SECTION 13710

WIN-PAK INTEGRATED SECURITY SOFTWARE AND MAXPRO ACCESS

Display hidden notes to specifier. (Don't know how? [Click Here](https://www.arcat.com/sd/display_hidden_notes.shtml))

*Copyright 2014 - 2023 ARCAT, Inc. - All rights reserved*

\*\* NOTE TO SPECIFIER \*\* Honeywell Commercial Security; security and automation solutions, access control.  
This section is based on the products of Honeywell Commercial Security, which is located at:  
715 Peachtree St. N.E.  
Atlanta, GA 30308  
Toll Free Tel: 800-323-4576  
Email: [request info (Shellie.Redden@Honeywell.com)](https://admin.arcat.com/users.pl?action=UserEmail&company=Honeywell+Commercial+Security&coid=48331&rep=&fax=&message=RE:%20Spec%20Question%20(13710hsg):%20%20&mf=)  
Web: <https://buildings.honeywell.com/us/en/brands/our-brands/security>   
 [ [Click Here](https://www.arcat.com/arcatcos/cos48/arc48331.html) ] for additional information.  
A History of Innovation  
For over 30 years, Honeywell has delivered integrated solutions that business leaders resolve security  
challenges by providing critical information that informs effective and efficient decision making. When  
protection is critical, so is the choice of your security system. As industry pioneers, Honeywell has  
developed many of the groundbreaking advances that have shaped today&#39;s commercial security  
systems. We made systems easier to install and use, following best practices and standards in  
developing secure and compliant cyber-resilient products.  
Research and Development  
For over 75 years as an industry leader, we have prioritized safety. Our commitment to quality and  
innovation produces connected and comprehensive systems built by teams that are invested in effective  
results.  
Commitment to Quality  
Our products are built in world-class production facilities and are subject to rigorous testing exceeding  
industry standards for quality and performance. Honeywell equipment complies with all ISO-9001  
protocols, an internationally recognized standard that defines a quality assurance system. We have  
more than 30 years of domain expertise, unmatched technical capabilities, a sterling global reputation  
and the financial stability to provide the support your customers expect and deserve, for decades to  
come.

1. GENERAL
   1. SECTION INCLUDES

\*\* NOTE TO SPECIFIER \*\* Delete items below not required for project.

* + 1. Integrated security software. (WIN-PAK)
    2. Web based modular access control system. (MAXPRO Access MPA 2 & 4 door systems)
    3. Access control readers.
    4. Access control credentials.
    5. Access control cables.
  1. RELATED SECTIONS

\*\* NOTE TO SPECIFIER \*\* Delete any sections below not relevant to this project; add others as required.

* + 1. Section 26 05 00 - Common Work Results for Electrical.
    2. Section 27 11 23 - Communications Cable Management and Ladder Rack.
  1. REFERENCES

\*\* NOTE TO SPECIFIER \*\* Delete references from the list below that are not actually required by the text of the edited section.

* + 1. Electronic Industries Alliance (EIA):
       1. RS232C - Interface between Data Terminal Equipment and Data Communications Equipment Employing Serial Binary Data Interchange.
       2. RS485 - Electrical Characteristics of Generators and Receivers for use in Balanced Digital Multi-Point Systems.
    2. Federal Communications Commission (FCC):
       1. FCC Part 15 - Radio Frequency Device.
       2. FCC Part 68 - Connection of Terminal Equipment to the Telephone Network.
    3. Federal Information Processing Standards (FIPS):
       1. Advanced Encryption Standard (AES) (FIPS 197).
       2. FIPS 201: Personal Identity Verification (PIV) of Federal Employees and Contractors.
    4. National Fire Protection Association (NFPA):
       1. NFPA70 - National Electrical Code.
    5. Homeland Security Presidential Directive 12 (HSPD-12).
    6. Underwriters Laboratories (UL):
       1. UL294 - Access Control System Units.
       2. UL1076 - Proprietary Burglar Alarm Units and Systems.
  1. DEFINITIONS
     1. ISMS: Information Security Management System od just Security Management System.
  2. SUBMITTALS
     1. Submit under provisions of Section 01 30 00 - Administrative Requirements.
     2. Product Data: Manufacturer's data sheets on each product to be used, including:
        1. Preparation instructions and recommendations.
        2. Storage and handling requirements and recommendations.
        3. Installation methods.
     3. Verification Samples: For each finish product specified, two samples, minimum size 6 inches (150 mm) square representing actual product, color, and patterns.
     4. Manufacturer's Product Data: Submit manufacturer's data sheets indicating systems and components proposed for use.
     5. Shop Drawings: Submit complete shop drawings indicating system components, wiring diagrams and load calculations.
     6. Record Drawings: During construction maintain record drawings indicating location of equipment and wiring. Submit an electronic version of record drawings for the Security Management System not later than Substantial Completion of the project.
     7. Operation and Maintenance Data: Submit manufacturer's operation and maintenance data, customized to the Security Management System installed. Include system and operator manuals.
     8. Maintenance Service Agreement: Submit a sample copy of the manufacturer's maintenance service agreement, including cost and services for a two-year period for Owner's review.
  3. QUALITY ASSURANCE
     1. Manufacturer: Minimum ten years' experience in manufacturing and maintaining Security Management Systems. The manufacturer shall be Microsoft Silver Certified.
     2. The installer must be certified by Honeywell Integrated Security Dealer Service Certification Program (DSCP).
  4. DELIVERY, STORAGE, AND HANDLING
     1. Deliver materials in manufacturer's labeled packages. Store and handle in accordance with the manufacturer's requirements.
  5. PROJECT CONDITIONS
     1. Maintain environmental conditions (temperature, humidity, and ventilation) within limits recommended by manufacturer for optimum results. Do not install products under environmental conditions outside manufacturer's recommended limits.
  6. WARRANTY
     1. Manufacturer's Warranty: Submit manufacturer's standard warranty for the security management system.

1. PRODUCTS
   1. MANUFACTURERS
      1. Acceptable Manufacturer: Honeywell Commercial Security, which is located at: 715 Peachtree St. N.E.; Atlanta, GA 30308; Toll Free Tel: 800-323-4576; Email: [request info (Shellie.Redden@Honeywell.com)](https://admin.arcat.com/users.pl?action=UserEmail&company=Honeywell+Commercial+Security&coid=48331&rep=&fax=&message=RE:%20Spec%20Question%20(13710hsg):%20%20&mf=); Web: <https://buildings.honeywell.com/us/en/brands/our-brands/security>
      2. Substitutions: Not permitted.
      3. Requests for substitutions will be considered in accordance with the provisions of Section 01 60 00.
   2. SYSTEM DESCRIPTION
      1. Product: WIN-PAK Integrated Security Software manufactured by Honeywell Commercial Security.
      2. Functions as an electronic access control system and integrate alarm monitoring, CCTV, digital and network video, ID badging and database management into a single platform. A one-stop gateway for all access control needs. A modular and network-enabled architecture allows maximum versatility for tailoring secure and dependable access and alarm monitoring solutions.
      3. Components: Divided into six components: Database Server, Archive Server, Communication Server, User Interface, WIN-PAK API Server, and WIN-PAK Web.
         1. Components are to run on a single computer or on multiple computers, allowing flexibility in configuring a networked system.
            1. Database Server: For storing the database tables. Data is accessible to a communication server and user interface for retrieving and generating reports. Installed on the client computer or any other network connected computer.
            2. Archive Server: To obtain data from the archive database consisting of backup details of the WINPAK main database.
            3. Communication Server: Routes user interface requests and access transactions to the panel. The panel in-turn processes transactions and sends information to the database server as well as responses to the user interface through the communication server. When sending information to the database server, it can also receive a request from the user interface. The communication server will consider the user request as a higher priority and stops the panel-database server communication until the user request is processed. Installed on the client computer or any other network connected computer.
            4. User Interface; Client: Helps operators communicate with the access control system. Installed on the computer where the database or communication server is installed, or any other computer connected to the network. Client computers can simultaneously access the single database server simultaneously. The number of client computers varies based on licensing information of ISMS.
            5. WIN-PAK API Server: Used to obtain and set the details in the WIN-PAK database using the Application Programming Interface (API).
            6. WIN-PAK Web: Application is an extension of the WIN-PAK host application with limited operations. Operations such as Adding Cards and Adding Card Holders that are common to both WIN-PAK host and WIN-PAK Web application are saved on a common database server.
         2. Services: Includes the following components.
            1. Command File Server: Provides text files containing device instructions stored in the command files database. Commands in the command files can be sent to devices automatically on receiving, acknowledging, or clearing an alarm. Command files can be manually executed.
            2. Guard Tour Server: A defined series of check points a guard must activate within a given amount of time. Check points are readers or input points where the guard presents the card or presses the button.
            3. Tracking and Muster Server: Enabled in an emergency event allowing card holders to swipe the readers. Muster areas are logical areas that contain readers to be used by card holders, only if there is a call for muster, in the event of a disaster, for example.
            4. Schedule Server: Schedules the list of events to be performed at a predetermined time and intervals such as hourly, daily, or monthly.
            5. Video Management Server: Interface to connect to various DVR's/NVR's. Provides CCTV control with live monitor display, PTZ control of cameras and video playback operations.
      4. Operational Requirements:
         1. A modular and network-enabled access control system capable of controlling multiple remote sites, alarm monitoring, video imaging, ID badging, mobile credential provisioning, paging, digital video, and CCTV switching and control that allows for easy expansion or modification of inputs and remote-control stations. The control at a central computer location shall be under the control of a single software program and shall provide full integration of all components. It shall be alterable at any time depending upon facility requirements. The reconfiguration shall be accomplished online through system programming.
         2. Includes the Following Features:
            1. Multi-User/Network Capabilities: Multiple operator workstations via local area network/wide area network; LAN/WAN. Communications between workstations and server computer will utilize the TCP/IP standard over industry standard IEEE 802.3 (Ethernet). Communications between the server and workstations are supervised, and automatically generates alarm messages when the server is unable to communicate with a workstation. Operators on the network server have the capability to log on to workstations and remotely configure devices for the workstation. Standard operator permission levels shall be enforced, with a full operator audit.
            2. Operating Environment: True 32-bit or 64-bit, 3-tier client/server, ODBC compliant application based on Microsoft tools and standards. Operate in the following environments: Microsoft Windows Server 2016, Windows Server 2012 R2, Windows 10 Professional for workstations only.
            3. WIN-PAK Web: Using the Web interface, any operator from any customer location can access the WIN-PAK database server from any computer on the network. The operators at the customer sites must be granted appropriate access rights for accessing the WIN-PAK database server through the Web interface. These access rights are granted by the WIN-PAK Administrator using the WIN-PAK host application.
            4. Multiple Servers: Consist of multiple servers including, but not limited to, database server, communications server, and client workstation. Servers to be capable of being installed on one or more computers across a network providing a distribution of system activities and processes. Support multiple communication servers on a LAN/WAN, to provide distributed networking capabilities, significantly improving system performance.
            5. Multi-level Password Protection: Multi-level password protection, with user-defined operator name/password combinations. Name/password log-on shall restrict operators to selected areas of the program. The application shall allow the assignment of operator levels to define the system components that each operator has access to view, operate, change, or delete.
            6. Graphical User Interface: Compliant with Microsoft Graphical User Interface (GUI) standards, with look and feel of software being that of a standard Windows application, including hardware tree-based system configuration.
            7. Online Help: User interface will include an Online Help requiring one click to activate. Special function key "F1" shall have the capability to be programmed to provide access to the help system.
            8. Guard Tour: The Security Management System shall include a guard tour module, which shall allow the users to program guard tours for their facility. Tours will not require independent or dedicated readers.
            9. Concurrent Licensing: Support concurrent client workstation licensing. Install on any number of client workstations and provide the ability for any client workstation to connect to the database server if the maximum number of concurrent connections purchased has not been exceeded.
            10. Concurrent Browser Connections: A minimum of 100 concurrent web connections to be included as standard to manage day-to-day access control tasks including but not limited to: Card and Cardholder (Names, Notes fields, Note Field creation and Note Field templates); Badge Printing; Door Schedules; Lock Control; Panic Door control; Schedules; Holidays; Access Level; Reports; Report Templates and Schedules; Messaging, viewing live card activities and Locate functions.
            11. WIN-PAK supports multiple installation types.

