SECTION 28 10 00

PRO-WATCH INTEGRATED SECURITY

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(13700hsg):%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'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. Access and security management system. (Pro-Watch)
    2. Visitor management system. (Pro-Watch Visitor Management)
    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. SECURITY MANAGEMENT SYSTEM DESCRIPTION

\*\* NOTE TO SPECIFIER \*\* Delete paragraph below if Pro-Watch not required for project.

* + 1. Pro-Watch: The Security Management System shall function as an electronic access control system and shall integrate alarm monitoring, CCTV, digital video, ID badging and database management into a single platform. A modular and network-enabled architecture shall allow maximum versatility for tailoring secure and dependable access and alarm monitoring solutions.
    2. FIPS Certification: The system shall support FIPS 201 certification.
  1. 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.
  2. QUALITY ASSURANCE
     1. Manufacturer: Minimum ten years' experience in manufacturing and maintaining Security Management Systems. The manufacturer shall be Microsoft Silver Certified.
     2. Installer must be certified by Honeywell Integrated Security Dealer Service Certification Program (DSCP).
  3. DELIVERY, STORAGE, AND HANDLING
     1. Deliver materials in manufacturer's labeled packages. Store and handle in accordance with the manufacturer's requirements.
  4. 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.
  5. 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(13700hsg):%20%20&mf=); Web: <https://buildings.honeywell.com/us/en/brands/our-brands/security>

\*\* NOTE TO SPECIFIER \*\* Delete one of the following two paragraphs; coordinate with requirements of Division 1 section on product options and substitutions.

* + 1. Substitutions: Not permitted.
    2. Requests for substitutions will be considered in accordance with the provisions of Section 01 60 00.
  1. ACCESS AND SECURITY MANAGEMENT SYSTEM (PRO-WATCH)
     1. Basis of Design: Pro-Watch Security Management System Suite as manufactured by Honeywell Commercial Security.
        1. Function as an electronic access control system and integrates alarm monitoring, CCTV, digital and network video, ID badging and database management into a single platform. A modular and network-enabled architecture allows maximum versatility for tailoring secure and dependable access and alarm monitoring solutions.

\*\* NOTE TO SPECIFIER \*\* Access Control Security Management Software Suite: Offers a complete access control solution alarm monitoring, video imaging, ID badging and video surveillance control.

* + - 1. Available in Four Scalable Editions:
         1. Pro-Watch Lite Edition: Utilizes the Microsoft SQL Express database for applications with one to four users and up to 32 controlled doors.
         2. Pro-Watch Professional Edition: Utilizes Microsoft SQL Express database for applications from one to five users and up to 64 controlled doors. Provides a set of tools to easily backup, restore and maintain the Database. Allows expansion to Corporate and/or Enterprise Edition without changing the user interface or database structure.
         3. Pro-Watch Corporate Edition: Utilizes Microsoft SQL Server database for applications from unlimited users and up to 20,000 controlled doors. Provides a set of tools to easily backup, restore and maintain the database. Allows for expansion Enterprise Edition without changing the user interface or database structure.
         4. Pro-Watch Enterprise Edition: Incorporate regional server architecture. Regional sites operate autonomously with all information required to maintain security locally. The enterprise server maintains any critical system information via synchronization with each regional site. A single enterprise server provides global management of all regional servers and acts as a central collecting point for all hardware configurations, cardholder and clearance code data and transaction history.

\*\* NOTE TO SPECIFIER \*\* Delete one of the two following paragraph options not required. If keeping the second option, delete the edition not required.

* + - 1. The contractor is to determine which edition best suites the application.
      2. Security Management Software for Project.
         1. Edition: Pro-Watch Lite.
         2. Edition: Pro-Watch Professional.
         3. Edition: Pro-Watch Corporate.
         4. Edition: Pro-Watch Enterprise.
    1. Software Requirements: The Security Management System; a modular and network-enabled access control system capable of controlling multiple remote sites with alarm monitoring, ID badging, video integration, and intercom and allowing for easy expansion or modification of inputs via remote monitoring stations. The System to be controlled at a central computer location under the control of a single software program and provide full integration of all components. It is to be alterable at any time depending upon facility requirements. Reconfiguration may be accomplished online through system programming.
       1. Multi-User/Network Capabilities: Support multiple operator workstations via local area network/wide area network (LAN/WAN).
          1. Communications Between the Workstations: The server computer utilizes the TCP/IP standard over industry standard IEEE 802.3 (Ethernet).
          2. Supervised communications between the server and workstations, automatically generate alarm notifications when the server is unable to communicate with a workstation.
          3. Network server operators have the capability to log on to workstations and remotely configure devices for the workstation.
          4. Standard operator permission levels shall be enforced with a full operator audit.
       2. Concurrent Licensing: Provides the ability for any client workstation to connect to the database server as long as the maximum number of concurrent connections purchased has not been exceeded.
       3. Terminal Services: Supports Windows Server Terminal Services.
          1. The Security Management System server application may reside on the Windows Terminal Server. Operating systems supporting a standard web browser must be capable of utilizing the thin client architecture.
          2. Unlimited connections, based on concurrent licensing to the Software. Obtain full functionality through the intranet connection allowing full administration and monitoring without needing a local installation.
       4. Relational Database Management System: Supports industry standard relational database management systems. This includes Microsoft SQL Server 2016 SP1, 2017 and 2019.
       5. Database Partitioning: Provides option to restrict access to sensitive information by user ID.
       6. Memory: Proprietary software programs and control logic information used to coordinate and drive system hardware are to be stored in read-only memory.
       7. LDAP/ Microsoft Active Directory Services: Support of Lightweight Directory Access Protocol (LDAP) for enabling users to locate organizations, individuals, and other resources such as files and devices in a network, whether on the public internet or on a private intranet.
          1. Provide a direct link to Microsoft Active Directory Services. Allow transfer of Active Directory users into the database via the Data Transfer Utility.
          2. Conversely, Users will be capable of being exported to the Active Directory.
       8. Unicode: Utilize Unicode worldwide character set standard. Support double-byte character sets to facilitate adaptation of the System user interface and documentation to new international markets.
          1. Language Support: Includes English, Spanish, Portuguese, French, German and Simplified Chinese.
       9. Encryption: Provide multiple levels of data encryption
          1. True 128-bit AES data encryption between the host and intelligent controllers.

