PART I GENERAL

* 1. **SECTION INCLUDES** 
     1. Access Control System Architecture
     2. Required Access Control Features
     3. Access Control User Interface
     4. Peripherals for Access Control Systems Including Field Devices
     5. Compatible Products
     6. Electrified Locking Hardware
     7. Client and Server Hardware
     8. Power Supplies
     9. Cabling
  2. **SCOPE OF WORK**
     1. Select from one of the following to describe the contractor’s scope of work.
        1. Provide a design / build, standalone, IMRON Corporation UNITYIS® access control system.

~OR~ (use the option immediately above or immediately below)

* + 1. Expand the Owner’s existing IMRON Corporation UNITYIS® access control system.
       1. Provide all requirements for an access control system that functions as stated in 1.03 System Function below.
       2. Provide infrastructure, conduit and pathway, back boxes, cabling, documentation and training.
       3. Terminate cabling to electrified locking hardware provided by others (If provided by Division 8 contractor).

~OR~ (use the option immediately above or immediately below)

* + - 1. Provide electrified locking hardware.
      2. Provide connectivity and communications with existing UNITYIS® access control database via LAN or WAN (If expanding an existing system). Provide all required communications, accessories, connectivity and service plans to properly interconnect system components locally and wide area.
      3. Provide access control system controllers, panels, input and output assemblies, communications devices, enclosures, cable management, wireways, power supplies (Or POE switches), battery backup, surge protection and tamper protection.
         1. Provide battery backup sufficient for one of the following:

Four (4) hours of full operation including both panel and electrified locking hardware.

Graceful shut down of servers.

Riding through backup generator startup cycle.

* + 1. Provide (#) access control credentials.
    2. Provide access control server and (#) client workstations.

~OR~ (use the option immediately above or immediately below)

* + 1. Configure Owner provided access control server and client workstations. Make sure cloud instance is specifically called out.
    2. Provide access control field devices including card readers, request to exit devices (only if intrusion alarm requires shunting), door position sensors, and end of line resistors.
    3. Provide peripheral devices such as remote door release buttons, duress alarm buttons and audible alarm buttons.
    4. Provide all materials, equipment, hardware, software, modules, accessories, and other options required to deliver a complete turn-key System.
    5. Provide expansion capability so that total credential reader, input, and output capacity is no more than at 50% capacity after install.
    6. Interfaces with other systems.
       1. Automated Door Operators
          1. Provide and configure interface and cabling to Automated Door Openers (Provided by others).
          2. Provide door integration boards to ensure door operators do not fight electrified locking hardware if automated door openers do not explicitly state this is an included function.
       2. Intrusion Detection System
          1. Provide cabling and double pole double throw (DPDT) door position sensors for monitoring of door position sensors individually by the access control system and intrusion alarm system (If required).
          2. Provide interface for arming and disarming the intrusion alarm system as well as resetting intrusion alarm status from the access control user interface and with access control readers at each intrusion alarm keypad.
       3. Video Surveillance System
          1. Call up live or recorded video.
          2. Link cameras stream to any access control device.
       4. Security Intercom System
          1. Provide a software interface to allow for remote unlocking of access-controlled doors or camera callup at intercom locations.
          2. Provide operator interaction as defined by the user for events / alarms generated through the intercom System. This interaction shall have the same as any alarm response structured by the user for operator response.
          3. Provide SIP telephone integration.
       5. Elevator control
       6. Parking control gates
       7. Fire alarm system
    7. Provide Warranty as specified in Section 1.10 below.
    8. Provide expansion capability of a minimum of 15% for future growth, including spare positions in wall fields and panels as well as space in cable distribution and riser pathways.
  1. **SYSTEM FUNCTION**
     1. The access control system shall allow entry into electronically locked spaces after presenting a valid access control credential to an access control reader controlling an area they are authorized to enter.
     2. The access control system shall be compatible with the owner’s current [ ] credentials (If owner has existing card stock).
     3. The access control system shall allow administrators to view or review access control and intrusion alarm events, conduct investigations and provide an audit trail of recorded events.
        1. The access control system shall allow administrators to view or review access control events, conduct investigations and provide an audit trail of recorded events over a mobile device.
        2. Remote viewing of live or recorded video and administration of system shall be available on tablet, or cell phone.
     4. The access control system shall monitor door position.
     5. The access control system shall monitor door forced conditions for when an intrusion alarm is set, and no authorized card read or request to exit signal occurs. Only if doors include REX devices for magnetic locking hardware and door forced alarms are being monitored.
     6. The System shall use a flexible, modular method of defining ‘who’, ‘where’ and ‘when’ a credential will be authorized access or egress secured locations within a defined site.
     7. As a credential is entered into the database the System shall automatically build a record and allow an authorized operator to assign access privileges.
     8. Assigning an ‘Access Level’ to a credential record defines ‘where’ that credential will have access within the facility or facilities.
     9. The System shall allow for an automatic Temporary Access start and stop date to be configured.
     10. The System shall allow for assigning a ‘Time Schedule’ to readers and credentials and define ‘when’ a credential will have access within the facility or facilities.
     11. The system shall be capable of interfacing with the video surveillance system and calling up camera views at associated doors or locations on an operator command, upon presenting a credential or on intrusion alarm.
     12. The system shall be capable of arming and disarming the intrusion alarm system as well as resetting intrusion alarm status from the access control user interface and with access control readers at each intrusion alarm keypad.
     13. The system shall be capable of affecting access control operation for selected intrusion detection or lockdown system events.
     14. System shall be capable of unlocking and re-locking Doors and Door Groups upon command from Operator Workstation. A command shall be capable of being executed by an authorized operator from pull-down menus, icons on status screens, text lines on event screens and icons on Custom Map Displays.
     15. The System shall automatically disable Door Forced conditions and ‘Door Open / Door Held’ conditions from doors that have been unlocked by an operator command.
     16. The System shall be capable of automatically unlocking and re-locking Doors and/or groups of Doors based on Time Schedule and Intervals. The System shall be capable of automatically disabling Door Forced conditions and Open-Too-Long conditions for Doors that have been unlocked by Time Schedule and Intervals.
     17. The System shall provide the capability to selectively disable Doors upon command from designated Operator Workstations based on operator profile, user name and password. Disabled Doors shall deny access to all credentials.
     18. The system shall be capable of responding to selected intrusion detection or lockdown system events generated by Emergency Notification System & Crisis Alert Software (Mass Notification).
     19. Coordination.
         1. Coordinate design, mounting, and support of equipment.
         2. Coordinate installation of required support devices and set sleeves in cast-in-place concrete, masonry walls, and other structural components as they are constructed.
         3. Coordinate access routes through the construction and equipment move-in.
         4. Coordinate location of access panels and doors for concealed equipment. Access doors and panels are specified in Division 08, Openings.
         5. Coordinate work from other divisions including rough in and equipment connections prior to performing work.
         6. Coordinate device finishes with Owner or Architect. Match finish with surrounding surfaces.
     20. Software level Integrations:
         1. Milestone Video. Hanwha, Vivotek, Rhombus, Axis, Arcules, SpotAI, CoremAI.
            1. Allow activation of a “virtual” monitor point when intercom sub-station call button is pressed, to allow initiation of camera call-ups and other events.
         2. Zenitel Intercom.
            1. Allow initiation of conversations and camera callup from internal or external devices as if part of a telephone, software or other communications.
         3. Intrusion alarm
            1. Bosch G & B Series Panels
            2. Elk M1 Panels
  2. **RELATED SECTIONS**
     1. Division 1, General Requirements
     2. Division 8, Door Hardware
     3. Division 26, Electrical
     4. Division 27, Communications
     5. Division 28, Electronic Safety and Security
     6. Division 32, Civil
  3. **REFERENCE STANDARDS**
     1. NFPA 70 - National Electrical Code.
     2. NFPA 101 - Life Safety Code.
     3. UL 294 - Access Control System Units.
     4. UL 1076 - Proprietary Burglar Alarm Units and Systems.
  4. **CONTRACTOR QUALIFICATIONS**
     1. The contractor shall be fully capable of installation, coordination, programming, and configuration of all aspects of the access control system and scope of work defined above.
     2. The contractor shall have a minimum of five years’ experience in the design, installation, testing, and maintenance of electronic access control systems.
     3. The contractor shall have experience with three or more access control system installations of comparable size, complexity, and type to the design specified.
     4. The contractor shall employ a minimum of three limited energy technicians licensed in the state where work is to be performed and located within 120 miles of the project location.
     5. The contractor shall be a factory trained and fully authorized dealer for IMRON UNITYIS® access control.
     6. The contractor shall maintain a local service facility within 120 miles of the project location and which stocks spare devices and/or components for servicing systems.
     7. The contractor shall be able to respond to service calls within (72, 24, 4) hours of initial service call during warranty period.
  5. **SUBMITTAL REQUIREMENTS**
     1. Submit with Bid or Proposal
        1. Provide three references for systems of comparable size, complexity, type and design as specified herein and at least one year after owner’s final acceptance. Include the names, locations, and point of contact for these installations as a part of the initial submittal documentation.
        2. Provide evidence that bidder is a factory trained and fully authorized dealer of manufacturer of the product proposed (IMRON UNITYIS®).
  6. **ADMINISTRATIVE REQUIREMENTS**
     1. Review Drawings of other trades and Owner provided equipment to avoid conflicts.
     2. Report potential conflicts to Architect, provide resolution prior to rough-in or installation.
     3. Verify the physical dimensions of equipment to fit the space available and reserved for security.
  7. **QUALITY ASSURANCE**
     1. Perform work in accordance with contract documents and governing codes and standards.
     2. Installed cabling systems shall not generate nor be susceptible to harmful electromagnetic emission, radiation, or induction that degrades cabling systems.
     3. Provide expansion capability of a minimum of 15% future growth.
     4. Visibly damaged goods are to be returned to the supplier and replaced at no additional cost to the Owner.
     5. Provide UL and/or ETL approved and labeled in accordance with NEC for products where labeling service normally applies.
     6. Materials and equipment provided shall be off the shelf and not special order or customized.
     7. Materials and equipment shall be readily available through manufacturers and/or distributors.
  8. **WARRANTY**
     1. Refer to Section 280500 Common Work Results for Life Safety and Security.
     2. Provide a written guarantee covering the work and equipment called out in this specification for a period of one calendar year from the date of acceptance or substantial completion by the Owner, and as required by the Contract General Conditions.
     3. Correct warranty items promptly upon notification and until:
        1. Free of defects of material and workmanship and in accordance with the Contract Documents.
        2. Delivering the full rated capacity at the efficiency for which it was designed.
  9. **SUBSTITUTIONS** 
     1. No substitution allowed for access control software.
     2. Controllers or field devices may be substituted when identified as “or approved equal” in PART II below.
        1. Proposed alternate equipment must meet specified requirements and requires written approval by Owner prior to ordering.
        2. Proposed equipment shall not void or change manufacturer’s warranty.
        3. Additional work performed by the Contractor will not be paid by Owner without signed approval of these changes prior to implementing changes. Submit a copy of signed change order upon billing.