Single Server Deployment: Installs all the WIN-PAK components such as client, server, web, API, VMS, and support programs.

Dual Server Deployment: The dual server deployment is hosted on two computers. The first computer, server 1, will have the complete host, API, and the VMS installed. The second computer, server 2, will have the host User Interface, Remote communication server, VMS, and Web installed.

* + - * 1. Relational Database Management System: Support industry standard relational database management systems including Microsoft SQL Server 2016 Enterprise Edition. Provide edit, add, delete, search, sort, and print options for records in the selected databases.
        2. Database Partitioning: The Security Management System will provide the option to restrict access to sensitive information by user ID.
        3. Unicode: The Security Management System shall utilize Unicode worldwide character set standard. The Security Management System shall support double-byte character sets to facilitate adaptation of the Security Management System user interface and documentation to new international markets. Language support shall include at a minimum English and French.
        4. Encryption: The Security Management System shall provide multiple levels of data encryption.

True 128-bit AES data encryption between the host and intelligent controllers. Encryption shall ensure data integrity that is compliant with the requirements of FIPS-197 and SCIF environments. Master keys shall be downloaded to the intelligent controller, which shall then be authenticated through the Security Management System based on a successful match.

Transparent database encryption, including log files and backups.

SQL secure connections via SSL.

Asymmetric Column level encryption is used for personal data fields (Card Holder's First name, Last name, Note fields) in the SQL data fields.

* + - * 1. Industry Standard Panel Communication: Communicates with access control panels via LAN/WAN connections utilizing industry standard communication protocols.
        2. Supervised Alarm Points: Both supervised and non-supervised alarm point monitoring. On recognition of alarm, system can switch and display video from camera connected to digital video recorder associated with alarm point.
        3. Multiple Account Support: Allowing separate access to the card database, badge layout, operator access, and reporting. Physical hardware may be filtered by operator level into sites. Sites may reside in multiple accounts.
        4. Logical Representation of Hardware Devices: The ISMS shall use Abstract Devices (ADV) for representing physical hardware devices in the system. The ADVs shall be used in Floor Plans to provide the user interface to control and monitor the system and shall also be used in the data trees to organize, display, and control system information.
        5. Access Control Functions: Validation based on time of day, day of week, holiday scheduling, site code, card number verification, automatic or manual retrieval of cardholder photographs, access validation based on positive card verification, card and PIN, card or pin, pin only and Site Code only.
        6. Digital Video Recorders (DVRs) Support: ADPRO, MAXPRO NVR, 35 Series Recorders and legacy Embedded Performance Series DVRs.
        7. Camera Functions: Pan/tilt, lens control, limits, and home.
        8. Live Video Display: An option to view live video from a camera connected to the digital video recorder on the computer screen. Allow users to change its size and location on the computer screen. Video controls (pan, tilt, zoom) to be available to customize the live video display to the user's requirements.
        9. Global and Local Anti-Passback: Support use of Anti-Passback mode. Cardholders must follow a proper in/out sequence within the assigned area.
        10. Alarm Events: Alarm events with defined priorities pop up automatically in the Alarm event window for operator attention. The pop-up displays the name of event (reader, alarm point, cardholder, or system alarm), time, date, site, account. In a card event, the card number, type of event and cardholder name are displayed. An event counter displays the number of times an event was reported to the Alarm event monitor prior to Acknowledgement or Clearing the event. Event instructions to be made available by double clicking on event. The event will display an icon to indicate that video is available for events so programmed. Alarm event window allows operator to initiate a physical response to the event as well as a written response. Responses include but are not limited to acknowledge, clear, open a pre-programmed floor plan, energize, de-energize, pulse, time pulse, add comment, retrieve event video, and bring up live video, shunt, or un-shunt.
        11. Manual Panel Control: Manual control of selected inputs, outputs, and groups of outputs. Include pulse, timed pulse, and energize/de-energize or return to time zone options for output points and shunt/unshunt or return to time zone options for input points. For entrances and readers manual control shall include but be limited to Lock, Un-Lock, Disable, Card only, Card-Pin only, Pin only, exit only and site code only. For partitions monitored by the intrusion panel the control shall include but not be limited to arm away, arm stay, disarm, refresh, and provide a virtual keypad for the partition. For zones monitored by the intrusion panel the control shall include but not be limited to bypass, unbypass, and refresh. Intrusion panel output control shall include activate, deactivate, and refresh.
        12. Levels of System Operation: Includes a feature to define the levels of system operation for each individual operator using passwords. System operation for individual operators shall include, but not be limited to, restricted time periods for login, available accounts, and default language selection at login. Operator actions range from no view or control rights to basic monitoring including the ability to block the viewing of card and or personal identification numbers, to full control of the system including programming.
        13. Hardware Configuration Changes: After installation of application, the customer shall be able to perform hardware configuration changes. These hardware configuration changes shall include, but not be limited to, door open time, door contact shunt time, point and reader names, when and where a cardholder is valid, and the ability to add or modify card databases as desired; For the intrusion system, any function that can be programmed from a physical keypad shall also be available from the system's virtual keypad, without the services of the Contractor or Manufacturer.
        14. Distributed Processing: All the control components shall utilize "Distributed-Processing" concepts. This includes the ability to download operating parameters to any field panel, thus allowing the field panel to provide full operating functions independent of the access control system computer.
        15. Flexible Component Replacement: Repair of hardware components associated shall be accomplished on site, by a new replacement, utilizing spare components.
      1. The application will have functional capabilities, considered essential for the system, categorized as follows:
         1. General:

Databases: Ability to add, delete, report, view, and edit information.

System Transactions: Saved in a retrievable file.

Events: Logged by date and time.

System or Selected System Transactions: Saved in a disk file.

End User: Has provisions to make any system configuration changes such as, but not limited to door open time, door contact shunt time, point and reader names, when and where a cardholder is valid, and the ability to add or modify card databases at any time.

Global Anti-Pass Back: Allows cardholders to enter/exit any such defined card reader on the same intelligent control panel or RS-485 dropline consisting of 2 and 4 door controllers.

Anti-Pass Back Modes: Include hard (no forgiveness), soft (allows access but generates an alarm event) and timed for all readers on the intelligent controller, on specified reader or card for a definable period of time up to 32,000 seconds.

Duress Feature: Where a PIN is used in conjunction with a card read; the numbers of digits are selected using the keypad where the PIN number is a value different from the normal PIN.

Two Card Holder Rule: Where two valid, non-identical "cards" must be used within a 20 second period to grant access.

Option to display the time when a card holder using a reader has accessed (opened) the door or the card was used, but the door was not opened.

Latch Mode Operation: Where the first card read unlocks the door and the second card read locks it.

System Operation Modes:

Stores system commands not accepted by the hardware.

Requires the operator to enter a response to an event when acknowledging it from the alarm view window.

Allows acknowledged alarms to be automatically cleared.

When an acknowledged, but not cleared event will be reissued requiring acknowledgement when the event changes to an alarm or trouble state.

Does not allow the operator to clear an alarm before prior to it being restored to normal.

Manual operator control of system output relays. Manual Functions: Include the ability to energize, de-energize, return to time zone, or pulse the output relay. The pulse time shall be a programmable setting.

Manual operator control of system doors. Manual Functions: Include the ability to Lock, Un-Lock, Disable, Card only, Card-Pin only, Pin only, exit only and site code only.

Automatically display stored "video image" of cardholder and switch real-time camera from CCTV or digital video server to card reader location for specific card usage.

The cardholder "video image" pop-up shall be activated based on a priority level set to the cardholder or reader. Information in the pop-up shall include, but not be limited to the card holder's primary image, a live video pop-up showing the person who initiated the pop-up, entrance name, time, date, cardholder name, and status. User shall be able to display up to 40 note fields. The size of the pop-ups shall be adjustable by the operator.

Multiple card reader technology including Proximity, Wiegand effect, Biometrics, Magnetic stripe, Bar Code, Keypad, Card/keypad (PIN), High-speed long-range Vehicle ID, Smart Card, and mobile credentials (smart phone with a credential/app).

Option for taking scheduled automatic backups of any or all database system files. Include a means to restore these files from a simple menu.

Ability to address 255 serial communication ports per communication server, where each port can be configured for hardwired, or dial up. Dial Up Configuration: Any one port can support multiple dial up locations.

Communication from access control communication servers to remote intelligent control panels shall be selectable.

Communication Options: RS-232 directly to the intelligent control, via RS-485 converter, dial-up, leased line from a defined communication port or by LAN/WAN using an IP address for direct connection to the intelligent controller via network interface card.

IP Addressing: Unacceptable to use a communication port converter device on the communication server side of the transmission. A minimum of 255 such IP connections shall be allowed per communication server.

Commands and Updates to the Panels: To be verified and automatically retry if communications fail.

System Scheduler:

Automatically calls remote locations to retrieve history transactions and update panel information, including time and date.

Activate or deactivate cards locally or at remote dial-up sites. Initiate a pre-programmed command event/action,

Synchronize system to intelligent controller time,

Run a pre-defined (template) History report. Run a pre-defined (template) Card Holder report, Card frequency report defined by readers, over a defined period of time with disposition options to automatically report or report and de-activate card or change the access level of the card, Frequency shall be defined as Never, Now, Once, Hourly, Daily, and Weekly, Once per 2 weeks, and Monthly.

Drop Boxes: For all system-required information that the user has previously entered.

Ability to initiate an email (via SMTP using SSL and TLS services) or page to a paging system based on a transaction state.

Transaction States: Defined as but not limited to Normal, Alarm, Trouble, Ajar, Trace, Not Found, Anti-Passback Violation, PIN Violation, Time Zone Violation, Site Code Violation, Door Used, Duress, No Second Card Presented, Trace Card or Expired Card, and System Alarms including, Panel Com, Panel Power Failure, Modem Pool, Guard Tour, and Tamper.

Intrusion Partition Events, Including but not Limited to: Alarm, Alarm Cancel, Aram Away, Arm Stay, Auto Arm, Auto Disarm, Bypass, Disarm, Early Arm, Early Disarm, Fail to Arm, Fail to Disarm, Normal, Not Ready, Part Arm, Quick Arm, Recent Close, Remote Arm, Remote Disarm, Unbypass, User Code Added, User Code Deleted, user Code Edited.