Encryption: Data integrity to be compliant with FIPS-197 requirements and SCIF environments.

Master Keys: Downloaded to the intelligent controller, which shall then be authenticated through the Security Management System based on a successful match.

* + - * 1. Transparent database encryption, including log files and backups.
        2. SQL secure connections via SSL or TLS1.2 with PW7K hardware.
      1. Supervised Alarm Points: Supervised and non-supervised alarm point monitoring.
         1. Upon Alarm Recognition: System to be capable of switching CCTV cameras that are associated with the alarm point.
      2. Compliance and Validation: Incorporate signature authentication where modifications to System resources will require either a single or dual signature authentication.
         1. Administrators: Have ability to select specified devices in the System where data manipulation will be audited, and signatures will be required to account for the data modification.
         2. Upon Resource Modification: User will be required to enter a reason for change or select a predefined reason from a list.
         3. Data will be securely stored and maintained in the database and can be viewed using the reporting tool.
         4. Functionality will meet the general requirements of Validation and Compliance through Digital Signatures with special attention to the case of Title 21 CFR Part 11 Part B compliance.
      3. Clean Room Solution:
         1. Overview: System provides a clean room solution which enables users to manage their "Clean Environments" or other areas requiring special restricted access through a process-oriented graphical user interface (GUI).
         2. Configuration: Users have the capability of adding, editing, or deleting clean rooms.
         3. Each "Clean Room:" Capable of having a contamination level set.

Entry to a higher-level contamination area will automatically restrict access to cleaner level areas.

Individual cards must be capable of being reset on an immediate one time, automatic, or per-hour basis.

* + 1. Security Management System Operational Requirements:
       1. System Operations:
          1. Windows Authentication Login: Use an integrated login method which accepts the user ID of the person who has logged on to Windows.
          2. Password: Use an integrated authentication method which utilizes Windows user accounts and policies.
          3. Information Access: Capable of limiting operators' access to sensitive information. Operators must have proper authorization to edit information.
          4. Shadow Login: Lets users login over a currently logged-on user without having the current user log off the System or out of the Windows operating system.
          5. Graphical User Interface: Compliant with Microsoft graphical user interface standards, with the look and feel of the software being that of a standard Windows application, including hardware tree-based system configuration.
          6. Guard Tour Module: Allows users to program guard tours for their facility. Tours do not require the need for independent or dedicated readers.
          7. Secure Mode Verification Control (e.g., force guard to do a visual verify): From the verification viewer. Allow user or guard to decide the access of an individual who presents their card at a designated secure mode reader.
          8. Database Partitioning: A System in which partitions are set up at installation and cannot be easily changed is not acceptable.
          9. Status Groups: Real-time system status monitors that graphically depicts all logical devices.
          10. Automatically Disable Card upon Lack of Use: Set a predefined time period in which cardholders may swipe their card through a card reader.
          11. User Functions and ADA Ability: Provide user functions and ADA (Americans with Disabilities Act) ability that provides the capability to trigger an event at the System intelligent controller when a defined card is presented.
          12. Pathways: Support pathways programming. A pathway is an object that combines input points to be masked (shunted) for a set duration, and an output point to be activated, when a particular card receives a local grant at a reader.
          13. Database Audit Log: Capable of creating an audit log in the history file following any change made to System database by an operator.
          14. Operator Log: Capable of creating an action log in the history file following actions performed by an operator.
          15. Alarm Routing: Capable of defining routing groups that determine what event information is to be routed to a user or class of users.
          16. Global and Nested Anti-Pass back: Support use of an optional Anti-Pass back mode, in which cardholders are required to follow a proper in/out sequence within the assigned area.
          17. Two Person Rule: Support a "two-person rule" to restrict access to specific access areas unless two cardholders present two different valid cards to the reader one after the other within a period time defined by the door unlock time multiplied by a factor of 2.
          18. Occupancy Restrictions: Allow user to define the minimum and maximum occupancy allowed in a designated area.
          19. Multiple Sequential Card Swipes to Initiate Procedure: Allow the user to define a logical device, quantity of consecutive identical events, a time period and a System procedure to trigger when the event occurs a maximum quantity of
          20. times in the allocated time period.
          21. Hardware Templates: Include ability to define hardware templates (door templates) to simplify the process of creating an access control system. Hardware templates allow a user to define a "typical" door configuration and then use that template over and over in the process of defining doors.
          22. Mercury Digital Terminal (MRDT) with Keypad: Accommodate Mercury Intrusion hardware like the MRDT.

