	Chad McCollom	Emperial Surveillance		Chad@imperialcctv.com
4	Alyssa Conejo	Imperial Surveillance		alyssa@imperialcctv.com
5	Monica Watson	midwest Integrated sautions		mwatson@midwestintegrated.com
6	FRANZ CARELO	DKA		
7	DOMINICIK DEMONICA	DKA		
8				
9				
10				
11				
12				
13				
14				
15				

DEMONICA KEMPER ARCHITECTS
125 North Halsted Street, Suite 301 Chicago, Illinois 60661 T 312.496.0000 | F 312.496.0001
www.dka-design.com

Pre-Bid Conference Sign-In Sheet

Client: IVCC **Project:** Key Card Access Upgrades **Project No.:** 20-026

Date: February 10, 2021

	Name	Company	Trade	Contact (tel or e-mail)
1	Michael Henson	Thompson Electronics Co.	Security Integrator	jmh@thompsonet.com
2	Ozzie Mata	Guardwell Systems	Integrator	ozzie@guardwellsystems.com
3				
4				
5				
6				
7				
8				
9				
10				
11				
12				
13				
14				
15				