Intrusion Zone Events, Including but not Limited to: Alarm, Alarm Restore, Bypass, Fault, Fault Restore, Normal, Trouble, Trouble Restore, and Unbypass.

Intrusion Output Events, Including but not Limited to: Alarm, Communication Loss, Normal, Tamper, and Tamper Restore.

Intrusion Panel Events, Including but not Limited to: Access Denied, Automatic Test, Comm Fail, Comm Restore, Faults, Faults Restore, Line Restore, Line Trouble, Manual Test, Pager Restore, Pager Trouble, AC Restore, AC Trouble, Alarm, Battery Low, Battery Low Restore, Disarm, Normal, Recent Close, Reset, Panic Alarm, Power Up, Program begin, Program Changed, Program End, System Shutdown, System Shutdown Restore, Tamper Alarm, Tamper Restore, Test End, Test Start, Time/Date changed.

Host Grant Mode of Operation: Requires host computer to grant access to "valid" cards. An alternate host grant mode shall allow the card access information to be downloaded along with unlocking the door for "valid" cards.

* + - * 1. Sub Accounts: An extension of the Accounts feature.

Allows management of spaces, credentials, and card holders relative as a separate group (subaccount) within the account.

Typical Application: An account being a multitenant building where each tenant (subaccount) manages their people and doors along with doors common to all in the building/account while only seeing and managing their people When an account is created, a sub-account is created by default. You can add multiple sub-accounts to an account. Administrators can create and manage sub-accounts within their parent account.

Administrators can add, select, edit, and delete sub-accounts by using their respective menus under account.

* + - * 1. Cards:

A simple card and card holder database import utility. The utility shall be password protected and accessible only to administrators of the access control system. Information that can be imported shall include but not be limited to: First Name, Last Name, Card Number, Activation Date, De-activation Date, Status, up to 40 note fields and Photo Images. A simple CSV (comma separated value) file shall be used for the importing of data and image file names.

Cardholder Information: Includes a unique card number up to 20 digits and an optional Personal Identification Number up to 10 digits.

Allow multiple cards, mobile access credentials or fingerprint enrollment per cardholder.

Allow 32 access levels to be assigned to a card, or a single "precision" access level. When using "precision" access levels it shall be possible to create a unique access level per card using an existing access level as a baseline template. This customized card access level shall have both beginning and ending dates.

Provide 40 user defined fields.

Each card holder note field shall allow the option to be entered as free form data or structured data. Structured data shall be by use of a template or drop list. The template and drop list shall be created by the operator. The capacity of the template shall allow for up to 65,000 characters.

Special Card Options Include, but are not Limited To:

Time zone reference, which defines valid time.

Visitor use, which provides a specified activation date and expiration date (spanning years).

Limited use up to 255 uses.

Allow arming of the intrusion system.

Standard, Supervisor and VIP card type providing special door privileges based on scheduled or event based functions.

Trigger control value, which can initiate a predefined procedure at the intelligent control independent from any control function from the system computer.

Card Tracing Function: Allow normal access control but provide a tracking alarm at the system monitor.

Store up to 99 digital images of cardholders or other digital images such as property or family members.

Store a written signature of cardholder or other signatures such as family members. Up to 99 such signatures shall be associated with the cardholder.

Prioritize up to 99 specific card event types with separate priority options that include but are not limited to Anti-pass back, Trace, PIN Violation, Normal, Not Found, Expired, Host Grant, Site Code and Time Zone card activities or violations.

Allow user the ability to send an e-mail message, selectable per card event type.

Upon Editing the Card and Biometric Information: The updated information shall be sent automatically to the appropriate access control panel, when hardwired, with no other user intervention. If the port is dial up, the entry will be stored on disk and updated when connection is made to the remote loop. If the scheduler is used, then card updates shall be sent based on scheduling.

In a traditional (Wiegand) 5-digit card database, the numbers 0 and 65,535 shall not be valid card numbers as some devices transmit these numbers on an improper read.

Duplicate Card Numbers: Not allowed within an Account. However, if more than one account is used, each account can have a single occurrence of the same number and per account that card number can be used by a different card holder.

Integrated Biometric Enrollment Functions: To be managed directly inside the PAC UI without the need to use a 3rd party software.

Integrated assignment/managing/enrollment of mobile access credentials shall be accomplished inside the PAC UI without the need to external or 3rd party portals or software.

1.Access Levels:  
a.Define specific access times.  
b.Define specific readers for access.  
c.Template of Defined Access Level Detail: Changes can be made to the template and saved as a new access level detail.

* + - * 1. Access Control Tree Structure: Allows groupings of entrances. Users to have the ability to group program all entrances on the branch or make specific changes to individual entrances.

e.Option per reader so configured, to select a predefined group of relays to utilize instead of a single relay. Commonly used for elevator control applications. The relay "Group" can also provide uniquely programmed pulse time used to allow varying access time for special needs application.

* + - * 1. Video Management Server: Support the following Digital Video Recorders (DVRs): ADPRO, MAXPRO NVR, 35 Series Recorders and legacy ENVR.

Interface to configure DVRs to a video management server.

Interface to configure cameras, inputs, and outputs to the DVRs.

Interface to a network of digital video servers.

Interface to discover all the cameras connected to the DVRs.

Manually access live video from any camera on any defined digital video server.

Viewer Windows: Allow 16 live videos to be displayed at a time.

Viewable Size of Viewer Salvo Window: Adjustable by using the "click and drag" method. When adjusting height or width, the image is to retain the correct aspect ratio.

Automatically pop-up any camera in the system based on any alarm point, system alarm or cardholder video image pop-up.

Manually control the pan, tilt, and lens functions (zoom, iris, and focus) of cameras so equipped.

A "live view" from the Digital Video Server is displayed on the system computer without the use of any add-in video capture card.

Live Views: Allow for the change in image resolution or aspect ratio to optimize the viewing quality to the native video.

Ability to change the size and location of the view.

Digital Video Server Window: Will also supply the ability to select a digital video server, camera, live, from stored video using user defined time and date.

A filter option allows the operator to define a date, time, transaction type, devices, card holder, card number, note field, card event type and alarm status. Once filtered all events will be displayed in a listing.

The listing includes on the event lines any associated video clips.

By clicking on the event, the time, date, camera, and digital server shall be preloaded in the manual selection boxes allowing the operator to simply click on the sorted event and then click on "show" to display the recorded event.

Video Masking with Four-Eye override will ensure privacy is managed in accordance with GDPR requirements.

* + - * 1. Camera Control:

Configure settings of cameras connected to the respective DVRs.

Manually control the pan, tilt, and lens functions (zoom, iris, and focus).

Automatically switch any camera in the system to any monitor in the system based on any alarm point or system alarm.

Display the live and recorded video in salvo window.

A set of options such as color correction, sync playback, flip, playing speed, and remove text overlay to customize the display of live and recorded video.

Configure the Video Motion, Video Loss, and PTZ loss events to cameras associated to all the DVRs.

* + - * 1. Alarm Monitoring; Alarms Only View:

Report alarm point activity.

Provide color for each specific alarm point action, "Alarm", "Normal", and "Trouble", conditions.

Ability to access the default floor plan graphic for any active alarm point by a right click option.

Live Video Pop-Up: From the digital video servers and are to follow the alarm event pop-up. There are to be no less than 16 possible live camera views in the pop-up window. The live pop-up window allows the user to define the quantity of views from 1 - 64. The live pop-up window is to be size adjustable.

Bypass alarms in the system.

Execute alarm notification in all modes of operation.

Acknowledge any intrusion alarm, event alarm, system alarm, card, or reader activity based on priority.

Display of system activity with the higher priorities displayed at the top of the list with identical points stacked with a frequency count of each point's change of state.

A video icon for events that have video associated with it. Right-clicking on such an event shall allow the option to retrieve recorded video or view "live". The stored video clip shall playback by default a minimum of 2 seconds before the actual event without any adjustment.

Viewable alarms include but not limited to:

Access Control Related Events: Door Normal, Door Alarm, Door Trouble, and Door Ajar.

Card Events: Not Found, Anti-Passback Violation, PIN Violation, Time Zone Violation, Site Code Violation, Door Used, Escort access Granted, Site Code Violation, Invalid format, Supervisor card Authenticated, Supervisor card Found, Supervisor mode Disabled, Supervisor mode Enabled, Supervisor card Required, Temporary Card Expired by Date, Temporary Card Expired by Number of Uses, VIP card Found, Duress, No Second Card Presented, Trace Card or Expired Card, and System Alarms including, Panel Com, Panel Power Failure, Modem Pool, Guard Tour, and Tamper.

Intrusion Partition Events: Alarm, Alarm Cancel, Arm Away, Arm Stay, Auto Arm, Auto Disarm, Bypass, Disarm, Early Arm, Early Disarm, Fail to Arm, Fail to Disarm, Normal, Not Ready, Part Arm, Quick Arm, Recent Close, Remote Arm, Remote Disarm, Unbypass, User Code Added, User Code Deleted, user Code Edited.

Intrusion Zone Events: Alarm, Alarm Restore, Bypass, Fault, Fault Restore, Normal, Trouble, Trouble Restore, and Unbypass.

Intrusion Output Events: Alarm, Communication Loss, Normal, Tamper, and Tamper Restore.

Intrusion Panel Events: Access Denied, Automatic Test, Comm Fail, Comm Restore, Faults, Faults Restore, Line Restore, Line Trouble, Manual Test, Pager Restore, Pager Trouble, AC Restore, AC Trouble, Alarm, Battery Low, Battery Low Restore, Disarm, Normal, Recent Close, Reset, Panic Alarm, Power Up, Program begin, Program Changed, Program End, System Shutdown, System Shutdown Restore, Tamper Alarm, Tamper Restore, Test End, Test Start, Time/Date changed.

Ability for operators to acknowledge and clear alarms from display. Prior to acknowledgment, users are to be allowed to enter a response per alarm. The system shall offer a means to require acknowledgement of an alarm before it can be cleared.

A display of the most current transactions in real time.

Ability for dynamic alarm monitoring of alarm points in real time on the system computer's video display terminal.

An alarm view filter is structured as a tree allowing the operator to select individual devices or groups of devices to be viewed.

A "System" alarm upon a loop integrity violation.

A "Panel Not Responding" alarm if communication to a panel is lost.

Real time printing of alarms as they occur by line printing with a dot matrix printer or provide printing of alarms, one page at a time, using typical Windows page printing.

* + - * 1. Alarm Monitoring/System Control - Tree View:

Dynamic alarm monitoring of alarm points in real time on the system computer's video display terminal.

Color and icon shapes for each specific alarm point action of "Alarm", "Normal", "Trouble", and "Shunted".

Access control panels in the alarm tree, like alarm points, shall also indicate if they are in the buffered mode of operation as well as any "system" related alarm such as "Tamper" or "Primary Power Loss" or Loss of communication.

Devices connected to the communication server shall provide additional popup information as to the communication port or IP connection the device is programmed for.

Launch a Virtual keypad from an intrusion panel partition to monitor the physical keypad remotely and to administer programming changes via the Virtual keypad.

The control tree shall be created by the user and allow for manual control of all system devices.

By right clicking on a device in the tree, the operator can initiate the appropriate action from a pick list.