PART II PRODUCTS

Manufacture’s verbiage in part II define the system and are useful in differentiating UNITYIS® from other manufacturer’s offerings. For owner bid projects, the exact verbiage can be used. For public and open bid projects, then less exclusive language can be used.

Add features section or put sections from existing here for features we want as a differentiator. Refer to specific sections below.

* 1. **REQUIRED ACCESS CONTROL SYSTEM ARCHITECTURE**
     1. The System shall be used to provide scalable access control, alarm monitoring, video integration, photo identification badging, and security control functions within the user’s facility or facilities.
     2. The System shall make use of flexible ‘Open Hardware Protocol’ architecture as well as having an ‘Open Database Connectivity’ (ODBC) compliant system design. System architecture shall facilitate sharing data with external databases and integration of a wide range of security hardware.
        1. Supported hardware shall include Mercury controllers, Azure Controllers, HID VertX EVO and EDGE EVO, ZKTeco USA, ASSA ABLOY Wireless and PoE Locks and the ELK M1 Panel without requiring customized protocols.
        2. Supported databases shall include MariaDB, mySQL, Postgre SQL, Microsoft SQL Express, and Microsoft SQL Server.
        3. Supported database management applications shall include Microsoft Management Studio or HeidiSQL.
     3. The UNITYIS® system shall have the ability to import access control data including personnel, hardware, and time schedules to be used for upgrading existing systems from other manufacturers.
        1. The UNITYIS® system shall have the ability to import and export personnel information based on time schedules, TCP commands, and file date/time modification.
        2. The UNITYIS® system shall have the ability to import using ODBC, Active Directory, LDAP, Text or CSV file.
     4. The System shall provide the ability to ‘Import’ information into the Security Management System host computer from existing data-compliant personnel databases to minimize required manual data entry. the need for persons managing the access control System to manually enter data.
        1. The UNITYIS® system shall have the ability to import information from the databases for the initial load of the credential database; and periodically for major loads of new information.
        2. The UNITYIS® system shall have the ability to update the credential database based on the import of an ‘Exception File’ reflecting changes in employee status.
        3. The UNITYIS® system shall have the ability to import exception files and allow the System to automatically add credential records, delete credential records, modify access privileges, and change other information contained in the credential database. The System shall allow the import of an exception file based on user requirements and existing database application capability.
        4. The System shall allow scheduling of minute by minute, hourly or daily imports.
        5. The System shall allow the import utility to be configured as a Windows Service.
     5. The System shall allow for Human Resource (HR) Integration such as PeopleSoft HCM through the available API/SDK from the HR system for bidirectional updates.
        1. New employee/user entered in the HR system will automatically add new records in the System thru the HR Integration.
        2. Updates to employee/user in HR system will automatically update changes of the record in the System thru the HR Integration.
        3. Deletion of employee/user in HR system will automatically disable/delete record in the System thru the HR Integration.
        4. The System shall not require a System restart or ‘reboot’ in order for data imports or updates to the credential record database to take effect — updates shall be made automatically upon receipt of data if configured by the user.
     6. The system shall support mobile credentials and provide commands for activating and revoking mobile credentials.
     7. The System shall support the option to either run in the cloud as a hosted solution or on-premises.
     8. The System shall be supplied using “standard” English text. At minimum, French, Spanish, Italian and German shall also be required.
     9. The system shall have a complementary support site that is accessible on the internet. The support site should have technical information, system instruction and troubleshooting information. This site should not require a user login and should be available in multiple languages.
     10. The security management system shall consist of the following basic components:
         1. Field Hardware: Field panels, shall be used to support access control, alarm monitoring, video interface and facility control (relay output control) functions within the defined facility or facilities as specified. An Intelligent System Controller shall serve as a distributed database management controller linking device sub-control modules, which connect to credential readers, monitor point inputs, and system outputs. The intelligent controllers shall support multiple device sub-controllers on an IEEE standard RS-485 parallel network, as shown in the drawings and defined herein. The intelligent controller(s) shall support on-board access readers and control terminations allowing the controller and readers to be managed with local on-board operational intelligence.
         2. Field panels shall be used to support access control, alarm monitoring, video management and facility control (relay output control) functions within the defined facility or facilities as specified.
     11. The system shall use a single registration key at the server to define system configuration. The dongle shall be transferable from one server to another if a computer failure occurs. The system configuration shall facilitate an easy system retrofit or service by the user if required.
     12. The system shall support a minimum of 1 door with expansion modules to four thousand ninety-six (4,096) doors with no change to the user interface or requirement for retraining operators.
     13. The system shall support door held and door forced conditions with configurable door held times up to 2048 seconds. The system shall allow for masking of door forced and door held conditions. The system shall include the ability to configure an unlimited access grant time to be used in conjunction with extended grant time settings while using the American Disability Act mode. Extended grant time settings shall be configurable per portal or reader.
     14. The system shall include the ability to configure a door de-bounce time up to 15 seconds to avoid incidental door-forced alarms. The system shall contain the ability to assign up to eight (8) door reader modes including: disabled, unlocked, locked (no access, allow REX), correct facility code required, credential only, pin only, credential and pin, credential, or pin for use with Mercury LP1501, LP1502, or LP2500 controllers. The system shall contain the ability to assign up to four (4) door reader modes including: unlocked, credential only, credential and pin, pin only for use with VertX or Edge platforms.
     15. The system shall include the ability to configure the offline reader modes to include: no offline mode, locked down (no access, no REX), unlocked, no access allow REX, correct facility code required for use with the LP1501, LP1502, LP2500 and Azure platforms. The UNITYIS® System shall allow for correct facility required as the offline reader mode for use with VertX EVO or EDGE EVO platforms. When Intelligent Controllers are in an “off-line’ (not in communication to UNITYIS® host computer) status, Intelligent Controllers shall store (‘buffer”) System events in memory. Each Intelligent Controller shall be capable of storing a minimum of five-thousand (5000) Events in memory.
  2. **REQUIRED ACCESS CONTROL FEATURES**
     1. The system shall include the ability to configure video links allowing live video to be displayed upon access or event for an individual portal or reader. The system shall allow for customizable alarm messages to annunciate on a pre-defined alarm condition. The system shall allow for customizable alarm multimedia files on a pre-defined alarm condition. The system shall allow for configurable maximum credentials per intelligent controller and shall also allow for configurable maximum events per intelligent controller.
     2. The system shall include the ability to view and configure all drivers, intelligent controllers, sub-controllers, devices, readers from a hierarchical tree structure with a uniquely assigned addressing schema. The system shall contain the ability to view real-time status and date/time of the intelligent controller. The system shall contain the ability to view real-time status of inputs, outputs and reader modes. The system shall have a viewable loaded credential count on a per controller basis. The system shall have the ability to control hardware devices from the hierarchical tree with unique hardware addressing down to the device level. The system shall have the ability to sort the hierarchical tree alphabetically or numerically, the sort order shall follow the hardware properties throughout the software.
     3. The System shall provide the capability for an authorized operator to assign an alphanumeric description (name) to each hardware hierarchical device. Description names field shall allow for a minimum of fifty (50) alphanumeric characters. The Description names field shall be used on System menus, displays and reports.
     4. The system shall support up to 255 regionalized access levels per controller group with up to 1000 controller groups. The system shall support the ability to assign alphanumeric characters to each access level. The access level name shall allow a minimum of fifty (50) alphanumeric characters. the system shall allow for access control reader groups or individual readers to be added to access levels using a drag and drop method or selection by menu. The system shall allow for pre-defined time schedules to be associated with an individual reader or access control reader group. The system shall allow for a reader or access control reader group to be added to more than one (1) access level with a different time schedule.
     5. The system shall support access control reader groups. An access control reader group shall be an operator specified combination of one or more portals or doors associated to a time schedule. The system shall allow the assignment of portals or doors to the access control reader groups with a drag and drop function or maybe added from a menu selection. The system shall allow an operator to define access control reader groups as required without limiting system expansion.
     6. The system shall support elevator assigned floor groups. Elevator assigned floor groups shall be an operator specified combination of one or more portals or readers associated to an access level and time schedule that have been pre-defined with an elevator assignment.
     7. The system shall provide the capability for an operator to assign an alphanumeric name to each access control reader group. Access group name shall allow for a minimum of fifty (50) alphanumeric characters. The access group name shall be used on system menus, displays and reports.
     8. The System shall provide an ability to automatically adjust the System time to accommodate changes at the beginning and end of Daylight Savings Time. System shall allow the dates associated with Daylight Savings Time to be set by System Operator in advance.
     9. Database Partitioning:
        1. The system shall provide the ability to partition the database.
        2. The system shall provide the ability to establish multiple ‘logical views’ of the access control system and credential database. Each controller group shall permit viewing and/or modification of only certain credential record fields, access levels, access groups, hardware configuration, and other such data. This capability shall allow the creation of controller group, logical sub systems. The system shall allow an authorized operator to create as many controller groups as required for a site or multiple sites.
        3. Each controller group shall have full system capabilities; and shall appear to the system operator and operate as if it were an independent access control system. The typical controller group may consist of a single building or multiple building; or a single department in multiple buildings, or a single department within a building which houses multiple departments.
        4. Creation of sub-systems shall be accomplished through system configuration and software partitioning of the database.
        5. The system shall allow system operator profiles to view, create, or edit data in only certain controller groups. As an example, a system operator who is assigned an operator profile for access to controller group 1 shall only be able to view and edit database records affecting region 1. This system operator would be restricted from viewing and modifying other portions of the system database based on his or her operator profile. An operator profile shall allow the system operator to assign one or more regions for operator access.
        6. The system shall allow the ability to partition the hardware down to the device level. The system shall allow system operator profiles to view, create, or edit hardware data for only those devices designated to the operator’s profile.
        7. System operator functions which may be restricted by operator profile and controller group shall include, but shall not be limited to, the following:
           1. Adding, deleting, and modifying Credential records.
           2. Locking and Unlocking of Doors.
           3. Arming and Disarming Secure Areas
           4. Masking and Un-masking Alarms
           5. Printing Reports.
           6. Configuration of Access Levels, Time Schedules, Access Groups, and other such system parameters.
           7. Establishment of automatic door lock and unlock times.
           8. Monitoring of Alarm Conditions from user defined Doors and Monitor Points.
        8. The System shall allow the assignment of any Door, Access Group, Monitor Point, Secured Area, Auxiliary Output Contact or other System element within a Controller Group.
        9. It shall be possible to assign any Door, Access Group, Monitor Point, Secured Area, Auxiliary Output Contact or other System element to more than one Region at the same time.