MRDT works with PW-6000/7000 panel to provide intrusion functionality. Mercury Intrusion requires a special Pro-Watch license.

* + - * 1. Panel Conversion Utility: PW6K hardware can be converted to PW7K hardware.
      1. Access Control Functional Requirements: Include validation based on time of day, day of week, holiday scheduling, site code verification, automatic or manual retrieval of cardholder photographs, and access validation based on positive verification of card/PIN, card, and video. The following features are programmable and capable of being modified by a user with the proper authorization:
         1. Time Zones: Define the period during which a reader, card, alarm point, door, or other system feature is active or inactive. In addition to Monday-Sunday, there shall be at least one day of the week called Holiday.
         2. Holidays: Allow holidays to be entered into the System. Holidays will have a start date plus duration defining multiple days. Holidays have a holiday type of 1, 2, or 3, which may be defined by the user.
         3. Response Codes: Allow user to enter a predefined code to represent a response to an alarm occurring in the facility.
         4. Clearance Codes: Allow user to establish groups of readers at a facility for the purpose of granting or denying access to badge holders. Clearance codes may be assigned to companies and individuals employed by the company and may be modified for individual users in the badge holder maintenance application.
         5. Companies: Each badge holder entered into the Security Management System must be assigned a company code identifying the individual's employer. The company information dialog box displays and maintains information related to companies having access to the facility.
         6. Access Groups: Allow a user or group of users via company selection, a temporary denial of access to specific readers or areas based on a preconfigured event. The group access function limits access to a group of cardholders, overriding other access criteria.
         7. Event: Definitions are shipped with system software but are capable, upon installation, of being modified, added to, or deleted from the System.
         8. Alarm Pages: Create an unlimited number of customized alarm pages for the alarm monitor and each are assignable to users and user classes.
         9. Event Types: Definitions are shipped with system software but are capable, upon installation, of being modified, added to, or deleted from the System.
         10. Dynamic Graphical Maps: Provides the user with the means to add maps and indicator icons to maps that represent input/output points, logical devices, or cameras located throughout the System.

Maps display the state and condition of alarm points.

Provides the ability to monitor the channels or panels.

* + - * 1. Brass Keys: Maintain information related to assets issued in the facility, including brass keys, laptops, RSA keys, cell phones, company cards, etc.
        2. ID Badging Client: Maintain information related to a badge holder's card access privileges. Upon entering this application, a window shall appear on the screen and all actions (add, modify, or delete) involving badges and cards are to be initiated from this window.

Access Privileges: Linked to cards used to gain access to facility doors.

Modifications are made by adding or deleting clearance codes, or by door types assigned to the cards or to a badge holder.

* + - * 1. ID Badging System: Includes seamlessly integrated ID badging system.
        2. Users: Information related to users of the System software is stored in the database. Users entered into the System are assigned access privileges of the class to which they are assigned.
        3. Elevator Control: To be of the System intelligent controller-based line of devices including Direct Dispatch. The elevator control is to include the following:

Elevator Call: Valid card read calls elevator to the floor. No reader in the elevator car.

Floor Control: Valid card read in the elevator car enables selectable floor buttons.

Floor Select: Valid card read in the elevator car enables selectable floor buttons and logs which floor is selected after the card is presented.

* + - * 1. Data Transfer Unit (DTU): Enables data to be imported from an external system directly into the System database and exported to an external system.

Insert Only: If a "data file key column number" is to be provided, the DTU will only insert a new badge record if the key column value is not found.

An error will be displayed in the log file if an existing badge record is found.

If no "data file key column number" is provided, every record will be inserted into the System.

Updates only: The DTU uses the "data file key column number" to look for the matching System record. An error is logged in the log file if the badge holder is not found in the System database.

Inserts, Updates: The DTU uses the "data file key column number" to look for the matching .System record. If a matching record is not found, the DTU inserts the data. If a matching record is found, the record is updated.

Supports SOAP web services.

* + - * 1. Generic Channel Interface: Ability to define generic communications channels over serial port or TCP/IP network socket including IP address and port/socket, to support custom integration of external foreign devices. Generate events based on data received from channel matching operator pre-defined instructions.
      1. Application Localization: Support at least seven languages including English.
         1. Available Languages: German, French, Spanish, Italian, Chinese (simplified), Portuguese (Brazil), Norwegian, Chinese (Traditional), Danish, and Dutch.
         2. Database resources will be localized and will include a standard U.S. English help file.
      2. Event Manager: Utilize an event manager as a component of system administration and offer ability to have users control the amount of data stored as well as a quick snapshot of the logged data in the system.
         1. Using the various logs in event manager, the user will be able to gather information about events, auditing, and operator actions.
         2. Defined Logs: Event log, audit log, and unacknowledged alarms.
         3. Intelligent Controllers - Hardware Requirements:
      3. Distributed Architecture: Allows controllers to operate independently of the host. The architecture places key access decisions, event/action processing and alarm monitoring functions within the controllers, eliminating degraded mode operation.
      4. Flash Memory Management: Supports firmware updates and revisions to be downloaded to the System. Upgrades to hardware and software occur seamlessly without the loss of database, configurations, or historical report data.
      5. The security management system is to be equipped with access control field hardware required to receive alarms and administer access granted/denied decisions.
      6. Field hardware must meet UL requirements.
      7. Subject to compliance with requirements, provide Field Controllers or comparable products by one of the following:

\*\* NOTE TO SPECIFIER \*\* Delete controls options not required. Then delete manufacturers and model numbers not required. Legacy controllers should not be used in design of New systems. They are listed as integration reference in retrofit designs. Select the appropriate components and delete the others, as necessary.