Actions shall include but not be limited to: Acknowledge All Alarms, Clear All Alarms, Send Time and Date, Send Camera Titles, Camera to Monitor Switch, Control Camera P/T/Z, Focus, Iris, Live Video, Retrieve Video from Clip, Run Command File, Lock, Unlock, Shunt, Unshunt, Pulse, Timed Pulse, Restore to Time Zone (Door Mode), Time Zone Schedule creation, change, Override Online Door Mode (Open, Lock, Card only, Card or PIN, Card and PIN, PIN only, Supervisor mode enable/disable, Supervisor mode, Escort Mode, Standard Mode), Initialize, Cancel Initialization, Buffer, Unbuffer, Connect Remote and Disconnect Remote from remote site.

For partitions monitored by the intrusion panel the control shall include but not be limited to arm away, arm stay, disarm, refresh, and provide a virtual keypad for the partition.

Zones monitored by the intrusion panel the control shall include but not be limited to bypass, unbypass and refresh.

Intrusion Panel Output Control: Include but not limited to Activate, deactivate, and refresh.

* + - * 1. Operator Database:

Allow assignment of operator levels to define the system components that each operator has access to view, operate, change, or delete.

View, edit, or delete cardholder sensitive information such as note fields, card number, PIN to be definable in field per operator.

Define the accounts that the operator has access to.

Log operator actions in the history files.

Select the default language during operator logon.

Specified time periods for the operator to log on.

Ability to select if access to the Web browser is allowed.

* + - * 1. Access Control Panels: Program Action Messages and assign an alarm event priority. Specific action messages may be displayed for each alarm, system alarm (communication, ground fault, power, panel reset, low voltage, and panel tamper), card, or reader usage state.

States include but not limited to: Wrong Password, Panel Configuration Error, Panel Remote Dial-up Failed, Panel Remote Dial-up Successful, Poll Response Alarm, Poll Response Normal, Primary Power Failure, Primary Power Normal, Tamper Switch Alarm, Tamper Switch Normal, Unsupported Panel Version, Anti-Pass back Violation, Anti-Pass back Violation Door Not Used, Anti-Pass back Violation Door Used, Card Not Found, Door Normal, Door Alarm, Door Trouble, Door Ajar, Door Locked, Door Unlocked, Duress Request Denied, Duress Request Door not Used, Duress Request Door Used, Forced Open, Free Egress Door Not Used, Free Egress Door not Verified, Free Egress Door Used, Host Grant Card Downloaded, Host Grant Door Unlocked, Invalid Format, Invalid Format Reverse Read, Invalid Pin, Invalid Site Code, Invalid Time zone, Issue Code, Never Allowed at this Door, No Second Card Presented, Site Code Verified Door Not Used, Site Code Verified Door Used Trace Card, Valid Card Door Not Used, Valid Card Door Used, Escort access Granted, Site Code Violation, Invalid format, Supervisor card Authenticated, Supervisor card Found, Supervisor mode Disabled, Supervisor mode Enabled, Supervisor card Required, Temporary Card Expired by Date, Temporary Card Expired by Number of Uses, and VIP card Found.

Intrusion partition events include but not limited to: Alarm, Alarm Cancel, Aram Away, Arm Stay, Auto Arm, Auto Disarm, Bypass, Disarm, Early Arm, Early Disarm, Fail to Arm, Fail to Disarm, Normal, Not Ready, Part Arm, Quick Arm, Recent Close, Remote Arm, Remote Disarm, Unbypass, User Code Added, User Code Deleted, user Code Edited.

Intrusion zone events including but not limited to: Alarm, Alarm Restore, Bypass, Fault, Fault Restore, Normal, Trouble, Trouble Restore, and Unbypass.

Intrusion output events including but not limited to: Alarm, Communication Loss, Normal, Tamper, and Tamper Restore. Intrusion panel events including but not limited to: Access Denied, Automatic Test, Comm Fail, Comm Restore, Faults, Faults Restore, Line Restore, Line Trouble, Manual Test, Pager Restore, Pager Trouble, AC Restore, AC Trouble, Alarm, Battery Low, Battery Low Restore, Disarm, Normal, Recent Close, Reset, Panic Alarm, Power Up, Program begin, Program Changed, Program End, System Shutdown, System Shutdown Restore, Tamper Alarm, Tamper Restore, Test End, Test Start, Time/Date changed, Identification Success: Fingerprint, Identification Success: Fingerprint and Card, Verification Success: Card, Verification Success: Card and Fingerprint, User download success, Identification Failed, Verification Failed, Not Granted, Identification Duress.

Program descriptions, shunt times, and momentary shunt times for all system alarm points.

Program descriptions, pulse times, and energize times for all system output relays used for door control and other auxiliary functions.

Program descriptions for all system card readers.

Monitor supervised and non-supervised alarm points with the ability to select by point which point shall be supervised and define if the point is a normally closed or normally open point contact.

Interlock any alarm point condition to an output relay.

Interlock any alarm point condition to another alarm point.

Interlock any alarm point to switch a camera to a system monitor.

Program alarms and associate incoming alarms with related outputs.

A programmable "delay" setting of 255 seconds for all system alarm points. The system shall not report the alarm condition until the delay setting has expired.

Allow 8 different site codes to be used in the system.

Support 32 readers per Intelligent Control Module.

* + - * 1. Reports:

Card holder report capability with filter options to define doors that a card holder has access to, reporting card holder name, Cards, Access Level/schedules, Activation/Expiration. Available in the Browser and workstation.

Reporting capability for printing of selected system transactions from the disk files by specific time and date selection, range from time and date to time and date, or from start time to end time each day of the selected date range. Available in the Browser and workstation.

Reporting capability for selected card number displaying an audit trail of card changes detailing from-to when and by who. Changes shall include but are not limited to access level changes, activation/expiration dates, card number edits, and card holder name changes. Available in the Browser and workstation.

History Reports for an Alarm Points State: Defined as Normal, Alarm, Trouble, or Ajar.

History Reports of System Alarms. A System Alarm State is defined by the panel and includes any of the following data: Communication, ground fault, power, panel reset, low voltage, panel tamper, and loop communication.

Abstract Device (ADV) Action Reports. Provide information on how the system ADVs are configured including detailed/advanced video configurations.

History Reports for a Card's State. A card state is defined as Normal, Trace, and Not Found, Anti-Passback Violation, PIN Violation, Time Zone Violation, Site Code Violation, or Expired card, Identification Failed, Verification Failed, and Not Granted.

Filter reports for defined reader locations.

Available in the Browser and workstation.

Additional search criteria available at the workstation includes cardholders that meet up to at least 3-note field restrictions.

History Report for System Operators Activities: Report includes time, date, operator name, the device associated with the action and type of operator action performed.

Activities: Include but not limited to acknowledged and cleared transactions, camera control, door mode, door, and relay controls such as unlock, lock; door and input controls such as shunt, Unshunt; login, logout, panel initialization, panel buffer and panel Unbuffer.

Complete Database Report: All data programmed into system data files.

Report how long a card holder has been in a defined area:

Allow time to be accumulated representing an attendance report. Definable Filters: Include time/date range, readers definition, card number, card holder and note field.

Report Output: Sort options to include First Name, Last Name, Event Time, and Card Number. Data to be selectable as Alpha or Numeric sorting and Ascending or Descending.

Report Based on Card Usage Frequency:

Operators may define a time/date period, a minimum and maximum usage limit, a means to define which reader or readers should be used to filter the report and the ability to further define the type of card to be reported on based on note field selections.

Report Availability: In the Browser and Workstation.

Workstation will provide a disposition function.

Cards Meeting Filtering Criteria: Will be acted upon based on the disposition setting.

Disposition Settings: Includes but not limited to; Report only, De-activate the card or Re-assign to a specified access level.

Report to also be available in the event scheduler.

When defining when to run the report, an option to select the number of previous days to run the report against shall be provided. As an example, a scheduled weekly report for the last 14 days could generate allowing for an overlap of time if desired.

Create Report Templates: Report templates available in the Browser and Workstation include, but not limited to, Access Level, Card, Card History, Door, Holiday, Time Schedules, and Card Holder information.

Templates may be assigned to a scheduler to run automatically per the scheduler settings.

* + - * 1. Tracking/Muster Report:

Tracking Feature: Allows system operators to identify an area and the persons in that defined tracking area. Defined Tracking Areas provide an automatic update of how many cardholders are in the area.

Defined Tracking Areas: Defined by readers representing an IN or OUT read status.

Areas Defined as Exits: Shall remove people from the tracking areas.

A view displaying cardholders in a defined tracking or muster area shall have the ability to be sorted in columns whereby clicking on the column the data in the column shall be sorted. At a minimum, the columns can be sorted by: Card Number, Status, Card Holder, Reader, and Time/Date.

Muster Area: Defined by readers used to "Muster" individuals in the event of an emergency.

Reports can be generated for the defined muster or tracking area.

Report Availability: In Browser and Workstation.

Reports may be generated for all muster or tracking areas in the system.

Tracking and Muster Report Templates: To be defined including whether it should be emailed and/or printed based on Events, Schedules or assigned to a "Hot key" on the tool bar to be manually run when needed.

Report Sorting: On time and date, card number, card holder name or matching note field. When sorted on note field, a page break between fields shall allow the report to be easily handled for departmental uses.

Tracking areas shall include "nested" areas. Nesting: Allows for various reports from a large area to smaller areas within the large area.

A Tracking and Muster area screen shall be continually updated with the most recent cardholder activity, therefore minimizing the time required for generating a report.

A history priming feature shall load history activities for the defined number of hours when the software is started. This priming feature shall be implemented if the system computer is offline when a muster call is initiated, thereby allowing the implementation of the tracking and muster features of the software. The history priming time shall be operator selectable in 1-hour increments up to 99 hours.

* + - * 1. Time Zones:

Time zone definitions shall include Starting time, Ending time, Days of the week, and Holiday override.

Time shall be defined in either AM/PM or 24-hour (military) time.

The minimum time zone that shall be assigned to a panel is 128.

The maximum time zones that shall be defined in a system is unlimited.

Holidays shall be defined in two different time zones allowing different time schedules to be programmed for each holiday type.

Holidays shall be grouped in a Holiday Group.

* + - * 1. Floor Plan Graphic: Capable of the following.

Import floor plan graphics stored in a WMF format.

Associate all ADV's (access, intrusion, and video) to floor plan graphics allowing users to control and monitor the system.

Link floor plan graphics together in a hierarchy fashion.

Multiple floor plan views to be displayed simultaneously.

* + - * 1. Remote Locations:

Communicate to panels in real-time via encrypted Ethernet communication or support remote dial-up locations. Dial-up locations are to support the ability to place remote control panels in an offline mode.

Offline Mode: Remote-control panels will retain all panel history events.

Number of Historical Events: Limited to panels' buffer capacity.

Place remote control panels in an offline mode where remote panel automatically calls to the communications computer to report system alarms or upload buffered events.

Manage up to 250 remote locations per communication server.

User-Defined Schedule: Automatically add cards to any number of sites.

\*\* NOTE TO SPECIFIER \*\* Delete paragraph if not required.

For Remote Panels not Configured for Real-Time Communications: Provide system time schedules the computer will use to automatically start uploading data to or downloading data from the remote sites.

Data to be sent to the panel includes, but not limited to, card database changes, time, date, and buffer condition.

Data received from panel includes all buffered events. While connected to the remote site, the system software shall poll, verify, and report any loss of panel communication.