        10. Operator access to specific Controller Groups shall be determined by System Operator user name and password. The use of Controller Groups shall not prevent authorized System Operators from making System-wide changes or generating System-wide reports.
            1. As an example, it shall be possible for an authorized System Operator to add/delete a credential from all sub-Systems with a single entry. The System shall not require that a separate entry be made to add/delete a credential from each Controller Group. Systems that require data add/delete entries in multiple partitions within the application shall be viewed as non-Compliant.
     10. Elevator Control:
         1. The System shall support elevator access control based on user controller group requirements and configuration. The minimum LP1501, LP1502, LP2500 configuration shall be eight (8) cars with up to thirty-two (128) floors each. The actual number of cars and floor selection outputs shall be user configurable. The System shall provide for the following elevator access control features, elevator call, and elevator floor select for individual or a group of elevator cars:
         2. Elevator call shall be an operator command or a time scheduled condition that electronically bypasses the normal use of an elevator call button at secured or unsecured floors.
         3. During a command or time scheduled event the normal elevator call button conditioning shall be replaced with an access reader-controlled output. If any credential presenting his or her credential to such a reader is authorized a sub-controller output shall activate the elevator call button to that floor.
         4. Elevator floor select shall be an operator specific configuration of credential readers and outputs designed to allow authorized credentials to enter an elevator and access only floors they have been pre-defined to access by a System operator. Elevator floor access selection replaces the normal elevator select push buttons inside the elevator car. To operate an access elevator car, a credential must present his or her access credential to a credential reader located inside the elevator car. The System shall respond to a valid access by activating outputs which temporarily enable the floor selection buttons for those floors to which the credential is authorized.
         5. The System shall allow outputs from elevator car floor selection buttons to be connected as monitor point inputs to the System to identify which floor was selected by each person using their credential. Once a floor is selected the LP1501, LP1502, LP2500 shall automatically reset allowing another authorized credential to select another floor.
         6. The elevator control feature shall provide a fully distributed functionality allowing managing access requests and activating floor selections even when an Intelligent Controllers is ‘off-line’ with the host computer. The System shall not rely on the host computer to provide elevator control functions.
     11. ADA Standard Shunt Time
         1. The System shall support an ADA (American Disabilities ACT) standard whereby a different shunt time can be set to allow users access with a longer held open / shunt time.
     12. Digital Keypad
         1. The System shall support keypad control features for access control and for intrusion detection.
         2. Access Control:
            1. In the access control applications, the System shall permit the use of digital keypads as an alternate or supplemental access control devices. Keypads shall provide no fewer than twelve numeric keys. Operation of digital keypad shall require the entry of a valid Personal Identity Number (PIN). The PIN for each user shall be definable by System Operator.
            2. PIN Keypads shall be capable of different mode assignments with access control readers. An operator may change a PIN keypad mode by command or automatically by a pre-set time of day.
            3. When in PIN Only Mode, entry of valid PIN number shall permit access. Use of an access credential shall not be required in PIN Only Mode.
            4. When in PIN Plus Credential Mode, the entry of valid PIN number, plus use of valid access credential shall be required to permit access. Use of an access credential alone or use of a PIN number alone shall not permit access when in PIN Plus Credential Mode.
            5. When in Credential Only Mode, the System will disable the PIN Keypad, allowing use of a valid access credential alone.
     13. Intrusion Detection:
         1. In the alarm access applications, the System shall permit the use of digital keypads as an arm or disarm alarm access device as well as a user keypad command station. Alarm access Keypads shall provide no fewer than sixteen numeric and static keys with a two level 16-character LCD display for local user interaction and status. Operation of digital keypad shall require the entry of a valid Personal Identity Number (PIN) or valid commands by the user. The PIN for each user shall be definable by and authorized operator.
         2. Alarm access keypads shall allow an operator to configure secured areas and allow local users to ‘Open and Close’ secured areas based on pre-configured conditions. Open early, Open late, Close early and Close late. Alarm access keypad use shall allow the user to integrate alarm and access into a single integrated reporting and response System.
         3. Alarm access keypads shall allow an operator to configure local controls to allow authorized users to active commands as well as Open/Close management. The System shall allow keypad commands to control any operator specified devices and controls by command code. Conditions such as open, close, lock, unlock, mask, un-mask, activate and de-activate shall all be assignable commands to a secured keypad area. Status and arm / disarm locations shall be displayed on the keypad LCD for pre-authorized users.
     14. Auxiliary Control
         1. The System shall provide ‘Auxiliary Output Contacts’ for auxiliary control purposes, such as the unlocking of non-credential reader-controlled doors, operation of audible alarm devices, and other such functions. Auxiliary Output Contacts shall be capable of being assigned to Door Groups; and shall be capable of being operated upon command from Operator Workstations, automatically by Time Schedule and Interval and Triggers and Macros. The System shall provide a minimum capacity of 10,000 auxiliary output contacts.
         2. Credential trigger codes in a credential record shall allow trigger and macro control for command activation and de-activation of auxiliary outputs based on access grant or deny activity. At a minimum; secure areas, macro conditions to lock and unlock locations, mask and un-mask access conditions, alarms, etc., shall be activated or de-activated based on a credential trigger code assignment.
         3. The System shall provide the capability for the System Operator to assign an alphanumeric name to each Auxiliary Output Contact. Auxiliary Output Contact name shall be a minimum of fifty (50) alphanumeric characters. The Auxiliary Output Contact name shall be used on System menus, displays and reports.
     15. Anti-Passback
         1. The UNITYIS® System shall be a System where credential readers are used for both entrance and egress and shall allow each credential reader to be operator-defined as either an ‘entry or ‘exit reader’. The System shall require credentials using a credential at an ‘entry’ reader to subsequently use the credential at an ‘exit’ reader before the credential can once again be used at an ‘entry’ reader, creating an Anti-Passback condition. Credentials attempting to use credentials without first exiting the Anti-Passback area shall be denied access and shall cause a ‘Passback Violation’ message to be sent to the central System for operator notice. If so configured, Passback Violations shall create an Alarm Condition causing an immediate report generated for operator alarm response.
         2. The System shall provide a Passback ‘forgive’ feature that can be activated by an authorized operator. The Passback forgive feature shall reset the Passback status of any credential to a neutral condition (neither ‘in’ or ‘out’ of the anti-Passback area), allowing the Passback sequence to be restarted.
         3. The System shall allow the Anti-Passback feature to be enabled and disabled upon authorized operator command,
         4. The System shall allow the APB mode to automatically be “reset” by a Time Code without the need to use an “exit” reader.
         5. A special Anti-Passback set flag shall be provided in the access control personnel record file that allows and authorized operator to specify a credential as Anti-Passback exempt. If a credential has the Anti-Passback exempt flag set, they may enter or egress any Anti-Passback area without causing an Anti-Passback event or alarm.
     16. Cardholder Records
         1. The System shall use the Credential Identification Number as the primary key to uniquely identify the record in the database. The System shall permit the use of access credential numbers as a key but shall not use access credential numbers as the primary key unless defined by an operator.
         2. The System shall provide a sort list of credential holders per Controller Group selected on the Personnel Manager screen. Sort keys shall allow the list to be sorted and displayed for an operator.
         3. The System shall permit the use of access credentials encoded in Wiegand formats of varying bit lengths from 26 bit to 75 bit.
         4. Note: Credential bit format limitations and constraints are controlled by the field hardware. It shall be the responsibility of the bidder to ensure that the field hardware proposed can meet the standards as set forth in the specification/RFQ.
         5. The System shall allow not less than two (2) different access credential numbers to be assigned to each credential record. The System shall not require that a separate credential record be created for each access credential number. The System shall allow each access credential number on the credential record to use a separate format. Systems that do not support a minimum of two credentials per credential record shall be viewed as non-Compliant.
         6. The System shall permit the creation of a Credential Record without requiring that an access credential number be assigned. This feature shall allow a Credential Record to be created for “PIN Only’ users who will be assigned a PIN number (1 to 8 digits) only and not an access credential.
         7. The System shall provide a hierarchical tree showing access level assignment for each credential in the Credential Record. This tree shall permit an authorized operator to list, and select, through ‘pop-up and drop-down windows’, any access level or access group defined in the System. To view access levels and access group shall not require an operator exit from the Credential Record screen to perform this function.
         8. The System shall allow the System Operator to identify the Access Levels, Access Groups, readers and Time Schedules associated with each credential without requiring the System Operator to exit from the Personnel Manager screen.
         9. The System shall allow for the automatic disabling of credential records based on the configured “Days of Non-Use before Deactivation” value.
         10. The System shall allow for the Personnel Manager heading tags to be modified to reflect headings based on the customer’s request.
     17. AUXILIARY CONTROL
         1. The System shall provide ‘Auxiliary Output Contacts’ for auxiliary control purposes, such as the unlocking of non-credential reader-controlled doors, operation of audible alarm devices, and other such functions. Auxiliary Output Contacts shall be capable of being assigned to Door Groups; and shall be capable of being operated upon command from Operator Workstations, automatically by Time Schedule and Interval and Triggers and Macros. The System shall provide a minimum capacity of 10,000 auxiliary output contacts.
         2. Credential trigger codes in a credential record shall allow trigger and macro control for command activation and de-activation of auxiliary outputs based on access grant or deny activity. At a minimum; secure areas, macro conditions to lock and unlock locations, mask and un-mask access conditions, alarms, etc., shall be activated or de-activated based on a credential trigger code assignment.
         3. The System shall provide the capability for the System Operator to assign an alphanumeric name to each Auxiliary Output Contact. Auxiliary Output Contact name shall be a minimum of fifty (50) alphanumeric characters. The Auxiliary Output Contact name shall be used on System menus, displays and reports.
     18. DOOR STATUS
         1. The System shall support fully supervised End-Of-Line input circuits which are software programmable by the System Operator.
         2. The System shall monitor the status of each access-controlled door to determine length of time a door is open after an authorized access grant. If the door is left open longer than a System Operator specified time period, the System shall generate a ‘Door Open / Door Held’ condition for operator notice
         3. The Door Open / Door Held timer shall be capable of being set for a System Operator-selected period of time between 1 to 4000 seconds. The Door Open / Door Held time period shall be individually selectable for each Door.
         4. The System shall provide the capability to remotely disable the Door Open / Door Held monitoring feature for each Door. Feature shall be capable of being disabled automatically by Time Schedule, Triggers and Macros and upon a command from an Operator Workstation.
     19. DOOR FORCED ALARMS
         1. The System shall monitor the status of each access-controlled Door to determine if a door is open or closed. If an access-controlled door is opened without the presentation of a valid credential the System shall generate a ‘Door Forced’ condition.
         2. Where a credential reader is provided only on the entry side of a door, the System shall allow the disabling of Door Forced monitor from the exit side of door. Disabling of Door Forced monitor shall be accomplished through the use of a request-to-exit input, defined as a ‘REX’. A REX input shall be a normally open dry contact input to System, allowing connection of release buttons, motion detectors and other devices.