* + - * 1. Intelligent Controller Board:

Honeywell Security PW7K1IC.

Honeywell Security PW7K1ICE.

Honeywell Security Legacy PW hardware

* + - * 1. Single Reader Module (SRM):

Honeywell Security PW7K1R1.

Honeywell Security PW7K1R1E.

* + - * 1. Dual Reader Module (DRM):

Honeywell Security PW1K1R2B.

* + - * 1. Alarm Input Module (AIM):

Honeywell Security PW7K1IN.

* + - * 1. Relay Output Module (ROM):

Honeywell Security PW7K1OUT.

* + - * 1. Mercury Family Hardware:

LP-1501.

LP-1502.

LP-2500 with Wiegand Reader.

LP-4502 with embedded authentication for FICAM and Elevator Destination Dispatch

MR16IN (16 Input Board).

MR16OUT (16 Output Board).

MR50-S3 (Single Reader Board).

MR62E (Single Reader Board ETHERNET).

MR52-S3B (2-Reader Board).

* + - * 1. Enclosures - Hardware Requirements:

Honeywell Security

PW5KENC1

PW5KENC2

PW5KENC3

PW5KENC4

Life Safety Standard Power Supplies with PW7K hardware:

HWP-4DR-E2HWTC

HWP-4DR-E2HWTD

HWP-8DR-E4H1WPC

HWP-8DR-E4H1WPD

HWP-16DR-E8H1WTC

HWP-16DR-E8H1WPD

HWP-24DR-E12HWPC

HWP-24DR-E12HWPD

HWP-4DR-RGHWTC

HWP-4DR-RGHWTD

HWP-8DR-RGXHWTC

HWP-8DR-RGXHWTD

Life Safety Managed Power Supplies with PW7K hardware:

HWP-4DRN-E2HWTC

HWP-4DRN-E2HWTD

HWP-8DRN-E4H1WPC

HWP-8DRN-E4H1WPD

HWP-16DRN-E8H1WTC

HWP-16DRN-E8H1WPD

HWP-24DRN-E12HWPC

HWP-24DRN-E12HWPD

HWP-4DRN-RGHWTC

HWP-4DRN-RGHWTD

HWP-8DRN-RGXHWTC

HWP-8DRN-RGXHWTD

* + - * 1. Card Readers - Hardware Requirements:

Honeywell Security: OmniSmart

Honeywell Security: OmniArch

Honeywell Security: OmniProx.

HID: Signo

HID: ProxPro.

HID: MiniProx.

HID: MaxiProx.

HID: ThinLine II.

HID: ProxPro II.

HID: ProxPoint Plus.

STiD: ARC

Indala: FlexPass.

Indala: FlexPass Linear.

Indala: FlexPass Arch.

Indala: FlexPass Curve.

Indala: FlexPass Long Range.

Indala: FlexPass Wave.

Biometric Readers: Idemia

Biometric Readers: Suprema

Biometric Readers: TBS Biometrics

Wireless Locks: SALTO SALLIS and SVN Wireless Locks

Wireless Locks: ILOQ Wireless Padlocks

Wireless Locks: Allegion NDE/LEB and AD-400 Wireless Locks.

Wireless Locks: ASSA ABLOY APERIO Wireless Locks

Wireless Locks: SCHLAGE Wireless Locks

* + 1. Digital Video Recording Systems:
       1. The Security Management System provides fully integrated support for a powerful network and digital video recording and transmission system.
          1. The system shall record, search, and transmit video, and shall provide users with live, pre- and post- event assessment capabilities.
          2. The NVRs/DVRs are to be seamlessly integrated with existing video equipment and incorporated into any TCP/IP network. The NVRs/DVRs shall provide multiple levels of integration with the System software, providing control of the network or digital video system from the access control application.

\*\* NOTE TO SPECIFIER \*\* Legacy recorders should not be used in design of New systems. They are listed as integration reference in retrofit designs.