If a site's communication time is longer than expected, the system will automatically adjust the time schedule to allow all selected sites to be updated.

The remote site can also be supported via an auto dial schedule allowing system to automatically dial the remote site at a predetermined time.

Auto Dial Schedule: Programmed with ability to dial Once, Now, Hourly, Daily, Weekly, Two Weeks, Monthly, or Never to the remote site.

Ability for operators to program when the next scheduled update will occur, based on time and date.

Communication to remote dial up sites to be accomplished using password protection. Remote sites provide a system with a site ID; the system responds with appropriate password. No commands or transactions occur until the communication link is verified.

The System can receive or send information to remote access control panels on demand.

Redial Attempts from Remote Location: Define from 1 to 5.

Pause Between Redial Attempts: Define from 1 to 120 seconds.

Pause Before Disconnecting: Define from 1 to 30 seconds.

* + - * 1. Guard Tour: Allow operators to program a series of guard check points that must be activated to accomplish the task of a Guard Tour.

Check Points: Card readers, alarm contacts, or mixture of both.

Guard Tour: Timed and sequenced with travel time ranges between check points with +/- tolerance. This allows alarms to be generated for early, missed, or late events.

Guard Tour: Un-sequenced with no time parameters.

Guard Tour Start Methods: Manual or scheduled by access control system scheduler.

* + - * 1. ID Badging System/Video Image System:

Allow any card data fields to be assigned to a badge.

Allow stored cardholder images to be associated to any background.

Each cardholder shall have any one of the background layouts associated with it.

Create temporary or permanent badges.

Badge Printing Via Workstations: Without assigning an access level or access control card number.

Numbers and access levels may be assigned after printing.

Badge Printing Via the Browser: After a card number has been assigned to the Cardholder.

Image Export Capability. Utilizes the Cardholder's name as the file name in .jpg format.

Unlimited Custom Badge Layouts: Only limited by hard disk capacity.

Color Palette: 24-bit (16.7 million) for background design or foreground text.

Implement all fonts supported by Windows.

Import Capabilities:

Background Information: Using video camera, BMP, JPG, or TGA files.

Video Images: From compatible BMP, JPG, PCX, or TGA files.

Be able to import multiple bitmap images to the badge layout.

Video Capture Capability:

Compatible TWAIN device.

DirectX device.

Compatible video capture device, i.e. a high-resolution color camera.

Badge Format: Horizontal or Vertical.

Printout of Cardholder Badge: By video or standard printers supported by Windows.

Allow multiple card enrollment/badging stations on networked system.

Text Fields: Limited to 255 characters per field.

Merging of data fields from card database to text field.

A field to be defined for bar code usage merging data from the card database.

Allow 99 different photos of the cardholder to appear on the same badge.

Provide line, rectangle, rounded rectangle, and ellipses to be created on the backdrop with provisions for line thickness and color.

Signature capture or import capability for 99 signatures that can be previewed in the cardholder's badge or printed on the cardholder's card.

Capable of printing a Cardholder's front and back selected layouts in one step (requires suitable printer) without reinserting the card.

Encode magnetic stripes with information from any of the card data fields to include, but not limited to: First Name, Last Name, Card Number, Activation date, Expiration Date, or any data from Cardholder's note field.

Encode data on track 1, 2, or 3 (requires suitable printer) without reinserting the card. Each track to be encoded with ABA, IATA, or TTS format.

* + - * 1. Networking:

Networking Capabilities (LAN or WAN): As allowed by the computer's operating system license.

Access Control Software: Two networking methods. Functionality to be one or the other and not both modes at the same time.

Domain Controlled Networks: For secure networking communications.

Peer-to-Peer (Workgroup) Networks: For lower security installations.

Network systems to support concurrent users up to the license limit (one station adding cards and making badges, another station monitoring alarms, yet other running data base reports, another controlling door openings and alarm shunting, and so on).

Workstations to have the same user interface functionality as the Server, except performing database maintenance functions.

* + 1. System Software and Hardware:
    2. NOTE TO SPECIFIER: Delete computer performance not required.
       1. WIN-PAK ISS shall be installed on a computer that supports 1 to 10 readers, 250 cards, and 2 communication ports. Workstations added to a Server shall also use these specifications. The minimum hardware and software requirements to fulfill this installation are:
          1. Processor: Intel Core i3 - Desktop class machine.
          2. CPU: 3.3 GHz.
          3. RAM: 8 Gigabytes (GB) for standalone installation; 4 Gigabytes (GB) for workstations.
          4. Hard Disk: 120 GB SATA with minimum 60 GB free space; Workstations 80 GB with 5 GB free.
          5. Serial Communication Ports: As required by the application.
          6. Secondary Storage: Tape or DVD burner.
          7. Printer port: 1 (or network printer).
          8. Monitor Display: Size: 15 Inches SVGA, Resolution: 1024 x 768, Colors: 256.
          9. Pointing Device: Mouse (USB preferred).
          10. Power Supply: UPS.
          11. Operating System: Minimum 64-bit Microsoft Windows 10 Professional; Windows 8.1 Professional for workstations.
          12. Database: Microsoft SQL Server 2016 Express Edition.
       2. The ISS shall be installed on a computer that supports 1 to 100 readers, 5,000 cards, and 8 communication ports. The recommended hardware requirements to fulfill this installation are:
          1. Processor: Quad Core Intel Xeon.
          2. CPU: 2.4 GHz.
          3. RAM: 16 Gigabytes (GB).
          4. Hard Disk: 250 GB SATA or SCSI or SSD (60 GB free space).
          5. Serial Communication Ports: 2.
          6. Secondary Storage: Tape or DVD burner.
          7. Printer port: 1 (or network printer).
          8. Monitor Display: Size: 20 Inches, Resolution: 1600 x 900, Colors: True color.
          9. Pointing Device: Mouse (USB preferred).
          10. Power Supply: Hot-swap, redundant with UPS
          11. Operating System: Microsoft Windows 10 Professional (standalone system or Workstations); Windows Server 2012 R2 Standard when additional workstations and or communication servers are added also use for additional communication servers (PE/CS only).
          12. Database: Microsoft SQL Server 2016 Express Edition.
       3. The ISS shall be installed in a computer that supports that supports more than 100 readers, 100,000 cards and 255 communication ports, the maximum/performance hardware requirements to fulfill this installation begin with:
          1. Processor: Intel Quad Core Xeon Intel Quad Core Xeon - Server class computer
          2. CPU: 3.5 GHz or more
          3. RAM: 32 Gigabytes (GB)
          4. Hard Disk: 1 TB SATA 15000 RPM or SSD
          5. Serial Communication Ports: As per the requirement
          6. Secondary Storage: Tape or DVD burner
          7. Printer port: 1 (or network printer)
          8. Monitor Display: Size: 24 Inches, Resolution: 1920 x 1200, Colors: True color.
          9. Pointing Device: Mouse (USB preferred)
          10. Power Supply: Hot-swap, redundant with UPS
          11. Operating System: Microsoft Windows Server 2016
          12. Database: Microsoft SQL Server 2016 with processor/core license
    3. Hardware Requirements:
       1. Intelligent Controllers:
          1. Distributed Architecture: Allows controllers to operate independent of the host. The architecture places key access decisions, event/action processing, and alarm monitoring functions within the controllers, eliminating degraded mode operation.
          2. Flash Memory Management: Support firmware updates and revisions to be downloaded to the system. Upgrades to hardware and software are to occur seamlessly without loss of database, configurations, or historical report data.
          3. Manufacturers: Subject to compliance with requirements, provide Field Controllers or comparable product by one of the following:

Honeywell P-Series Controller (PRO-3200, PRO-4200, PW-6000 and PW-7000 controllers) PRO-3000 (APAC regional panel).

P Series Panel Capabilities:

Store 50,000 cards/key codes for PRO-4200.

Store 240,000 cards/key codes for PRO-4200.

Communication Formats: OSDP and WIEGAND

Four SIO Boards are included in the PRO-4200 panel. SIO boards enable extended input and output capabilities to the panel.

Readers, inputs, and outputs that can be connected to the panel are based on the type of SIO Board that is added to the panel.

SIO Board Types: From Honeywell Security.

Single Reader Module (SRM): PRO42R1.

Dual Reader Module (DRM): PRO42R2B.

Alarm Input Module (AIM): PRO42IN. 16 Inputs 2 Outputs.

Relay Output Module (ROM): PRO42OUT. 16 Outputs 2 Inputs.

MPA2 and MPA4 Panel Capabilities:

Panels are called Gateway panels when added directly to the communication server.

Supports the downstream devices feature. This feature extends the input and output capabilities of the Panels.

Supports OSDP and WIEGAND communication format.

MPA2 panels allow multiple sets of card numbers and site codes embedded in a card format. These multiple embedded sets are represented as A, B, C, and D sets of card numbers and site codes. The A set is the default / primary card and site code numbers. The resulting maximum card number length will be 64 bits (20-digit card number). This is why system defaults incorporate the ability to select a 20-digit card number size in addition to existing 5, 12 and 16 digits.

Supports 128 time slots and 255 holidays (per holiday group). Holidays: Definable in three different holiday types allowing for different operational time definitions for each holiday type.

Panels have a provision to add a new time zone while within the panel database.

After creating the new time zone, it will be added to the Time Zones database and applied to the panel's database.

Panel options such as Anti-Passback, Groups, Forgiveness, Continuous Card Reads, Reverse Read LEDs, Host Grant, Site Codes, and Command File can be set for providing access to the readers, input points, and output points attached to the MPA panels.

MPA2 panels allow configuring of 8 relay inputs with default values.

MPA2 panels support 2 readers with WIEGAND and 4 readers with OSDP.

MPA4 panels support 4 readers with WIEGANG and 8 readers with OSDP.

Honeywell NetAXS Controllers: NetAXS-123 and NetAXS-4 are the two types of NetAXS controllers. (Legacy support).

* + - 1. Field Hardware:
      2. NOTE TO SPECIFIER: Select the appropriate components and delete the others as necessary.
         1. The security management system is to be equipped with access control field hardware required to receive alarms and administer access granted/denied decisions. All field hardware shall meet UL requirements.
         2. Card Readers:

Proximity.

Biometric Readers: Idemia.

Biometric Readers: Suprema.

Magnetic Stripe.

Wiegand.

OSDP.

Barcode.

BLE.

* + 1. System Interfaces: For Security Management Systems.
       1. Digital Video Recording Systems:
          1. Provide fully integrated support for a powerful digital video recording and transmission system. The Security Management System shall record, search, and transmit video, and provide users with live, pre-and post-event assessment capabilities.

DVRs: To be seamlessly integrated with existing video equipment and incorporated into any TCP/IP network. Provide multiple levels of integration with the Security Management System software, providing control of the digital video system from the access control application.

* + - * 1. WIN-PAK shall support the following Digital Video Recorders (DVRs):

ADPRO.

MAXPRO NVR.

35 Series Recorders.

ENVR (Legacy).

NOTE TO SPECIFIER: Live video is streamed from all the supported cameras of these DVRs.

* + - 1. Intrusion Detection Panels:
         1. Honeywell VISTA-128FBPT, VISTA-250FBPT, VISTA -128BPT and VISTA-250BPT

General Requirements: Support hardwired and TCP/IP communication for the VISTA 128FBPT/VISTA-250 FBPT panel. Each panel shall have 8 partitions and 15 zone lists. Zones, partitions, and the top-level panel shall have an events page, with all supported events present.