         3. If the System is so configured, operation of a REX input shall disable the Door Forced monitor for a System Operator-specified period of time, allowing exit without causing a Door Forced condition. If the System is so configured, a REX input shall also be capable of unlocking the door. One (1) REX input shall be provided for each access-controlled Door per door controller.
         4. System shall provide the capability to remotely disable REX features for each Door. Each REX shall be capable of being disabled automatically by Time Schedule, Triggers and Macros and upon command from an operator workstation.
         5. Door Forced and Door Open / Door Held conditions shall be immediately processed by the System based on parameters pre-configured by the System Operator. If so configured, Door Forced and Door Open / Door Held conditions shall create an Alarm Condition; causing an immediate report to be sent to a designated Operator Workstations through the System Alarm Manager for alarm acknowledgment; and causing other System Operator-specified System operations to occur.
     20. ALARM MONITORING FEATURES
         1. The System shall provide monitoring of contact inputs from door switches, motion detectors, and other sensors located at field locations. Each input shall be defined as an individual ‘Monitor Point’. The System shall provide the capacity for a minimum of ten-thousand (10,000) Monitor Points.
         2. Monitor Point inputs shall utilize a supervised circuit requiring the use of an End-Of-Line (EOL) resistor circuit. The System shall allow an authorized operator to specify, through the System software, the EOL circuit requirements of each individual input.
         3. Monitor Point inputs shall accept both normally-open and normally-closed dry contact input signals. Monitor Point inputs shall provide a minimum of three distinct states, including ‘normal’ (input is in normal or inactive condition), ‘alarm’ (input is in alarm or active condition), and ‘trouble’ (input is in fault or tamper condition).
         4. Each Monitor Point shall be identified on System displays by a unique Monitor Point number. In addition, the System shall provide the capability for the System Operator to assign an alphanumeric name to each Monitor Point. Monitor Point name shall be a minimum of fifty (50) alphanumeric characters. The Monitor Point name shall be used on System menus, displays and reports.
         5. The System software shall provide an ‘A Virtual Door Monitoring Feature’. The virtual door monitoring feature shall permit a REX input point to be logically associated in software with a Monitor Point and Auxiliary Output to create a ‘Virtual’ access door. This feature shall allow non-credential reader doors to be monitored for both Door Forced and Door Open / Door Held conditions without requiring a credential reader or credential reader sub-controller.
         6. Monitor Points shall be capable of being grouped for the purpose of alarm management. A Secured Area shall be a System Operator-specified group of Monitor Points. The System shall provide the minimum number of System Operator-definable Secured Areas as required by the user.
         7. The System shall provide the capability for the System Operator to assign an alphanumeric name to each Secured Area. Secured Area name shall be a minimum of fifty (50) alphanumeric characters. The Secured Area name shall be used on System menus, displays and reports.
         8. The System shall provide the capability to Arm (enable) and disarm (disable) secured areas by command from Operator Workstation and by Time Schedule and Interval. Arm and Disarm commands shall be capable of being executed from pull-down menus, icons on status screen, through triggers and macros and icons on Custom Map Displays.
         9. The System Operator shall be able to enable a Monitor Point allowing the Monitor Point to cause an Alarm Condition for operator notice, if point is activated or activates after enabling. The System Operator shall be able to disable a Monitor Point allowing the monitor Point to activate without causing an Alarm Condition for operator notice. Monitor Points shall be capable of being armed and disarmed individually, and by Secured Area.
         10. The System shall have capability to automatically Arm and Disarm Monitor Points and Secured Areas by Time Schedule and Interval.
         11. Triggers and Macros shall be capable of locking and unlocking any number of access-controlled doors and door groups, change any number of credential reader modes, enable and disable any number of monitor points and activate and deactivate any number of output points based upon a monitor point status change. Triggers and macros shall be system operator configurable and shall use any monitor point status change, access condition change, keypad commands and/or credential trigger codes for conditions of change.
     21. CUSTOM MAP VIEWS
         1. The system shall allow customizable map views to display status and give control of remote devices.
         2. Mapping tools include use of color graphics and icons to represent Doors, Monitor Points, Auxiliary Output Contacts, Cameras and Keypads in context of owner supplied backgrounds.
         3. A library of complex graphic shapes including lines, circles, multi-sided polygons, complex curves, filled objects, and photos shall be available.
         4. The system shall store maps as wmf files (not bitmaps) and shall allow “dynamic resizing” of map displays. “Dynamic resizing” shall allow a map image to be created and stored as a vector-based file. Once created, the image shall be capable of being “panned” and “zoomed” without loss of detail, allowing a single image to be viewed on screen at a zoomed scale.
         5. The system shall provide for up to 10 separate layers for plotting on any map. The user shall have the ability to select the layer and plot System device assigned icons as a separate layer on a map, graphic diagram.
         6. System shall provide an unlimited number of unique Custom Map Displays.
     22. ARCHIVAL STORAGE AND BACK-UP FEATURES
         1. System shall allow backup of all System and database files, including the credential database to the local computer or external / network device concurrent with normal system operation and administration. System shall provide a menu-driven backup and restore capability, with operator prompts, enabling backups and data restoration to be made while the UNITYIS® application program is running. The System shall allow for scheduling of automated backups. configurable days and times for the backup to automatically occur.
         2. Backups shall be capable of being initiated from any Operator Workstation. Backup capability shall be available without requiring that the UNITYIS® application be closed and making backups shall not interrupt System operation or require restarting of the UNITYIS® host computer.
         3. System shall provide for archival transfer of event data from hard disk to CD. Archival transfer shall load event data to the local drive or external / network location and shall clear event data from the on-line System Journal file after verifying good archive copy. System shall provide a menu-driven utility to allow archival transfer. The System shall allow for configurable days and times for the archive process to occur automatically.
         4. The System shall permit archival storage and back-up to external storage devices via the Users network.
     23. Database Retrieval
         1. The system allows for audit trail to be shall allow for an audit trail.
         2. The System shall provide basic search tools to allow selective retrieval of events according to criteria established by System Operator. As a minimum, search tools shall allow selective recall of events by type, time frame, location, credential name, and credential number. Basic search tools shall be usable by non-technical people who have received a minimal amount of training. Basic searches shall not require knowledge of any type of programming language.
         3. In addition to basic search tools, the database retrieval System allows the use of Structured Query Language (SQL) to conduct more advanced searches. The SQL used shall be an industry-standard type that is in common use. SQL queries shall permit access to all data stored in System Journal and well as all data in System configuration database including Credential Records.
         4. The system shall allow reports to be printed, exported in industry standard data formats including .CSV, TAB, PDF.
         5. System shall provide a menu-driven utility that allows the retrieval of journal data from archival storage for the purpose of generating reports. Retrieval, reporting, and viewing of data shall not interrupt System operation or require that the current event data be cleared from hard disk.
     24. Badging
         1. The Badging System shall provide full-featured badge design and production and management.
         2. The system shall support multiple user groups such as employees or vendors.
         3. The system shall share a common language and user interface and appearance with the access control application.
         4. The system shall store photo image and other badge information for each Credential Record.
         5. The system shall permit an unlimited number of badge designs and store them as reusable badge templates.
         6. As a minimum, system editor shall:
            1. Permit badge layouts to be designed with either vertical or horizontal badge orientation.
            2. Permit insertion, sizing, and placement of photo images on badge layout.
            3. Permit insertion, sizing, and placement of text boxes within badge layout. Two types of text boxes shall be available; field text boxes which insert variable text from a selected field within the Credential Record, and label text boxes which produce fixed text.
            4. Permit use of any standard Windows True type font in point sizes between 4 and 48 points. Text shall be capable of being formatted as normal, bold, italic and bold italic.
            5. Permit use of both uppercase and lowercase text characters within a text box.
            6. Permit use of both vertical and horizontal text on badge, irrespective of badge orientation.
            7. Provide text justification within text boxes. Types of justification shall include right justification, left justification, and centered.
            8. Permit text boxes to be defined for “scale-to-fit” formatting, where text size is automatically adjusted to accommodate available space within text box.
            9. Permit use of standard Windows colors for text, text box background, badge background, photo background, signature, signature background, and borders.
            10. Permit the import, sizing and placement of graphic images (such as logos) on the badges and shall accept images in standard graphics formats such as .JPG, .BMP, .GIF, etc.
            11. Permit the assignment of aspect ratio to imported images.
         7. The Badging System shall permit the capture of signatures using any electronic signature pad which utilizes standard WINTAB device drivers.
         8. The Badging System shall permit the use of signatures on badges.
         9. The Badging System shall permit the use of any badge printer that utilizes standard Windows printer drivers. If supported by the printer the Badging System shall permit double-sided printing. If supported by printer, Badging System shall permit edge-to-edge printing on credential.
         10. The Badging System shall permit the capture of color photographic images from any of the following sources:
             1. Direct video source, such as live video camera, connected to video capture board installed in any Operator Workstation.
             2. Scanned image from any standard TWAIN-compliant scanner supported by Windows.
             3. Image file in standard .JPG format from digital camera or other source.
         11. The Badging System shall provide a “print preview” feature which allows badges to be viewed in a “what-you-see-is-what-you-get” (WYS IWYG) mode prior to being printed.
     25. Signature Pad
         1. The system allows tablet input devices to be used as a signature pad for using signatures as a badging options.
         2. A signature gathering area of at least 60 cm x 30 cm.
         3. Allows the use of any standard pen and shall not require an electronic stylus.
         4. Fully compatible with Security Management System software, including device drivers and all other hardware and software needed to use signature.
     26. Printer
         1. Heavy-duty, high-speed identification credential printer: Full-color badge printer for direct print on proximity credentials.
         2. Provide with software TWAIN compatible drivers for Windows.
         3. Provide printer with a complete set of ribbons.
         4. Provide with manufacturer’s recommended cleaning kit.
         5. Provide printer with table-top slot punch to allow punching of proximity credentials in horizontal or vertical direction. Punch to be factory calibrated for vertical punching.
     27. Video Management Add to System Function
         1. The System shall provide a software level integration to the Video Management Systems. The video management system of choice shall be a Milestone System or pre-approved equal.
         2. Live Video Call-Up from the Hardware Device Tree for any IP based camera.
         3. Plot cameras onto graphic maps to call up Live Video for any IP based camera.
         4. Selection of specific cameras upon receipt of command from Security Management System.
         5. Activation and positioning of PTZ camera “presets” upon receipt of command from Security Management System.
         6. Automatic activation of video recording System upon receipt of command from Security Management System.
  3. **ACCESS CONTROL USER INTERFACE** 
     1. The UNITYIS® shall allow non-technical personnel to operate and administer the system.
        1. The system shall allow authorized users to define and modify operating parameters, such as credential records, doors, time codes, monitor points, and alarm conditions.
     2. “Client Software” shall allow “industry-standard” computers running a web browser to serve as client workstations for the access control system.