* + - 1. Acceptable Products:
         1. Honeywell Pro-Watch and MAXPRO NVRs
         2. Honeywell 35 Series Recorders
         3. Honeywell ADPRO Recorders \*No Intelligent Command
         4. Honeywell Performance Recorders (Legacy) \* No Intelligent Command
    1. Video Management Systems (VMS):
       1. With VMS Integration, the System can control multiple sources of video subsystems in a facility to collect, manage and present video in a clear and concise manner.
          1. VMS intelligently determines the capabilities of each subsystem across various sites, allowing video management of any analog or digital video device through a unified configuration and viewer.
          2. Disparate video systems are normalized and funneled through a common video experience.
          3. Drag and drop cameras from System hardware tree into VMS views.
          4. Leverage System alarm integration and advanced features such as pursuit that help the operator track a target through a set of sequential cameras with a single click to select a new central camera and surrounding camera views.
       2. Acceptable Product: Honeywell Security Pro-Watch and MAXPRO VMS.
    2. Intercom Interface:
       1. Provides control of remote and master intercom stations from within the System application. Allows the user to define the site, channel, description, and address as well as provide a checkbox for primary station.
       2. Administrators: Have the capability to program a list of intercom functions that report to the alarm-monitoring module as events.
          1. These functions coincide with intercom functions provided with the intercom system.
          2. For each intercom function, System Administrators can define an alphanumeric event description 1 to 40 characters in length and shall also be able to set the parameter value of that function.
       3. Intercom Interface: Allow for secondary annunciation of intercom calls, events, and alarms in the alarm-monitoring window.
          1. Intercom reporting to the alarm monitoring window, reports as other access control alarm and has the annunciation and display properties of access control alarms.
       4. All intercom calls, events, and alarms that report into the System are to be stored in the system database for future audit trail and reporting capabilities.
          1. Intercom events include but not limited to: Station busy, Station free, Intercom call to busy station, Intercom call to private station, Station disconnected, Function dialed outside connection, Intelligent station ID, Station reset, Station lamp test, Audio program changed, Group hunt occurred, Mail message, Digit dialed during connection, Direct access key pressed, Handset off hook, M-key pressed, C-key pressed.
       5. Manufacturers and part numbers:
          1. Legacy Zenitel Alphacom series intercoms.
          2. Commend series intercoms.
    3. Intrusion Detection Panels:

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

* + - 1. Honeywell VISTA-128FBP, VISTA-128BPE, VISTA-128BPT, VISTA-250FBP, VISTA-250BPE, and VISTA-250BPT Controllers:
         1. General Requirements: Support hardwired and TCP/IP communication for the VISTA 128FBP/VISTA-250 FBP panel.

Each panel is to have 8 partitions and 15 zone lists.

Zones, partitions, and the top-level panel is to have an events page, with all supported events present.

* + - * 1. 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 S3100, GD264 and GD520 Controllers:
         1. Users can control and monitor group and zone status using the 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 System, a 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.
         2. Features:

Disarm a zone on a card swipe.

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

Supports linking intrusion panel users with System cardholders.

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

The system can associate alarm events with video commands to look at current or historic footage.

Stores and reports on intrusion events.

* + 1. Gunshot Detection: Fully integrated support for gunshot detection system with appropriate license:
       1. Manufacturer: EAGL Technology, Inc
    2. Third Party Integrations (SDK and API)
       1. Permit custom integration with other third-party systems through an SDK or API.
          1. SDK: To support OBIX communication protocol and interface directly with the Niagara Framework for support of additional communications protocols.
          2. API: Utilizes SOAP and REST protocols.
       2. Acceptable Products:
          1. Manufacturer and Part Number: Honeywell Security HSDK
          2. Manufacturer and Part Number: Honeywell Security API.
    3. Visitor Management System:
       1. Allow user to track visitors, employees, assets, and deliveries as they enter and exit the facilities.
       2. Print custom designed visitor passes with details like expiration date, visit area, host being visited, and visit purpose.
       3. Acceptable Products: Honeywell Security Pro-Watch Visitor Management.
    4. Web Client - Intelligent Command:
       1. Alarms.
       2. Incident Workflows.
       3. Events.
       4. Badging.
       5. Mapping.
       6. Dashboards.
       7. Reports.
    5. Supported Web Browsers:
       1. Google Chrome
       2. Microsoft Edge
       3. Firefox