Features:

Disarm and unlock a door on card swipe.

Arm and lock a door on card swipe.

Common area arm/disarm.

Access denied if intrusion system is in alarm or armed.

Monitor and log intrusion system events and alarms in the Security Management System.

Associate intrusion system events and alarms with video surveillance integrations.

* + - * 1. Honeywell Galaxy Dimension Controllers: GALAXY\_GD264, GALAXY\_GD\_48, GALAXY\_GD\_96 GALAXY\_GD\_520, Firmware 6.80 and above, Ethernet module firmware 2.08 and above controllers. Honeywell Galaxy Grade 3 Controllers: GALAXY\_144, GALAXY\_20, Firmware 5.04/5.50 and above, Ethernet module firmware 2.01 and above. Honeywell Classic Panel Controllers: GALAXY\_60, GALAXY\_128, GALAXY\_500, GALAXY\_504, GALAXY\_512, Firmware 4.50 and above, Ethernet module firmware 2.10 and above.

Security Management System users can control, and monitor Group and Zone status using the Security Management System client and control the individual zones and groups using Security Management System Access control credentials. Depending on the combined user profiles and access permissions defined in Security Management System, Security Management System cardholder is allowed or denied permission to arm/disarm zones and groups. The access control functionality of the intrusion panel is disabled when the integration is operational.

Features:

Disarm a zone on a card swipe.

Arm a zone on consecutive card swipes. Security Management System will support definition of quantity of swipes required and the timeout time in seconds to recognize consecutive swipes.

Security Management System supports linking intrusion panel users with Security Management System cardholders.

Security Management System operators may be given control permissions for intrusion input and output alarms.

Security Management System can associate alarm events with video commands to look at current or historic footage.

Security Management System stores and reports on intrusion events.

* 1. WEB BASED MODULAR ACCESS CONTROL SYSTEM
     1. System: MAXPRO Access (MPA) MPA2/4 Modular Access Control System manufactured by Honeywell Commercial Security.

\*\* NOTE TO SPECIFIER \*\* Delete model options not required.