        1. The “Web Client” shall be browser agnostic and allow any web-enabled hardware device including mobile phones and tablets to serve as the interface for the UNITYIS®.
        2. Client workstations shall be connected to the UNITYIS® host computer using TCP/IP Ethernet protocol and fully function within the end-user’s Ethernet network.
     3. The use of a personal computer as an client workstations shall not prevent other application software such as word processors, spreadsheets, and electronic mail programs from being used on the same computer.
     4. The system shall be multi-user, multi-tasking, allowing the simultaneous use of multiple Operator Workstations. The system shall allow any number of client workstations to be in use at the same time.
     5. If configured, system events shall display at designated Operator Workstations and or print.
     6. The system shall be capable of selectively displaying all System configuration data at an Operator Workstation screen, allowing the viewing of Credential Records, Clearance Codes, Doors, Time Intervals, Time Codes, Monitor Points, Door Groups, Secured Areas, and other configuration data. System shall provide ability for System Operator to selectively view specific types and numerical ranges of data all based on their user assigned operator profile.
     7. User Interface – Profiles and Permissions
        1. Access to any UNITYIS® Web Client shall require an Operator username and password. The System shall default allowing 50 unique operator profiles. The number of operator profiles shall be user-defined. Operator profiles shall be shown in a drop-down window display box.
        2. The process of adding an operator profile may be restricted and can be configured to require an operator password and/or an access credential or token.
           1. Operator passwords shall be stored in encrypted form and shall be hidden for those authorized to administrate the system.
        3. Strong passwords shall be allowed and include uppercase and lowercase letters as well as numerals within passwords.
        4. The system shall support single sign on authentication from Microsoft, Apple, Google, Facebook, LinkedIn or Amazon.
        5. The system shall also support UNITYIS® System Authentication or Windows Authentication with the ability to support user accounts in Active Directory/LDAP shall be configurable.
        6. Each operator profile is configurable to allow or deny various groupings of commands and system functions.
           1. Administrators may assign or deny access by an operator to any System Controller Group.
           2. Administrators shall be able to conceal such items as System messaging, personnel records, access levels and hardware utilizing System Controller Groups.
           3. Administrators shall be able to configure each user profile to view, add, change, delete or add commands to application modules.
           4. Operator profiles shall allow access to application modules, user access levels, time schedules, secured areas, point status monitoring and commands, event management, alarm management, conditional commands (triggers and macros), custom commands, video management, graphics, system settings, system utilities and personnel information including the ability to assign field level permissions of no access, read/write, read only, and mask field.
        7. All System functions shall be available at any client workstation with the appropriate permissions.
     8. User Interface - Graphical Features
        1. System software shall use menu-driven commands and provide interactive prompts. Program and error messages shall provide clear and understandable sequencing of events. The user interface and menu structures shall be consistent throughout the System. The System shall have multi-language support for error messages and menu items.
        2. The system shall provide a standard Windows-style graphical user interface using a Web browser that makes extensive use of graphical elements such as toolbars, icons, and pull-down list boxes. System commands and functions shall be available by using a mouse or pointing device. The system shall comply with established Microsoft Windows including the ability to drag and drop items, such as access levels and graphical maps.
        3. All System functions shall be available through the graphical user interface and without requiring text-based system commands or a command shell.
        4. Up to 50 customized command buttons shall be available and able to be partitioned by user profile and permissions.
     9. Alarm Monitoring
        1. Activation of Monitor Point shall be immediately processed by the System in accordance with parameters as established by the System Operator.
        2. If so configured, the activation of a Monitor Point shall create an Alarm Condition causing an immediate report to be sent to the Alarm Manager on the Operator Workstations.
        3. Any event/alarm shall be configurable in the Triggers and Macro module to cause other System specified operations to occur.
        4. The maximum time period from activation of Monitor Point until Alarm Condition is displayed on the Operator Workstation shall not exceed five (5) seconds.
        5. The system shall be capable of displaying customizable Operator Instruction Displays. Operator Instruction Displays shall be System Operator-created text messages per alarm point or based on a typical response message from file. System shall provide a message file for every alarm setup by the System administrator or authorized operator.
        6. Upon Alarm Condition, the System shall sound an audible warning configurable by the System Operator, display an alarm message on a graph map by the point that activated into an alarm condition on all operators logged on to the System with an alarm monitoring profile. Systems requiring Operator-designated Operator workstations only shall be viewed as non-Compliant.
        7. If so configured any Alarm Condition shall automatically display a specified Custom Map display at any logged on authorized operator workstation. The symbol (icon) representing the Door Monitor Point, or other device causing the Alarm Condition shall change color or flash to identify point of alarm origination on the map display.
        8. If so configured and Alarm Condition shall automatically display a specified Custom Operator Instruction with the specific Custom Map display.
        9. The System shall provide real-time tracking of the actual status of each Armed Monitor Point, providing an indication of when Monitor Point is activated, and of when Monitor Point is cleared. A user selected Point Status Window shall be selectable by an operator to display the real-time status of all points, outputs and readers based on their regional operator profile.
        10. Alarm Conditions shall require Operator acknowledgment. Administrator Operators shall have the ability to acknowledge all alarms simultaneously. In addition, the System shall allow Alarm Conditions to be configured as “log only” events.
        11. The System shall provide a visual indication of all unacknowledged Alarm Conditions in the “Alarm Manager” window on any authorized operator workstation.
        12. The system shall provide an Alarm Manager to display the status of all active and user assigned alarm points for any logged-on and authorized operator at any client on the network.
        13. The system shall provide ability to automatically play audio messages on designated Operator Workstations upon Alarm Condition. The system shall allow attachment of separate audio and media files to each Alarm Condition. Audio files shall be standard .WAV format audio files, media files are MS standard.
     10. Alarm Outputs
         1. All Alarm Conditions, including Door Forced conditions and Door-Held-Open conditions, shall be capable of activating one or more Auxiliary Contact Outputs to enable operation of audible sounders, door alarm horns, and other such devices.
         2. The system shall permit the global relationship of Alarm Conditions to Auxiliary Output Contacts, where conditions occurring at one Intelligent Controller shall be capable of causing outputs to occur at any Intelligent Controller in the System.
         3. The System shall allow System Operator to define how each output is to operate during each Alarm Condition. As a minimum, the System shall permit the following operating conditions all configured in a separate software module, Triggers and Macros. Systems that do not support fully configurable Triggers and Macros based on any System event/alarm shall be viewed as non-Compliant.
         4. Output tracks Alarm Condition / Event / Activity: Output activates when Alarm Condition is active and deactivates when Alarm Condition clears.
         5. Output tracks acknowledgment: Output activates when Alarm Condition is active and deactivates when Alarm Condition is acknowledged by System Operator, even if Alarm Condition has not yet cleared.
         6. Timed output: Output activates when Alarm Condition is active, and deactivates when Alarm Condition has cleared, or after a preset time, whichever occurs first. Time shall be definable by System Operator for periods of between 1 and 300 seconds.
         7. Access Events: Output activates or de-activates based on any access event/status change with time of day and other event conditioning.
         8. Credential Event: Output activates or de-activates base on a credential trigger code and access event (granted or denied).
     11. Alarm Communications
         1. E-Mail Or Text Messaging Upon Alarm Condition
         2. System shall provide ability to send E-mail messages to designated recipients upon Alarm Conditions or operator selection. System shall utilize standard SMTP E-mail protocols to permit transmission to any valid Internet E-mail address. This capability shall allow transmission of alarm messages to any device capable of receiving E-mail messages (pager, cell phone with text messaging, etc.).
         3. E-mail messages shall be capable of being sent to E-mail Address Groups based on Time Code.
         4. System events shall be immediately sent to the UNITYIS® host computer and stored on hard disk when intelligent controller status is on-line,
     12. Reporting
         1. The system shall provide:
         2. Trace feature that can be set individually for each credential. The trace feature shall allow real-time tracking of system operator-specified credentials. Use of a credential that has been set for trace shall be automatically logged, and if so configured, initiates an event displayed at an operator workstation. Trace reports are in addition to any regular report as the result of credential activities such as valid access or invalid access attempt.
         3. An automatic credential activity and reader access report.
         4. An electronic log of events, with date and time, recorded on a real-time basis as they occur.
         5. An audit trail of recorded events.
         6. The System shall allow events to be selectively reported to Operator Workstations and Printers. As a minimum, the System shall allow the selective reporting of the following events: Alarm Condition, Monitor Point activity, Forced Door, Door-Held, Invalid Access Attempt, Passback Violation, Trace, Hardware Failure, Communication Failure, Tamper, Power Fail, etc.
         7. A current system status report upon command from Operator Workstation. Status reports will indicate: current status of Doors, Monitor Points, and Alarm Conditions; current status of System Operator imposed commands such as Disarm, Unlock, and Disable; current status of timed System operations, such as timed Unlock, and timed Disarm; and current status of equipment, communications, and power failure conditions.
         8. Logging for Valid Access, Invalid Access Attempt, and Trace conditions, the System shall be capable of logging the following information as a minimum: Door name and number; credential number; and credential name (If truncated, shall be 12 characters minimum). For Invalid Access Attempts, the System shall display and log reason for rejection.
         9. Logging for Monitor Point and Alarm Condition activity.
         10. Logging for Operator Workstation Commands including Unlock, Re-lock, Arm, Disarm, Disable, Silence, Acknowledge, Reset, and other such System Operator commands. Log of Operator commands shall identify the System Operator who issued each command. The System shall log unauthorized attempts to gain access to the System, such as the use of an invalid password, including the terminal node and/or network address from which the attempt was made.
         11. Logging of all automatic System operations that occur by Time Code, including Unlock, Re-lock, Arm, Disarm, and other such timed operations.
         12. Logging of Hardware Failure, Communications Failure, Power Fail, and other such System conditions.
         13. Logging of system Operator configuration activity, such as modification to Clearance Codes, Time Codes, Monitor Points, Credential Records, and other System data, shall be recorded to an operator audit log. As a minimum, the operator audit log shall identify the type of data that was modified, old data, new data and identify the System Operator who modified it. The System shall allow the Audit report to be filtered by date and by System Operator.
         14. The System shall support standard network printing facilities to allow the use of any printer connected to the user’s local computer or network. The use of specific printers for specific types of reports shall not be required.
         15. The system shall be capable of printing all System configuration data to printer, allowing print-out of Credential Records, Clearance Codes, Doors, Time Intervals, Time Codes, Monitor Points, Door Groups, Secured Areas, and other configuration data. System shall provide ability for System Operator to selectively print specific types and numerical ranges of data all based on an operators assigned operator profile.
     13. Help
         1. The system shall provide online, context searchable help instructions and manuals available 24 hours a day seven days a week.
         2. The system shall provide online help should allow for language translation and the ability to be printed or e-mailed directly from the online help system all other systems without this functionality will be considered non-Compliant.
  4. **COMPATIBLE PRODUCTS**