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

* 1. VISITOR MANAGEMENT SYSTEM
     1. Product: Pro-Watch Visitor Management as manufactured by Honeywell Commercial Security: The Visitor Management System shall allow the user to track visitors as they enter and exit the facilities. The system shall also support printing of custom designed visitor passes with details like expiration date, visit area, host being visited, QR code access credential and visit purpose.
     2. The Visitor Management System shall allow the user to:
        1. Define location-specific pre-registration questionnaire, email templates, and kiosk welcome screens for their visitor locations.
        2. Define a publicly facing pre-registration website for visitors to view, complete, and acknowledge ahead of their visit including health questionnaire questions that can be scheduled up to 72 hours prior to an on-site visit.
        3. Define if a visitor location supports QR or Physical Access Card issuance and the specific access areas associated with these locations.
        4. Define a location's default language for notifications to visitors.
        5. Define a location's number of days of data retention before deletion.
        6. Allow users to select a preferred language amongst 14 supported languages in the visitor management system, pre-registration site, and kiosk welcome screen.
        7. Secure visitor management system invitation and visit log through Administrator, Operator or Host role definition in Pro-Watch Access Control.
        8. View and export user-defined fields on visit list or invitation list to .csv or .pdf for reporting and tracking.
        9. Integrated scheduler to initiate common workflows for automatic system check-out, access enable /disabling based on visitor status, physical access card not returned reminder emails.
        10. Define a list of Watchlist users who will be prevented from visiting your locations.
        11. Process most visitors in 20 seconds.
     3. Visitor Pre-Registration:
        1. Visitor pre-registration website with location-specific requirements defined by administrators including identification information, configured health questionnaire inputs, view & acknowledge training video, non-disclosure agreement acknowledge, and data retention policy acknowledgement.
        2. Upon completion, visitor can receive check-in code for expedited onsite Kiosk check-in.
        3. Complete visitor registration processing within 20 seconds.
     4. Visitor Information Capture:
        1. Quick and complete capture of visitor information as an essential component for proper record keeping and security checks.
        2. Completed during pre-registration or on-site at kiosk or with support of an operator.
     5. Visitor Authentication:
        1. Recalling previous visit information (including pictures) when a visitor revisits.
        2. Detecting each attempted visit and deterring potential security breaches before they affect the user facilities.
        3. Importing guests ranging from disgruntled ex-employees to known felons into the watch list to alert personnel of a potential threat to the organization.
     6. Visitor Authorization:
        1. Enforcing visitor authorization prior to printing a badge, entering the premises, authorizing visits at reception, security lobby, or remotely by the host employee.
        2. Delegating authorization responsibility to specific individuals.
        3. Providing a denied visitors list.
     7. Visitor Badges Generation:
        1. Provide quick, cost-effective, and individualized badging as an essential component of proper visitor identification.
        2. Allow printing of individualized visitor badges containing name, picture, expiration date, and valid access areas (including the access 2D barcode code if applicable)
        3. Customize badge templates for visitors and apply them to specific locations.
        4. Supports tight integration with Pro-Watch Security systems that allow the assignment of access control privileges via 2D barcode or physical access card to visitors.
     8. Host Notification:
        1. A visitor's arrival by e-mail message.
        2. A visitor's missing physical access card return after check-out.
     9. Visitor Tracking:
        1. Track events automatically by an accurate log as they relate to the visitor's activities on site.
        2. Track the number of times the visitor signs in and signs out.
        3. Support quick sign in and out using a 2D barcode scanner.
        4. Proactive checking for expired visits and network notification to hosts and visitors of expired visits.
        5. Web access to the visitor manifest.
     10. Security Policies:
         1. Accurate and consistent application of security policies.
         2. A means to view a picture and a person's attributes, reason for being on the watch list, and the action to be performed upon visitor's arrival.
         3. Check each visitor against his/her previous visit information.
         4. Ensure visitors sign out by tracking expired visits and informing their hosts.
     11. Host Management:
         1. Assign the capabilities available to employees based on their requirement.
         2. Approve or deny an uninvited visitor.
         3. Invite visitors for single day or multiple day visits to locations across the system.
         4. View their list of visitors and their corresponding invitation statuses.
         5. Edit and reschedule visits and kickoff the reschedule notification workflow to visitor's email.
     12. Operator Management:
         1. Assign card numbers in visitor management for visitors requiring a physical access card credentials for their visit.
         2. Print badges for visitors from the visitor management system.
         3. Capture visitor image upon check-in.
         4. Able to do a visual verify of the employee to their photo at the operator desk.
     13. List Filter, Sort, Search and Export:
         1. Users can configure column for display on visit list and invitation list.
         2. Users can sort, filter, and search columns on visit list and invitation list.
         3. Operators and Administrators can sort, filter, and search columns on watchlist.
         4. Administrators can export visit list, watchlist, and invitation list to .csv or pdf for reporting and tracking.
     14. Self-Registration Visitor Kiosk:
         1. Full featured to handle visitor registration needs in a busy or unattended lobby.
            1. Used to perform touchscreen visitor registration using a visitor's inputs from kiosk or scan of QR code on mobile device.
         2. Used to take picture of visitors for true visitor identification, as well as display visitation rules/non-disclosure agreement.
         3. Print a visitor badge at the station operator desk and allow for remote authorization of the visit by the host or security desk.
         4. Notifies the hosting party when their visitor arrives.
     15. Security Audit Compliance:
         1. Secure database.
         2. Audit log.
         3. Tamper proof visitor records.
         4. Audit reports.
         5. Backup and restore capabilities.

\*\* NOTE TO SPECIFIER \*\* Delete article if Readers are not required or delete readers 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 that comply with these standards.
        3. Output credential data in compliance with SIA AC-01 Wiegand standard:
        4. Reads standard proximity format data from OmniClass cards and outputs data as encoded.
           1. Reads card serial number (CSN) of a MIFARE or DESFIRE card with configurable outputs as 26-, 32-, 34-, 40-, or 56-bit.
        5. Use up to 128-bit authentication keys to reduce the risk of compromised data or duplicate cards. The card reader and cards require matching keys to function together. All RF data transmission between the card and the reader is to be encrypted, using a secure algorithm. Card readers are to be provided with keys that are compatible with the OmniClass cards.
        6. The reader shall be of potted, polycarbonate material, sealed to a NEMA rating of 4X (IP65).
        7. Field change operational features using factory-programmed command cards. Update firmware by flashing the card reader.
           1. Operational Programming Options Include:

Output configurations.

LED and Audio configurations.

Keypad configurations.