* + - 1. MPA2C3: 2 Door Control Panel (No Enclosure).
      2. MPA2MPSU: 2 Door Control Panel with Enclosure, Battery, and Power Supply.
      3. MPA2C3-4: 4 Door Control Panel (No Enclosure).
      4. MPA4MPSU: 4 Door Control Panel with Enclosure, Battery, and Power Supply.
    1. The access control system shall function as a web-based open architecture facility management system that tracks individuals, defines, and controls access levels, monitors alarms, and generates reports. The system is capable of configuring alarms and incorporating scheduled events that may be activated by either time or a specific programmed event. Access is controlled through a password-protected user interface. Operators communicate with the system through a host software system or by connecting to the web server through an Ethernet connection.
       1. System Control Panels: Fully upgradeable using flash memory firmware.
       2. When MPA panels are connected to MAXPRO Cloud, it is possible to download firmware updates directly from the Cloud.
    2. System Architecture:
       1. Access Control and Alarm Monitoring System: Flexible single-user, open-architecture facility management system. Reliable state-of-the-art technology allows for easy and economical expansion. The scalable design allows for operation from an embedded Web-based server without a dedicated server or PC workstation. The panel is capable of operating in a hosted mode with WIN-PAK XE/SE/PE/CS access control software.
       2. Embedded Linux software intelligently controls the reader network providing automated data collection and configuration updates, facilitating seamless operation from controllers. Control panels utilize off-line distributed processing concepts including inter-controller communication if upgraded.
       3. Built-in communications options using Ethernet, RS-485 and USB-C for direct WEB mode, which requires USB driver for PC.
    3. System Software Suite:
       1. Comprises various integrated software modules that allow for the full integration and retrieval of transactions from the hardware, as well as alarm monitoring, reporting, and scheduling capabilities.
          1. Software Modules: Editing of personnel, access levels, system configuration and reporting is controlled by a password protected user interface. System operation for individual operators is possible using assigned passwords only.
       2. Users to have the ability to perform hardware configuration changes during or after installation which include functions such as door open time, door contact time, location and reader names, and access rights configuration.
       3. The system includes a Bluetooth based wireless communication to a dedicated application for iPhone and/or Android by which initial configuration can be accomplished.
       4. System software supports configuration of alarms triggering the system.
       5. System incorporates scheduled events activated by either time or a specific programmed event, therefore being time or event triggered.
       6. Access Control Functions: Include validation based on time of day, day of week, holiday scheduling, and access validation based on positive verification of card or card + PIN (Personal Identification Number).
       7. Zone-related Software Features:
          1. Supervisor card unlock.
       8. Card-related Software Management:
          1. Time-limited access.
          2. PIN codes.
          3. Suspension of cards.
          4. Multiple card access.
          5. Card access groups.
          6. Time patterns (schedules).
          7. Anti-pass back (APB) control.
          8. Reporting.
          9. First Card Rule (Activates the door time zone).
          10. Two Card Rule-Supervisor card and regular card to allow access.
          11. Time zone card toggle for door locks.
          12. Latching mode for door locks.
          13. Enhanced support for elevator control for buildings up to 8 floors.
    4. Hardware:
       1. Quantities of Components: Determined and installed by the Contractor based on the requirement to provide a fully operational integrated access control system as per the design intent.
       2. Communication Between Components: Ethernet with legacy support for RS-485.
       3. Terminals and Controllers: Allow for direct Firmware upgrade via network connection.
          1. Units are upgradeable during normal system operation.
          2. Should one unit be in upgrade mode, other units continue to operate normally.
          3. Firmware is stored in FLASH memory on the individual units.
       4. System Controller: Honeywell MPA2 or MPA4 door controller.
          1. Each Controller Loop: Capable of 16 panels or 64 readers.
          2. Standard Controller Configuration: Supports 100,000 card and event capacity.
       5. Door Control: Terminals and remote readers supported by the controller shall be any combination of the following: card only, card and pin, card or pin, pin only, lockdown, disabled, supervisor, escort, limited use card, expire on date, first card rule, snow day rule, time zone toggle and Anti-Passback with local/global capability and hard and soft implementation.
       6. Inputs: Provides 16 (+8) Configurable four-state supervised input points Factory default settings: Status, REX, Reader Tamper A, Reader Tamper B and 8 Auxiliary inputs.
       7. FACP (Fire) Input: One supervised normally open contact or reversed polarity triggered Fire input forces all 4 door outputs in fail-safe state, releasing fail-safe locking devices and unlocking all connected doors for escape/evacuation purposes.
          1. Hardware solution overrides any software or controlled setting.
          2. When controller is used in WIN-PAK host system, set up system to automatically disable power to any maglocks in case of fire alarm trigger.
       8. Outputs: 4 SPDT (jumper selectable NO or NC contact) output Rated 3 A at 30 Vdc per push in terminal block Rated 500 mA at 30 Vdc per RJ45 Rated 500 mA at 12Vdc per RJ45 and limited at 750 mA at 12 Vdc per 2 RJ45 (Self-powered from panel).
       9. Cards and Database: Card and event buffer capacity to be 10,000 card capacity and 25,000 event capacity. The firmware revision shall have on-board flash memory for field firmware revisions and feature expansion. Offline database backup will be available. Export capabilities for card database, alarms, and events. The panel shall support 128 unique card formats and 8 site codes. The maximum card format size shall be 75 bit suitable for handling the card format of PIV, TWIC, and FRAC cards. The time zones support will be a minimum of 127 with 128 access levels and 255 holidays.
       10. Reports and Analysis: Capable of integrated reports, import/export of card database and alarms and events can be exported and saved in offline storage.
       11. Embedded Web Server: Supported browsers include Google Chrome. The web browser control will allow full control monitor, view live events, and manually control doors and readers. Secure web browsing to have TLS1.2 encryption.
       12. System Information: Support Global Geographic Time Zone support and Daylight-Saving Time support.
       13. System to be EMC/CE and FCC compliant with UL-294 listing.
       14. System Testing: Contractor will demonstrate the system functionality upon completion of installation, document test results, and provide results to the Customer.
       15. Warranty: Equipment and systems to be guaranteed by the Contractor for a period of one year commencing with the filing date of the Notice of Completion, provided the system has been inspected and signed off by the Owner. The guarantee shall cover all costs for Warranty Service, including parts, labor, prompt field service, pick-up, transportation, and delivery.
    5. The MPA2MPSU and MPA4MPSU Door access Controllers shall have the following mechanical specifications:
       1. Unit Dimensions: 14.1 inch (360 mm) h x 16.1 inch (410 mm) x 4.3 inch (110 mm) Ethernet Connector: RJ45.
       2. Enclosure Type: Metal.
       3. Wiring Access Holes: 25.
    6. The MPA2MPSU and MPA4MPSU access door controllers shall have the following electrical specifications:
       1. Voltage: 10 to 19 VDC, Typical 13.8 VDC (standard power supply from metal enclosure).
       2. Power over Ethernet 802.3af.
    7. The MPA2MPSU and MPA4MPSU Door Access System shall be designed to meet the following environmental conditions:
       1. Operating Temperature: 14 to 113 degrees F (-10 to 45 degrees C)
       2. Emissions: EMC/CE, FCC compliant, UL 294.
       3. NOTE TO SPECIFIER: Delete if not required.
  1. ACCESS CONTROL READERS (Data security with OmniClass cards.)
     1. Contactless Smart Card Readers: Single-package type; combining electronics and antenna in one package in the following configurations:
        1. Surface Mounting Style: 13.56 MHz or 13.56 MHz and 125 kHz prox contactless smart card readers suitable for minimal space mounting configurations as shown on the project plans.
        2. Comply with ISO 15693, ISO 14443A (CSN), and ISO 14443B and read credentials complying with these standards.
        3. Output credential data must comply with the SIA AC-01 Wiegand standard as follows:
           1. Reads standard proximity format data from OmniClass cards and outputs data as encoded.
           2. Reads card serial number (CSN) of a MIFARE or DESFIRE card with configurable outputs as 26-bit, 32-bit, 34-bit, 40-bit, or 56-bit.
        4. Data Security with OmniClass Cards: Use up to 128-bit authentication keys to reduce the risk of compromised data or duplicate cards. The contactless smart card reader and OmniClass cards shall require matching keys in order to function together.
           1. RF data transmission between cards and readers to be encrypted, using a secure algorithm. Provide card readers with keys compatible with the OmniClass cards.
        5. Reader to be of potted, polycarbonate material, sealed to a NEMA rating of 4X (IP65).
        6. Provide the ability to change operational features in the field using a factory-programmed command card. Additionally, firmware may be updated by flashing the reader. Command card operational programming options shall include:
           1. Output configurations.
           2. LED and Audio configurations.
           3. Keypad configurations.
        7. Provide the Following Programmable Audio/Visual Indication:
           1. An Audio Transducer: Provides various tone sequences to signify access granted, access denied, power up, and diagnostics.
           2. A High-Intensity Light Bar: Provides clear visual status (red/green/amber) that is visible even in bright sunlight.
        8. Certifications, Meet the Following:
           1. UL 294.
           2. Canada/UL 294.
           3. FCC Certification.
           4. Canada Radio Certification.
           5. EU and CB Scheme Electrical Safety.
           6. EU - R and TTE Directive.
           7. CE Mark (Europe).
           8. IP55 Rated.
           9. C-Tick (New Zealand/Australia/Taiwan).
        9. Meet the Following Environmental Specifications:
           1. Operating Temperature: -30 to 150 degrees F (-35 to 65 degrees C).
           2. Operating Humidity: 5 to 95 percent relative humidity non-condensing.
           3. Weatherized design suitable to withstand harsh environments.
        10. Cabling Requirements:
            1. Manufacturer: Honeywell Cable
            2. Cable distance (Wiegand): 500 feet (150 m)
            3. Cable distance (OSDP): 1,640 feet (500 m)
            4. Cable type: 6-conductor No. 22 AWG minimum with overall foil shield and drain wire.
            5. Standard reader termination: 18 inches (.5 m) cable pigtail.
        11. Warranty: Lifetime against defects in materials and workmanship.
     2. Product: OS20TOSDP Mullion 13.56 MHz Contactless Smart and 125 kHz Prox Card Readers as manufactured by the Honeywell Commercial Security:
        1. Typical Read Range:
           1. Seos, MIFARE Classic, MIFARE DESFire EV1/EV2/EV3 and ISO14443A Single Technology Cards: 1.6 to 4 inches (4 to 10 cm)
           2. HID / AWID Proximity, Indala Proximity, EM Proximity, and 125 kHz Single Technology Cards: 2.4 to 4 inches (6 to 10 cm)
        2. Meet the Following Physical Specifications:
           1. Dimensions: 1.77 x 4.78 x 0.77 inches (45 x 121.5 x 19.5 mm).
           2. Weight: 3.35 oz (95 g).
           3. Material: UL94 Polycarbonate.
           4. Two-part design with separate mounting plate and reader body.
           5. Color: Black.
        3. Meet the Following Electrical Specifications:
           1. Operating Voltage: 12 VDC
           2. Current Requirements: NSC4: 60 mA Peak: 250 mA Max. Avg: 70 mA IPM5: 45 mA.
     3. Product: OS20KTOSDP 13.56 MHz Contactless Smart and 125 kHz Prox Card W/ Keypad Readers as manufactured by the Honeywell Commercial Security:
        1. Typical Read Range:
           1. Seos, MIFARE Classic, MIFARE DESFire EV1/EV2/EV3 and ISO14443A Single Technology Cards: 1.6 to 4 inches (4 to 10 cm)
           2. HID / AWID Proximity, Indala Proximity, EM Proximity, and 125 kHz Single Technology Cards: 2.4 to 4 inches (6 to 10 cm)
        2. Meet the Following Physical Specifications:
           1. Dimensions: 1.78 x 4.79 x .85 inches (45 x 121.5x 21.5mm).
           2. Weight: 3.88 oz (110 g).
           3. Material: UL94 Polycarbonate.
           4. Two-part design with separate mounting plate and reader body.
           5. Color: Black.
        3. Meet the Following Electrical Specifications:
           1. Operating Voltage: 12 VDC
           2. Current Requirements: NSC4: 65 mA Peak: 250 mA Max. Avg: 75 mA IPM5: 48 mA.
     4. Product: OS40TOSDP US Single-Gang 13.56 MHz Contactless Smart and 125 kHz Prox Card Readers as manufactured by the Honeywell Commercial Security:
        1. Typical Read Range:
           1. Seos, MIFARE Classic, MIFARE DESFire EV1/EV2/EV3 and ISO14443A Single Technology Cards: 1.6 to 4 inches (4 to 10 cm)
           2. HID / AWID Proximity, Indala Proximity, EM Proximity, and 125 kHz Single Technology Cards: 2.4 to 4 in (6 to 10 cm)
        2. Meet the Following Physical Specifications:
           1. Dimensions: 3.30 x 4.80 x 0.85 inches (8.38 x 12.19 x 2.16 cm).
           2. Weight: 8.8 oz (249.5 g).
           3. Material: UL94 Polycarbonate.
           4. Two-part design with separate mounting plate and reader body.
           5. Color: Black.
        3. Meet the Following Electrical Specifications:
           1. Operating Voltage: 12 VDC.
           2. Current Requirements: NSC4: 65 mA Peak: 250 mA Max. Avg: 75 mA IPM5: 45 mA.
     5. Product: OS40KTOSDP 13.56 MHz Contactless Smart and 125 kHz Prox Card W/ Keypad Readers as manufactured by the Honeywell Commercial Security:
        1. Typical Read Range:
           1. Seos, MIFARE Classic, MIFARE DESFire EV1/EV2/EV3 and ISO14443A Single Technology Cards: 1.6 to 4 inches (4 to 10 cm)
           2. HID / AWID Proximity, Indala Proximity, EM Proximity, and 125 kHz Single Technology Cards: 2.4 to 4 in (6 to 10 cm)
        2. Meet the Following Physical Specifications:
           1. Dimensions: 3.30 x 4.80 x 0.90 inches (8.38 x 12.19 x 2.28 cm).
           2. Weight: 10 oz (283.4 g).
           3. Material: UL94 Polycarbonate.
           4. Two-part design with separate mounting plate and reader body.
           5. Color: Black.
        3. Meet the Following Electrical Specifications:
           1. Operating voltage: 12 VDC
           2. Current requirements: NSC4: 70 mA Peak: 250 mA Max. Avg: 80 mA IPM5: 55 mA
     6. Product: OS20TT2OSDP Mullion 13.56 MHz Contactless Smart Card Readers as manufactured by the Honeywell Commercial Security:
        1. Typical Read Range:
           1. Seos, MIFARE Classic, MIFARE DESFire EV1/EV2/EV3 and ISO14443A Single Technology Cards: 1.6 to 4 inches (4 to 10 cm)
        2. Meet the Following Physical Specifications:
           1. Dimensions: 1.77 x 4.78 x 0.77 inches (45 x 121.5 x 19.5 mm).
           2. Weight: 2.65 oz (75 g).
           3. Material: UL94 Polycarbonate.
           4. Two-part design with separate mounting plate and reader body.
           5. Color: Black.
        3. Meet the Following Electrical Specifications:
           1. Operating Voltage: 12 VDC.
           2. Current Requirements: NSC4: 60 mA Peak: 250 mA Max. Avg: 70 mA IPM5: 45 mA.
     7. Product: OS20KTT2OSDP Mullion 13.56 MHz Contactless Smart Card Readers as manufactured by the Honeywell Commercial Security:
        1. Typical Read Range:
           1. Seos, MIFARE Classic, MIFARE DESFire EV1/EV2/EV3 and ISO14443A Single Technology Cards: 1.6 to 4 inches (4 to 10 cm).
        2. Meet the Following Physical Specifications:
           1. Dimensions: 1.78 x 4.79 x .85 inches (45 x 121.5x 21.5 mm).
           2. Weight: 3.17 oz (90 g).
           3. Material: UL94 Polycarbonate.
           4. Two-part design with separate mounting plate and reader body.
           5. Color: Black.
        3. Meet the Following Electrical Specifications:
           1. Operating Voltage: 12 VDC.
           2. Current Requirements: NSC4: 65 mA Peak: 250 mA Max. Avg: 75 mA IPM5: 48 mA.
     8. Product: OS40TT2OSDP US Single-Gang 13.56 MHz Contactless Smart Card Readers as manufactured by the Honeywell Commercial Security:
        1. Typical Read Range:
        2. Seos, MIFARE Classic, MIFARE DESFire EV1/EV2/EV3 and ISO14443A Single Technology Cards: 1.6 to 4 inches (4 to 10 cm)
        3. Meet the Following Physical Specifications:
           1. Dimensions: 3.30 x 4.80 x 0.85 inches (8.38 x 12.19 x 2.16 cm).
           2. Weight: 8.8 oz (249.5 g).
           3. Material: UL94 Polycarbonate.
           4. Two-part design with separate mounting plate and reader body.
           5. Color: Black.
        4. Meet the Following Electrical Specifications:
           1. Operating Voltage: 12 VDC.
           2. Current Requirements: NSC4: 65 mA Peak: 250 mA Max. Avg: 75 mA IPM5: 45 mA.
     9. Product: OS40KTT2OSDP 13.56 MHz Contactless Smart Card with Keypad Readers as manufactured by the Honeywell Commercial Security:
        1. Typical Read Range:
           1. Seos, MIFARE Classic, MIFARE DESFire EV1/EV2/EV3 and ISO14443A Single Technology Cards: 1.6 to 4 inches (4 to 10 cm).
        2. Meet the Following Physical Specifications:
           1. Dimensions: 3.30 x 4.80 x .90 inches (8.38 x 12.19 x 2.28 cm).
           2. Weight: 10 oz (283.4 g).
           3. Material: UL94 Polycarbonate.
           4. Two-part design with separate mounting plate and reader body.
           5. Color: Black.
        3. Meet the Following Electrical Specifications:
           1. Operating voltage: 12 VDC.
           2. Current requirements: NSC4: 70 mA Peak: 250 mA Max. Avg: 80 mA IPM5: 55 mA.
     10. Contactless Proximity Card Readers: Single-package type, combining electronics and antenna in one package in the following configurations:
         1. Style: Surface Mounting: 125 kHz contactless proximity card readers suitable for minimal space mounting configurations as shown on the project plans.
         2. Output credential data in compliance with the SIA AC-01 Wiegand standard:
            1. Reads standard proximity format data from OmniProx cards and outputs data in Wiegand format.
            2. Reads card number with formats up 84 bits.
         3. Material: Potted, polycarbonate, sealed to a NEMA rating of 4X (IP65).
         4. Ability to field change operational features using a factory-programmed command card. Firmware may be updated by flashing the reader. Operational Programming Options shall Include:
            1. Output configurations.
            2. LED and Audio configurations.
            3. Keypad configurations.
         5. Provide the following programmable audio/visual indication:
            1. An Audio Transducer: Provide various tone sequences to signify access granted, access denied, power up, and diagnostics.
            2. A High-Intensity Light Bar: Provide clear visual status (red/green/amber) visible even in bright sunlight.
         6. Meet the Following Certifications:
            1. UL 294.
            2. Canada/UL 294.
            3. FCC Certification.
            4. ROHS compliant
            5. Canada Radio Certification.
            6. CE Mark (Europe).
         7. Meet the Following Environmental Specifications:
            1. Operating Temperature: -25 to 145 degrees F (-31 to 63 degrees C).
            2. Operating Humidity: 0 to 95 percent relative humidity non-condensing.
            3. Weatherized design suitable to withstand harsh environments.
         8. Cabling Requirements:
            1. Manufacturer: Honeywell Cable.
            2. Cable Distance: (Wiegand): 500 feet (150 m).
            3. Cable Type: 6-conductor No. 22 AWG minimum with overall foil shield and drain wire.
            4. Standard Reader Termination: 18 inches (.5 m) cable pigtail.
         9. Warranty: Lifetime against defects in materials and workmanship.
     11. Product: OP10 Mini-Mullion 125 kHz Contactless Proximity Card Readers as manufactured by the Honeywell Commercial Security:
         1. Typical Read Range:
            1. 1.5 to 4 inches (3.8 to 10.2 cm) using OmniProx card.
         2. Meet the Following Electrical Specifications:
            1. Operating voltage: 5.0 to 16 VDC, reverse voltage protected. Linear power supply recommended.
            2. Current requirements: 60/120 mA at 12 VDC.
         3. Meet the Following Physical Specifications:
            1. Dimensions: 3.15 x 1.57 x 0.50 inches (80 x 40 x 12.8 cm).
            2. Material: UL94 Polycarbonate.
            3. Two-part design with separate reader body and cover.
            4. Color: Black, charcoal gray and ivory interchangeable bezels.
         4. Contactless Card Reader: Honeywell OP10 compatible with selected card media.
         5. NOTE TO SPECIFIER: Delete product not required.
     12. Product: OP30 Mullion 125 kHz Contactless Proximity Card Readers as manufactured by the Honeywell Commercial Security:
         1. Typical Read Range:
            1. 1.5 to 4 inches (3.8 to 10.2 cm) using OmniProx card.
         2. Meet the Following Electrical Specifications:
            1. Operating voltage: 5.0 to 16 VDC, reverse voltage protected. Linear power supply recommended.
            2. Current requirements: 60/120 mA at 12 VDC.
         3. Meet the Following Physical Specifications:
            1. Dimensions: 5.71 x 1.69 x 0.79 inches (145 x 43 x 20 cm).
            2. Material: UL94 Polycarbonate.
            3. Two-part design with separate reader body and cover.
            4. Color: Black, charcoal gray and ivory interchangeable bezels.
         4. Contactless Card Reader: Honeywell OP30 compatible with selected card media.
     13. Product: OP40 Single-Gang (US) 125 kHz Contactless Proximity Card Readers as manufactured by the Honeywell Commercial Security:
         1. Typical Read Range:
            1. 1.5 to 4 inches (3.8 to 10.2 cm) using OmniProx card.
         2. Meet the Following Electrical Specifications:
            1. Operating voltage: 5.0 to 16 VDC, reverse voltage protected. Linear power supply recommended.
            2. Current requirements: 60/120 mA at 12 VDC.
         3. Meet the Following Physical Specifications:
            1. Dimensions: 4.33 x 2.95 x 0.59 inches (110 x 75 x 15 cm).
            2. Material: UL94 Polycarbonate.
            3. Two-part design with separate reader body and cover.
            4. Color: Black, charcoal gray and ivory interchangeable bezels.
         4. Contactless Card Reader: Honeywell OP40 compatible with selected card media.
     14. Product: OP45 Single-Gang (EU/APAC) 125 kHz Contactless Proximity Card Readers as manufactured by the Honeywell Commercial Security:
         1. Typical Read Range:
            1. 1.5 to 4 inches (3.8 to 10.2 cm) using OmniProx card.
         2. Meet the Following Electrical Specifications:
            1. Operating voltage: 5.0 to 16 VDC, reverse voltage protected. Linear power supply recommended.
            2. Current requirements: 60/120 mA at 12 VDC.
         3. Meet the Following Physical Specifications:
            1. Dimensions: 3.5 x 3.5 x 0.595 inches (88.9 x 88.9 x 15 cm).
            2. Material: UL94 Polycarbonate.
            3. Two-part design with separate reader body and cover.
            4. Color: Black, charcoal gray and ivory interchangeable bezels.
         4. Contactless Card Reader: Honeywell OP45 compatible with selected card media.
     15. Product: OP90 Single-Gang (US) 125 kHz Contactless Proximity Card Vandal Resistant Readers as manufactured by the Honeywell Commercial Security:
         1. Typical Read Range:
            1. 1.5 to 4 inches (3.8 to 10.2 cm) using OmniProx card.
         2. Meet the Following Electrical Specifications:
            1. Operating voltage: 5.0 to 16 VDC, reverse voltage protected. Linear power supply recommended.
            2. Current requirements: 60/120 mA at 12 VDC.
         3. Meet the Following Physical Specifications:
            1. Dimensions: 4.5 x 3.15 x 0.59 inches (114 x 80 x 15 cm).
            2. Material: UL94 Polycarbonate.
            3. Two-part design with reader body and cover.
            4. Color: Silver.
         4. Contactless Card Reader: Honeywell OP90 compatible with selected card media.
     16. Product: OP95 Single-Gang (US) 125 kHz Contactless Proximity Card Vandal Resistant Readers + Keypad as manufactured by the Honeywell Commercial Security:
         1. Typical Read Range:
            1. 1.5 to 4 inches (3.8 to 10.2 cm) using OmniProx card.
         2. Meet the Following Electrical Specifications:
            1. Operating voltage: 5.0 to 16 VDC, reverse voltage protected. Linear power supply recommended.
            2. Current requirements: 60/120 mA at 12 VDC.
         3. Meet the Following Physical Specifications:
            1. Dimensions: 4.5 x 3.15 x 0.59 inches (114 x 80 x 15 cm).
            2. Material: UL94 Polycarbonate.
            3. Two-part design with separate reader body and cover.
            4. Color: Silver.
         4. Contactless Card Reader: Honeywell OP95 compatible with selected card media.
         5. NOTE TO SPECIFIER: Delete article if not required.
  2. ACCESS CONTROL CREDENTIALS
     1. Access cards shall be used with access readers to gain entry to access controlled portals (e.g.; doors, gates, turnstiles) and to hold information specific to the user and shall be Contactless Smart Card or Contactless Proximity Card technology credentials.
     2. Contactless Smart Cards
     3. NOTE TO SPECIFIER: Delete if not required.
        1. Single Technology Access Cards:
           1. Meet these contactless smart card standards: ISO 15693 and ISO 14443B2.
           2. Meet ISO 7810 specifications for length, width, thickness, flatness, card construction and durability.
           3. Be in a form suitable for direct two-sided dye-sublimation or thermal transfer printing on the specified badge printer.
           4. Presentation to the access control reader at any angle within a minimum of one inch (25 mm) shall result in an accurate reading of the card.
           5. Unique 64-bit, fixed card serial number, used for anti-collision and key diversification.
           6. Support capability, with a minimum of 2 Kbits (256 bytes) of EEPROM memory or 16 Kbits (2048 bytes) of EEPROM memory. The 2 Kbit card shall have a minimum of 2 Application Areas, and the 16Kbit shall have either 2 or 16 Application Areas to support future applications. Data retention shall be 10 years, nominal. Wiegand card data up to 84 bits in length shall be factory programmed in Application Area 1 for use with access control systems.
           7. Each Application Area on the cards shall be secured with up to a 128-bit unique, diversified security key, such that data stored in that area cannot be accessed or modified until the card and reader have completed a mutual authentication process.
           8. Capable of completing any write operation, even if cards are removed from the RF field during that operation.
           9. Warranted against defects in materials and workmanship for two years.