Provide only products compatible with UNITYIS®.

* + 1. Field Devices
       1. CARD / BIOMETRIC READERS AND KEYPADS
          1. Provide credential reader types as indicated as needed.
          2. Standard 125kHz/13.56 MHz proximity readers at interior locations with a Wiegand interface.
          3. Standard 125kHz/13.56 MHz proximity readers at exterior locations with a Wiegand interface.
          4. Credential readers shall be standard, unmodified product. Readers which have been specially modified for use with a specific UNITYIS® manufacturers System shall not be used.
          5. Provide credential readers with all necessary accessories, including mounting brackets, connectors, cables, installation tools, and other such components necessary for a complete installation.
          6. If required, Biometric readers shall include a proximity credential reader incorporated into the same reader housing that shall be weather resistant.
       2. MAGNETIC CONTACT SWITCHES
          1. Contact switches on overhead doors, roof hatches, gates, and the like shall be Heavy-Duty Surface Mounted contacts or Heavy-Duty Floor Mounted contacts.
          2. Heavy-Duty Surface Mounted: Wide-gap surface mount magnetic contact switch, heavy-duty all-metal construction with stainless steel armored cable, 3/4” to 2 1/2” gap. Single-pole- double-throw (SPDT) hermetically sealed switch contacts with biasing magnet. U.L. Listed.
          3. Heavy-Duty Floor Mounted: Wide-gap floor mount magnetic contact switch, heavy-duty all- metal construction with stainless steel armored cable, 3/4” to 2 1/2” gap. Single-pole-double- throw (SPDT) hermetically sealed switch contacts with biasing magnet. U.L. Listed.
          4. Provide all hardware, mounting brackets, adapters and plates required for magnetic contact switch installation. All contact switches, magnets, and brackets shall be mounted using tamper-resistant fasteners.
       3. TAMPER SWITCHES
          1. Provide tamper switches at every control panel, power supply, and equipment enclosure and at all junction boxes containing splices or connections. Tamper switches shall cause activation of alarm point when door on panel or enclosure is opened.
          2. Tamper switches shall be recessed plunger switches with closed-loop contacts. Provide with mounting brackets as required to mount to sides of panels and within junction boxes. Tamper switch type to be selected as required to suit conditions.
       4. REQUEST-TO-EXIT MOTION DETECTORS – Stand Alone
          1. Request-To-Exit (REX) motion detector: Passive infrared (PIR) detection technology with normally open contact output, integral walk-test indicator. 12 VDC operation. Detector shall be specifically designed for use as REX detector.
          2. REX detector shall contain a built-in electronic sounder.
          3. REX detector coverage pattern shall provide positive REX detection of person at exit side of door but shall be adjustable to avoid unwanted detection in other areas.
          4. Provide trim plate to enable mounting of REX detector to single-gang electrical box (mounted horizontally). Trim plate shall completely cover rough-in opening. Trim plate color and finish to match REX detector.
       5. PROXIMITY CARDS
          1. Proximity credentials shall be ‘credit credential’ sized (3 318” x 2 1/8). Thickness of proximity access credentials shall not be greater than .033’.
          2. Proximity credentials shall be “direct print” credentials capable of directly receiving a printed image using the specified badge printer. Proximity credentials shall have white photo image surface on both sides, allowing both sides to receive a printed image.
          3. Proximity access credentials shall be white/white, with a dye-sub photo compatible surface on both sides. Credentials shall not be slot punched but shall be capable of accepting a horizontal or vertical slot punch.
          4. Credentials shall be in standard Wiegand 37-bit open format. Credentials shall not be provided in either the contractor’s or Security Management System manufacturer’s proprietary format.
          5. Proximity credentials shall carry a minimum of a two-year warranty against defects in material and workmanship.
       6. AUXILIARY BUTTONS
          1. Manual Release:

Manual release button in surface mounted enclosure. Suitable for mounting to desk or counter. Momentary operation. DPST contacts rated at 3 amperes.

Manual release button on single-gang plate. Suitable for mounting to wall. Momentary operation. All steel momentary push button with SPDT contacts rated at 3 amperes.

* + - * 1. Duress Alarm Button:

Manual panic button, latching type, SPDT contact switch. Indicator light indicates when button has been tripped. Pull-type actuator designed to resist accidental activation. ABS fire-retardant plastic construction.

* + - 1. AUDIBLE SOUNDERS
         1. Electronic sounder mounted to single-gang stainless steel plate. 12 VDC operation. Shall provide audible output of not less than 85db at 12 VDC.
      2. AUXILIARY RELAYS
         1. Relays shall be heavy-duty industrial grade approved. 24 VDC coil, contacts rated at no less than 5 amperes at 28 VDC.
      3. Cabling
         1. Open Supervised Device Protocol (OSDP)

PVC

RS-485, 2 Pair 22AWG (7x30) Tinned Copper, PE Insulation, Tinned Foil Copper Braid Shield, PVC Outer Jacket, UL Listed, and oil resistant, Non-Plenum.

Rated for installed environment.

Model #: Belden 3107A, or Equal.

* + - * 1. Plenum

RS-485, 2 Pair 24AWG (7x32) Tinned Copper, FEP Insulation, Overall Tinned Foil Copper Braid Shield, PVC Outer Jacket, CMP.

Rated for installed environment.

Model #: Belden 82842, or Equal.

* + - * 1. Wiegand

18/6 AWG stranded, shielded, Plenum.

Rated for installed environment.

Model #: Belden 6304FE, or Equal.

* + - * 1. Multi Function, Single Outer Jacket Cabling

Plenum-CMP, 3-22 AWG pairs, 4-18 AWG conductors, 4-22 AWG conductors, 2-22 AWG conductors, All conductors stranded bare copper with insulation, shielded.

Rated for installed environment.

Model #: Belden 658AFJ, or Equal.

* + - * 1. Electrified Locking Hardware

For low inrush hardware (Approx 2amps) up to 450' from power supply

18/2 AWG stranded, unshielded, Plenum.

Rated for installed environment.

Model #: Belden 1863A, or Equal.

For higher inrush hardware

14/2 AWG stranded, unshielded, Plenum.

Model #: Belden 1861A, or Equal.

Request to Exit (REX), Door Position Sensor (DPS), Peripheral Door Device, Input/Output Contact Closure or Output to Electrified Locking Hardware or Gate Operator.

22-4 AWG stranded, unshielded, Plenum.

Rated for installed environment.

Model #: Belden 6502UE, or Equal.

Intrusion Alarm Cabling

Motion Detector, Glass Break, DPS, or Input/Output Contact Closure.

Rated for installed environment.

Model #: Belden 6502UE, or Equal.

Keypad or device requiring shielded cabling or RS422/RS485.

RS-485, 2 Pair 24AWG (7x32) Tinned Copper, FEP Insulation, Overall Tinned Foil Copper Braid Shield, PVC Outer Jacket, Plenum.

Rated for installed environment.

Model #: Belden 82842, or Equal.

1. PART III EXECUTION
   1. **Examination**
      1. Verify site conditions match project assumptions.
      2. Verify:
         1. Scope of work required by others.
         2. Measurements.
         3. Pathway
         4. Electrical
         5. Data and Cabling
   2. Report changes or site conditions effecting scope of work.
   3. Prior to installing contact switches on doors, carefully examine each door to determine if doors are in satisfactory condition to accept.
   4. **Installation**
   5. Install cabling in accordance with NFPA 70, National Electrical Code.
   6. Wiring method:
      * 1. Install cabling in conduit pathway for any public areas, where required for rough in, where required by Authorities Having Jurisdiction or AHJs, where subject to damage or environment.

~OR~ (use the option immediately above or immediately below)

* + - 1. Install cables within conduit from field device to head end.

~OR~ (use the option immediately above or immediately below)

* + - 1. Use cabling listed for its intended wet rated, riser and plenum locations, including within underground raceway.
      2. Conceal cabling unless surface mounting explicitly called for by design team or owner or within back of house, equipment spaces or where infrastructure and conduit is exposed.
      3. Include additional 10’service loop for cables.
      4. Maintain manufacturer required distance limitations for cable lengths.
      5. Provide tamper resistant security screws for devices junction boxes and enclosures.
  1. Intelligent Controllers
     + 1. May require the following:

Enclosures, environmentally rated enclosures, chases, raceway and surface mount raceway to properly interconnect controller hardware and accessories.

Wiring harnesses, connectors, and cabling.

U.L. listed 12vdc and 24vdc Power supply per manufacturer requirements.

Input and Output boards, connectivity, tamper, din rails, fuses and auxiliary relays, locks and other best practice accessories.

Relays shall be heavy-duty industrial grade approved. 24 VDC coil, contacts rated at no less than 5 amperes at 28 VDC.

* + - 1. Minimum Power Requirements
         1. 12 VDC Three Ampere Auxiliary Power Supply

12 VDC power supply, three 2.5 ampere minimum capacity, with integral battery charger, to be used to power REX detectors, audible sounders, door alarm horns, and other such auxiliary devices. U.L. listed. Power-limited with built-in over current protection.

Power supply shall provide dry-contact power fault output.

Voltage regulation, ripple current, and other such tolerances shall be in accordance with equipment manufacturer’s guidelines.

Provide each 12 VDC power supply with one (1) 12 VDC 7 ampere hour gelled electrolyte, sealed lead acid battery.

* + - * 1. 24 VDC Three Ampere Lock Power Supply

Lock Power Supply: 24 VDC power supply to be used exclusively to power electric lock hardware. 5 amperes minimum continuously usable output. U.L. listed. Power-limited with built-in over current protection.

When primary power is present, power supply shall continuously maintain a charge on standby batteries. Power supply shall be capable of recharging batteries while providing full lock output.

Provide each 24 VDC power supply with two (2) 12 VDC 7 ampere hour gelled electrolyte, sealed lead acid batteries.

Provide battery wiring harness as needed to properly connect batteries to power supply.

Provide with relay to supply dry-contact power fault output.