* + - 1. Provide the Following Programmable Audio/Visual Indication:
         1. Audio Transducer: Provide tone sequences to signify access granted, access denied, power up, and diagnostics.
         2. High-Intensity Light Bar: Provide clear visual status; red, green, and amber, that is visible in bright sunlight.
      2. Certifications Compliance:
         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).
      3. 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.
      4. Contactless smart card reader cabling requirements shall be:
         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.
      5. Warranty: Lifetime against defects in materials and workmanship.
    1. Product: OS20TOSDP Mullion 13.56 MHz Contactless Smart and 125 kHz Prox Card Readers as manufactured by the Honeywell Commercial Security.
       1. Read Range:
          1. Seos, MIFARE Classic, MIFARE DESFire EV1/EV2/EV3, and ISO14443A Single Technology Cards. Dimensions: 1.6 to 4 inch (4 to 10 cm).
          2. HID / AWID Proximity, Indala Proximity, EM Proximity, and 125 kHz Single Technology Cards.Dimensions: 2.4 to 4 inches (6 to 10 cm).
       2. Dimensions: 1.77 x 4.78 x 0.77 inches (45 x 121.5 x 19.5 mm).
       3. Weight: 3.35 oz (95 grams).
       4. Material: UL94 Polycarbonate.
       5. Two-part design with separate mounting plate and reader body/
       6. Color: Black.
       7. Electrical Operating Voltage: 12 VDC
          1. Current Requirements: NSC4: 60 mA. Peak: 250 mA Maximum. Avg: 70 mA. IPM5: 45 mA.
    2. Product: OS20KTOSDP 13.56 MHz Contactless Smart and 125 kHz Prox Card with Keypad Readers as manufactured by the Honeywell Commercial Security:
       1. Read Range:
          1. Seos, MIFARE Classic, MIFARE DESFire EV1/EV2/EV3 and ISO14443A Single Technology Cards. Dimensions: 1.6 to 4 in (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. Dimensions: 1.78 x 4.79 x 0.85 inches (45 x 121.5x 21.5 mm).
       3. Weight: 3.88 oz (110 grams).
       4. Material: UL94 Polycarbonate.
       5. Two-part design with separate mounting plate and reader body.
       6. Color: Black.
       7. Electrical Operating Voltage: 12 VDC
          1. Current requirements: NSC4: 65 mA. Peak: 250 mA Maximum. Avg: 75 mA IPM5: 48 mA.
    3. Product: OS40TOSDP US Single-Gang 13.56 MHz Contactless Smart and 125 kHz Prox Card Readers as manufactured by the Honeywell Commercial Security:
       1. Read Range:
          1. Seos, MIFARE Classic, MIFARE DESFire EV1/EV2/EV3 and ISO14443A Single Technology Cards: 1.6 to 4 in (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. Dimensions: 3.30 x 4.80 x .85 inches (8.38 x 12.19 x 2.16 cm).
       3. Weight: 8.8 oz (249.5 grams).
       4. Material: UL94 Polycarbonate.
       5. Two-part design with separate mounting plate and reader body.
       6. Color: Black.
       7. Electrical Operating Voltage: 12 VDC.
          1. Current requirements: NSC4: 65 mA. Peak: 250 mA Maximum. Avg: 75 mA. IPM5: 45 mA.
    4. Product: OS40KTOSDP 13.56 MHz Contactless Smart and 125 kHz Prox Card W/ Keypad Readers as manufactured by the Honeywell Commercial Security:
       1. 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).
          3. Dimensions: 3.30 x 4.80 x 0.90 inches (8.38 x 12.19 x 2.28 cm).
          4. Weight: 10 oz (283.4 grams).
          5. Material: UL94 Polycarbonate.
          6. Two-part design with separate mounting plate and reader body.
          7. Color: Black.
          8. Electrical Operating Voltage: 12 VDC.

Current Requirements: NSC4: 70 mA. Peak: 250 mA Maximum. Avg: 80 mA. IPM5: 55 mA.

* + 1. Product: OS20TT2OSDP Mullion 13.56 MHz Contactless Smart Card Readers as manufactured by the Honeywell Commercial Security:
       1. 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. Dimensions: 1.77 x 4.78 x 0.77 inches (45 x 121.5 x 19.5 mm).
          3. Weight: 2.65 oz (75 grams).
          4. Material: UL94 Polycarbonate.
          5. Two-part design with separate mounting plate and reader body.
          6. Color: Black.
          7. Electrical Operating Voltage: 12 VDC.

Current Requirements: NSC4: 60 mA. Peak: 250 mA Maximum. Avg: 70 Ma. IPM5: 45 mA.

* + 1. Product: OS20KTT2OSDP Mullion 13.56 MHz Contactless Smart Card Readers as manufactured by the Honeywell Commercial Security:
       1. Read Range:
          1. Seos, MIFARE Classic, MIFARE DESFire EV1/EV2/EV3, and ISO14443A Single Technology Cards: 1.6 to 4 in (4 to 10 cm).
       2. Dimensions: 1.78 x 4.79 x 0.85 inches (45 x 121.5 x 21.5 mm).
       3. Weight: 3.17 oz (90 grams).
       4. Material: UL94 Polycarbonate.
       5. Two-part design with separate mounting plate and reader body.
       6. Color: Black.
       7. Electrical Operating Voltage: 12 VDC.
          1. Current Requirements: NSC4: 65 mA. Peak: 250 mA Maximum. Avg: 75 mA. IPM5: 48 mA.
    2. Product: OS40TT2OSDP US Single-Gang 13.56 MHz Contactless Smart Card Readers as manufactured by the Honeywell Commercial Security:
       1. 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. Dimensions: 3.30 x 4.80 x 0.85 inches (8.38 x 12.19 x 2.16 cm).
       3. Weight: 8.8 oz (249.5 grams).
       4. Material: UL94 Polycarbonate.
       5. Two-part design with separate mounting plate and reader body.
       6. Color: Black.
       7. Electrical Operating Voltage: 12 VDC.
          1. Current requirements: NSC4: 65 mA. Peak: 250 mA Maximum. Avg: 75 mA. IPM5: 45 mA.
    3. Product: OS40KTT2OSDP 13.56 MHz Contactless Smart Card with Keypad Readers as manufactured by the Honeywell Commercial Security:
       1. 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. Dimensions: 3.30 x 4.80 x 0.90 inches (8.38 x 12.19 x 2.28 cm).
       3. Weight: 10 oz (283.4 grams).
       4. Material: UL94 Polycarbonate.
       5. Two-part design with separate mounting plate and reader body.
       6. Color: Black.
          1. Electrical Operating Voltage: 12 VDC.
          2. Current requirements: NSC4: 70 mA. Peak: 250 mA Maximum. Avg: 80 mA. IPM5: 55 mA.