If Multiple Technologies are Used:

With a Magnetic Stripe: Card to have a fifteen-month warranty.

With a Contact Chip: Card to have a one-year warranty.

* + - * 1. Provide "smart" access cards, compatible with the specified card readers. Cards shall be factory encoded with Wiegand card data.
        2. Must not carry identification showing the property location unless otherwise specified herein.
        3. Capable of accepting a slot punch on one end, allowing it to be hung from a strap/clip in a vertical orientation.
        4. NOTE TO SPECIFIER: Delete if not required.
      1. Multiple Technology Access Card:
         1. Support 13.56 MHz OmniClass contactless smart chip and antenna plus any or all the following technologies, simultaneously:

125 kHz HID Proximity chip and antenna.

Magnetic Stripe.

Embedded Contact Smart Chip Module.

* + - * 1. To be available with a 13.56 MHz OmniClass contactless smart chip and antenna plus a Wiegand Strip with an optional magnetic stripe, meeting all ISO 7810 standards except for card thickness, which shall be 0.037 inch (0.939 mm). The card will not be available with 125 kHz proximity technology and/or an embedded contact smart chip module.
        2. NOTE TO SPECIFIER: Delete if not required.
      1. Access Key Fob:
         1. Meet these contactless smart card standards: ISO 15693 and ISO 14443B2.
         2. Durable injection molded polycarbonate plastic, with slot molded into one end, and suitable for placement on a key ring.
         3. Presentation to the access control reader at any angle within one inch (25 mm) shall result in an accurate key fob reading.
         4. Compatible with the specified card readers.
         5. Must not carry identification showing the property location unless otherwise specified herein.
         6. Warranted against defects in materials and workmanship for two years.
         7. NOTE TO SPECIFIER: Delete if not required.
      2. Access Stickers:
         1. Meet these contactless smart card standards: ISO 15693 and ISO 14443B2.
         2. Flat disc-shaped with a polycarbonate cover and a self-stick adhesive back.
         3. Capable of affixation to non-metallic personal items such as PDAs, cell phones, business assets, or existing access control or identification cards to transition from earlier technologies to contactless smart cards.
         4. Not to be used with tractor-feed (full insertion) readers.
         5. Presentation to the access control reader at any angle within one inch (25 mm) shall result in an accurate Sticker reading.
         6. Warranted against defects in materials and workmanship for two years.
         7. Compatible with the specified card readers.
         8. Must not carry identification showing the property location unless otherwise specified herein.
    1. Contactless Proximity Cards:
       1. Meet the following standards for contactless proximity cards:
          1. Proximity Chip and Antenna: 125 kHz HID.
          2. ISO 7810 specifications for length, width, thickness, flatness, card construction and durability. Must be in a form suitable for direct two-sided dye-sublimation or thermal transfer printing on the specified badge printer.
          3. Presentation to the access control reader at any angle within a minimum of one inch (25 mm) shall result in an accurate reading of the card.
          4. Capable of completing any write operation, even if the card is removed from the RF field during that operation.
          5. Warranted against defects in materials and workmanship for two years.

If Multiple Technologies are Used: Magnetic stripe cards shall have a fifteen-month warranty.

* + - * 1. "Smart" access cards, compatible with the specified card readers.
        2. Factory encoded with Wiegand card data, in 26-bit or 34-bit formats.
        3. Must not carry any identification showing the property location unless otherwise specified herein.
        4. Capable of accepting a slot punch on one end, allowing it to be hung from a strap/clip in a vertical orientation.

1. EXECUTION
   1. EXAMINATION
      1. Examine site conditions to determine site conditions are acceptable without qualifications. Notify Owner in writing if deficiencies are found. Starting work is evidence that site conditions are acceptable.
   2. PREPARATION
      1. Clean surfaces thoroughly prior to installation.
      2. Prepare surfaces using the methods recommended by the manufacturer for achieving the best result for the substrate under the project conditions.
   3. INSTALLATION
      1. System, including but not limited to access control, alarm monitoring and reporting, time management, and user identification cards shall be installed in accordance with the manufacturer's installation instructions.
      2. Supervise installation to appraise ongoing progress of other trades and contracts, make allowances for all ongoing work, and coordinate the System installation requirements.
   4. FIELD TESTING AND CERTIFICATION
      1. Testing: The control, alarm monitoring and reporting, time management, and user identification cards shall be tested in accordance with the following:
         1. Conduct a complete inspection and test of all installed access control and security monitoring equipment. This includes testing and verifying connection to equipment of other divisions such as life safety and elevators.
         2. Provide staff to test all devices and all operational features of the System for witness by the Owner's representative and authorities having jurisdiction as applicable.
         3. Correct deficiencies until satisfactory results are obtained.
         4. Submit written copies of test results.
   5. PROTECTION
      1. Protect installed products until completion of project.
      2. Touch-up, repair or replace damaged products before Substantial Completion.

END OF SECTION