* + - * 1. Install each panel in equipment closet locations as indicated. Install each panel at a location and height to facilitate ease of service.
        2. Identify the software and hardware address of each panel with a permanent marking label installed on the exterior of the cabinet.
        3. Neatly dress and tie all wiring within panel. Do not obstruct access to terminal strips and configuration jumpers with wiring.
        4. Provide terminating resistor on all unused input connections.
        5. Label all inputs and outputs with a permanent marking label.
        6. Ground all shielded cables in accordance with manufacturer’s instructions. Trim and wrap all unused shield wires to prevent shorting or inadvertent grounding.
  1. Power Supplies
     + 1. Install all System power supplies at Intelligent Controller panel backboard locations as indicated.
       2. Unless otherwise noted, all System accessories, such as REX motion detectors, door alarm horns, sounders and the like shall be powered from 12 VDC auxiliary power supply located at equipment backboard.
       3. Unless otherwise noted, power all electric lock hardware from 24 VDC lock power supply located at equipment backboard. Do not power lock hardware from other power supplies.
       4. Connect power supply fault output to input point on Intelligent Controller. Provide pilot relay where needed to provide dry-contact output from power supply.
  2. Card Reader Installation
     + 1. Where possible, all credential readers mounted outdoors shall be installed out of direct exposure to sunlight, rain, and snow.
       2. Unless otherwise noted, credential readers are to be mounted at a height of 40” above the finished floor (measured from floor to centerline of credential reader.) to be ADA compliant.
       3. Securely mount all credential readers using tamper-resistant fasteners.
       4. Credential readers shall completely cover any electrical back box or other electrical rough-in. Provide trim plates, adapters and back boxes at locations where required.
       5. Credential readers shall be installed so that they are “low-profile” and protrude from the wall only a minimum distance.
       6. Completely seal all exterior openings of outdoor mounted credential readers to make weather tight.
       7. Make credential reader field adjustments in accordance with manufacturer’s instructions.
  3. Electrified Locking Hardware
     + 1. Provide wiring and final connection to electric strikes, electric locks, transfer hinges, electric exit devices, detention hardware, and other such devices.
       2. Provide diode for transient suppression across coils of electric locks, electric strikes, and relay coils.
       3. Verify operating voltage and current requirements of all lock hardware with hardware supplier. Coordinate cable requirements and connection points. Thoroughly test the operation of all electric lock hardware for proper operation.
       4. Install pilot relay to control lock hardware where current requirements of hardware exceed relay contact rating of Intelligent Controller or where electrical isolation is required.
  4. Door Contacts
     + 1. Install contacts using tamper-resistant fasteners. Contact and magnet to be at door head. Contact shall be placed three inches (3”) from latch side of door unless otherwise specified.
       2. Contact and magnet shall not interfere with door hardware, weather-stripping, or door operation.
       3. Flush-mounted contact switch to be installed flush with door jamb. Magnet to be flush with top of the door. Provide spacers as required. Do not over-drill mount holes. Contact and magnet shall fit snug within mounting hole. Use silicon rubber adhesive/sealer as required.
       4. Install end-of-line resistors at each contact switch. End-of-line resistors shall be connected to flexible wire leads and protected with heat-shrink tubing or equivalent.
       5. Test all contact switches for proper operation.
  5. Cable
     + 1. Install cabling in conduits, cable trays, and cable rings provided under the work of other Sections.
       2. Coordinate cable installation in shared cable trays, cable rings, equipment rooms, and racks with the installers of other Systems such as telecom, data, security, building management, etc.
       3. Provide additional cable support as needed to fasten cable above ceiling in locations where cable tray/cable rings are not provided by others.
       4. All cable shall be run straight and level in relation to floor and ceiling and parallel and perpendicular to walls. All changes in direction shall be made in a gradual radius so that cable is not pinched or strained.
       5. Cable installed above suspended ceilings shall not lie on or touch ceiling tiles. Cable shall not interfere with the removal of ceiling tiles.
  6. Field Devices
     + 1. Connect credential readers, inputs, and outputs to Intelligent Controllers as indicated on the enclosure or otherwise indicated.
       2. Credential reader, door switch, request-to-exit, and lock output wiring shall be “home-run” and connected to Sub-Controller as indicated on the enclosure or otherwise indicated.
       3. Use standard and consistent wire conductor color-coding for device wiring. Use the same colors for each function throughout the project, for example: Red and Black colored wires always used for power, Green and Yellow colored wires always used for detection circuit, etc.
       4. Install end-of-line resistors at detection device. End-of-line resistors shall be connected to flexible wire leads and be protected with heat-shrink tubing or equivalent. Direct crimp or wire nut connections to resistor are not permitted.
       5. Mount devices on single gang or manufacturer’s recommended back box.
       6. Mount wall mount panic devices with stainless steel unless specified.
  7. Request To Exit Device (REX)
     + 1. Install detector to provide positive detection of person approaching door to exit. Direct detector to minimize unwanted detections in halls, corridors, rooms and the like. Carefully adjust to provide trouble-free REX operation.
       2. Unless otherwise specified, REX detectors shall be installed on the door frame or on the wall above the door within 12” of the top of door frame. Do not install REX detectors on ceilings or on side walls unless construction conditions prevent installation above the door.
       3. For single doors, REX detector shall be centered above door. For pairs of doors, REX detector shall be centered between doors.
       4. Detector shall be mounted in coordination with other building elements and to maintain building lines. Avoid interference with other electrical and mechanical Systems. Where conflict exists between proper detector operation and other elements, notify Security Consultant and Owner.
       5. Connect audible sounder in REX detector to 12 VDC auxiliary power via auxiliary output contacts as indicated in panel schedules. Program UNITYIS® to activate sounders upon door-forced open and door held open conditions.
       6. Ninety (90) days after final Acceptance, re-test all REX detectors. Test to assure proper operation. Re-adjust and relocate detectors as required.
  8. Fire Alarm
     + 1. Fire alarm output module will provide a single Form C dry-contact output rated at one ampere. Contractor to provide pilot relays as needed to provide additional contacts or greater current capacity.
  9. Elevator Interface Panel
     + 1. Coordinate installation of credential access System for elevator with elevator installer.
       2. Coordinate requirements for conductors in elevator traveling cables with elevator installer. Verify that conductor quantities and types are suitable for use with credential reader.
       3. Provide credential readers to elevator installer for installation in elevator. Make final connections to credential reader.
       4. Provide relay interface circuit between Security Management System and elevators as indicated on drawings. Route cabling in the elevator machine room to locations designated by elevator installer.
       5. With cooperation and assistance of elevator installer, fully test all elevator control functions. Provide assistance to elevator installer as required to troubleshoot any elevator control related problems.
  10. Programming and Configuration
      + 1. Contractor shall provide initial programming and configuration of the software to make the Security Management System fully operational.
        2. Initial programming of the software shall include but shall not be limited to: creating operators and permissions; establishing alarm reporting and alarm routing; creating doors and device groups, input and outputs and input and output groups; establishing clearance codes; establishing schedules and operating modes, configuring interfaces to external Systems, and installing and configuring operator workstation software.
        3. Input of all program data shall be by Contractor. Contractor shall consult with Owners Representative and Security Consultant to determine descriptor names and System operating parameters.
        4. Owner, with the cooperation and assistance of Contractor, wilt input the credential data for each access credential.
        5. Contractor shall maintain hard copy worksheets which fully document the System program and configuration. Worksheets shall be kept up to date daily by Contractor until final Acceptance by Owner. Worksheets shall be subject to inspection and approval by Owner. Provide final copies to Owner prior to Project Close-out.
        6. Contractor shall maintain a complete, up-to-date backup of the System configuration and credential database. Backup shall be maintained throughout programming period until final Acceptance by Owner.
        7. Change any default passwords and provide a list to owner’s security organization.
  11. Maps
      + 1. Contractor shall be responsible for creating initial set of graphic floor plan maps for the Security Management System.
        2. Owner shall provide floor plan and site plan drawings in the form of Auto-cad .DWG files for use in the creation of maps. Contractor shall be responsible for converting these files to a format usable by the UNITYIS® graphics software, and the editing of the maps to remove or add graphic information as needed to produce an accurate map.
        3. Once usable graphic maps have been created, Contractor shall be responsible for adding icons representing each UNITYIS® device to the maps and linking these icons to System events as needed to create an interactive System display.
        4. Maps shall be created at a scale to allow icons for UNITYIS® devices to be placed accurately on the floor plan. Where many UNITYIS® devices are concentrated in a specific floor plan area, provide a larger scale map to avoid the “bunching” or overlapping of icons on the map.
        5. Contractor shall consult with Owner’s Representative and Security Consultant to determine map creation parameters prior to start of map creation. Contractor shall periodically review completed maps with the Owner’s Representative as the work progresses to assure that Owner’s expectations are being met.
  12. Functional Testing
      + 1. Conduct functional testing and document the following:
      1. Access Granted Valid
      2. Access Granted No Entry
      3. Unlock Time
      4. Relock On Time
      5. Held Open Alarm and Time
      6. Forced Open Alarm
      7. Valid REX
      8. Door Position Closed
      9. Power Fail
      10. Network Drop
      11. Network Restoration
  13. Closeout Drawings
      + 1. Shop Drawings
        2. Record Copy Drawings
        3. As Built Drawings
  14. Training
      + 1. Training agenda to include:
           1. Overview of the System hardware and software components.
           2. Procedures for creating a Security Management System database.
           3. Establishing operator permission groups, user logins and passwords.
           4. Configuring intelligent controllers, printers, operator workstations, credential readers and input/output points.
           5. Establishing access control System configuration: defining doors, door groups, time intervals, time codes and clearance codes.
           6. Creating credential records.
           7. Importing graphic drawing files and plotting points.
           8. Defining alarms and Device Groups / Areas.
           9. Defining actions to occur upon alarm condition, including operator instructions, sound effects, and E-mail messaging.
           10. Establishing alarm routing.
           11. Establishing database partitions; creating logical sub-Systems, assigning System elements to sub-Systems, and assigning operators to sub-Systems.
           12. Creating activity reports.
           13. Inputting credential record data and issuing access credentials.
           14. Viewing current System status.
           15. Database backup and restore; System archive and restore.
           16. Handling common System errors and exceptions.
  15. Maintenance
      + 1. Conduct site visit at least once every three months during the first year to perform inspection, testing, and preventive maintenance. Submit report to Owner indicating maintenance performed along with evaluations and recommendations.
        2. Provide trouble call-back service upon notification by Owner:
        3. Include allowance for call-back service during normal working hours at no extra cost to Owner.
  16. Painting
      + 1. Touch up marred and bared surfaces of primed, galvanized, and finish painted equipment, materials, and accessories installed.
        2. Restore patched surfaces as close to the original condition and finish as reasonably possible.  Where patching occurs in smooth painted surface, extend final paint coat over entire unbroken surface containing patch, after patched area has received two coats of primer and two coats of finished paint.