\*\* NOTE TO SPECIFIER \*\* Delete article if Credentials are not required or delete credentials paragraphs not required.

* 1. ACCESS CONTROL CREDENTIALS
     1. Access Cards: Used with access readers to gain entry to access controlled portals (e.g., doors, gates, turnstiles) and hold information specific to the user and be Contactless Smart Card or Contactless Proximity Card technology credentials.
     2. Contactless Smart Cards:

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

* + - 1. Single Technology Access Card:
         1. Standards Compliance: ISO 15693 and ISO 14443B2.

ISO 7810 for length, width, thickness, flatness, card construction, and durability. Suitable for direct two-sided dye-sublimation or thermal transfer printing on the specified badge printer.

* + - * 1. Card to have no identification showing location of property unless otherwise specified.
        2. Compatible with specified card readers. Factory encoded with Wiegand card data.
        3. Presentation to Access Control Readers: Any angle within a minimum of one inch (25 mm) must result in an accurate card reading.
        4. Fixed Card Serial Number: Unique 64-bit. For anti-collision and key diversification.
        5. Support Capability:

EEPROM Memory: 2 Kbits (256 bytes) minimum.

Application Areas: 2

EEPROM Memory: 16 Kbits (2048 bytes).

Application Areas: 2 or 16 to support future applications.

Data Retention: 10 years, nominal.

Wiegand Card Data: Length: Up to 84 bits.

Application Area 1: Factory programmed for use with access control systems.

* + - * 1. Application Areas on the Card:

Unique Security Key: 128-bit. Cannot access or edit stored data until card and reader have completed a mutual authentication process.

* + - * 1. The card must be capable of completing any write operation, even if the card is removed from the RF field during that operation.
        2. Warranty: Against defects in materials and workmanship for two years.

If Multiple Technologies are Used:

Magnetic Stripe: Fifteen months.

Contact Chip: One-year warranty.

* + - * 1. May be slot punched on one end, for lanyard attachment in a vertical orientation.

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

* + - 1. Multiple Technology Access Card:
         1. Available with 13.56 MHz OmniClass contactless smart chip and antenna.

Available with any or all the following technologies, simultaneously:

125 kHz HID Proximity chip and antenna.

Magnetic stripe.

Embedded Contact Smart Chip Module.

* + - * 1. Available with 13.56 MHz OmniClass contactless smart chip and antenna meeting all ISO 7810 standards except for card thickness.

Available with the following technologies, simultaneously:

Wiegand strip

\*\* NOTE TO SPECIFIER \*\* Magnetic stripe is optional. Delete if not required.

Magnetic stripe.

Card Thickness: 0.037 inch (0.939 mm).

Not available with 125 kHz proximity technology.

Not available with Embedded Contact Smart Chip Module.

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

* + - 1. Access Key Fob:
         1. Standards Compliance: ISO 15693 and ISO 14443B2.
         2. Construction: Durable injection molded polycarbonate plastic, with a slot molded into one end. Suitable for key ring placement.
         3. Presentation to the Access Control Reader: At any angle within one inch (25 mm) minimum must result in an accurate reading.
         4. Compatible with specified card readers.
         5. Must not carry identification showing location of property unless otherwise specified.
         6. Warranty: Against defects in materials and workmanship for two years.

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

* + - 1. Access Sticker: For transitioning from earlier technologies to contactless smart cards.
         1. Standards Compliance: ISO 15693 and ISO 14443B2.
         2. A flat disc-shaped unit. Polycarbonate cover. Self-stick adhesive back.
         3. Capable of affixation to non-metallic personal items such as PDAs, cell phones, business assets, or to existing access control or identification cards
         4. Not to be used with tractor-feed, i.e. full-insertion readers.
         5. Presentation to Access Control Readers: Any angle within one inch (25 mm) minimum must result in an accurate reading.
         6. Compatible with specified card readers.
         7. Must not carry identification showing location of property unless otherwise specified.
         8. Warranty: Against defects in materials and workmanship for two years.
    1. Contactless Proximity Cards:
       1. HID Proximity Chip and Antenna: 125 kHz.
          1. Meet ISO 7810 specifications for length, width, thickness, flatness, card construction, and durability.

Printing: Suitable for direct two-sided dye-sublimation or thermal transfer on specified badge printers.

* + - * 1. Presentation to Access Control Reader: Any angle within one inch (25 mm) minimum must result in an accurate reading.
        2. Capable of completing any write operation, even if the card is removed from the RF field during that operation.
        3. Smart Access Cards: Compatible with

Wiegand Card Data: Factory encoded with 26- or 34-bit formats.

* + - * 1. Must not carry identification showing location of property unless otherwise specified.

May be slot punched on one end, for lanyard attachment in a vertical orientation.

* + - * 1. Warranty: Against defects in materials and workmanship for two years.

If Multiple Technologies are Used:

Magnetic Stripe: Fifteen months.

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 requirements of the installation of the System.
   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