SECTION 281300

INTEGRATED SECURITY MANAGEMENT SYSTEM

PART 1 GENERAL

1.1 SECTION INCLUDES

A. Provide a modular and network-enabled access control system for security management, including engineering, supply, installation, and activation.

1.2 RELATED SECTIONS

NOTE TO SPECIFIER: Include the related sections as appropriate if access control system is integrated to other systems.

A. Section 260500 – Common Work Results for Electrical, for interface and coordination with building electrical systems and distribution.

B. Section 280513 – Conductors and Cables for Electronic Safety and Security, for cabling between system servers, panels, and remote devices.

C. Section 280528 – Pathways for Electronic Safety and Security, for conduit and raceway requirements.

D. Section 281600 – Intrusion Detection, for interface to building intrusion detection system.

E. Section 282300 – Video Surveillance, for interface to video surveillance system.

F. Section 283111 – Digital, Addressable Fire Alarm System, for interface to building fire alarm system.

G. Section 283112 – Zoned (DC Loop) Fire Alarm System, for interface to building fire alarm system.

1.3 REFERENCES

A. Reference Standards: Systems specified in this Section shall meet or exceed the requirements of the following:

1. Federal Communications Commission (FCC):

a. FCC Part 15 – Radio Frequency Device

b. FCC Part 68 – Connection of Terminal Equipment to the Telephone Network

2. Underwriters Laboratories (UL):

a. UL294 – Access Control System Units

b. UL1076 – Proprietary Burglar Alarm Units and Systems

3. National Fire Protection Association (NFPA):

a. NFPA70 – National Electrical Code

4. Electronic Industries Alliance (EIA):

a. RS232C – Interface between Data Terminal Equipment and Data Communications Equipment Employing Serial Binary Data Interchange

b. RS485 – Electrical Characteristics of Generators and Receivers for use in Balanced Digital Multi-Point Systems

5. Federal Information Processing Standards (FIPS):

a. Advanced Encryption Standard (AES) (FIPS 197)

b. FIPS 201: Personal Identity Verification (PIV) of Federal Employees and Contractors

6. Homeland Security Presidential Directive 12 (HSPD-12)

1.4 INTEGRATED SECURITY MANAGEMENT SYSTEM DESCRIPTION

A. The Integrated Security Management System (ISMS) shall function as an electronic access control system and shall integrate the alarm monitoring, CCTV, digital video, ID badging and database management into a single platform. ISMS shall function as a one-stop gateway for all the access control needs. A modular and network-enabled architecture shall allow maximum versatility for tailoring secure and dependable access and alarm monitoring solutions.

1.5 SUBMITTALS

A. Manufacturer's Product Data: Submit manufacturer's data sheets indicating systems and components proposed for use.

B. Shop Drawings: Submit complete shop drawings indicating system components, wiring diagrams and load calculations.

C. 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.

D. Operation and Maintenance Data: Submit manufacturer's operation and maintenance data, customized to the Security Management System installed. Include system and operator manuals.

E. Maintenance Service Agreement: Submit a sample copy of the manufacturer's maintenance service agreement, including cost and services for two years, for the Owner's review.

1.6 QUALITY ASSURANCE

A. Manufacturer: A minimum of ten years of experience in manufacturing and maintaining Security Management Systems. Manufacturer shall be Microsoft Gold Certified.

NOTE TO SPECIFIER: Specify minimum level of DSCP certification: Silver, Gold, or Platinum.

B. The Installer must be certified by Honeywell Integrated Security Dealer Service Certification Program (DSCP).

1.7 DELIVERY, STORAGE, AND HANDLING

A. Deliver materials in manufacturer's labeled packages. Store and handle in accordance with the manufacturer's requirements.

1.8 WARRANTY

A. Manufacturer's Warranty: Submit manufacturer's standard warranty for the security management system.

1.9 DEFINITIONS

A. Access Card: A coded employee card, usually the size of a credit card, recognizable to the access control system and read by a reader to allow access. It can be used for photo identification of the cardholder and for other data collection purposes. Card technologies include magnetic strips, Wiegand-effect, proximity (active/passive), barium ferrite, smart/intelligent cards and mobile credentials (smart phone with a credential/app).

B. Abstract Device: An Abstract Device (ADV) is a logical representation of a physical device. The ADVs can be associated with any hardware device, including communication interfaces, panels, alarm points, entrances, and CCTV equipment. The ADVs help in monitoring the device status and controlling the actions of a physical device through the Control Map, Floor Plan, or Alarm View.

C. Access Control System: An interconnected set of controllers, managing the entrance and exit of people through secure areas.

D. WIN-PAK Web: The WIN-PAK Web application is an extension of the WIN-PAK host application with limited operations. The day-to-day operations such as Card/User management, Reports, Door control, Schedules, viewing live card event activities that are common to both WIN-PAK host and WIN-PAK Web application are saved on a common database server. The WIN-PAK Web UI works using the WIN-PAK Web server.

E. Access Level: The door or combination of doors and/or barriers an individual is authorized to pass through.

F. Anti-Pass back (Anti-Tailgating): This feature protects against more than one person using the same card or number. It defines each system card reader and card ID number as IN, OUT or other. Once a card is granted access to an IN reader, it must be presented to an OUT reader before another IN reader access is granted. Cards will continue to have access to all authorized OTHER readers.

G. Alarm: A signal that indicates a problem.

H. Alarm input: A device that is monitored by the access control panel. An alarm signal will be generated if the device is activated.

I. Badge: Badge is a template or a design for creating a card. WIN-PAK includes a full-featured badge layout utility for designing, creating, and printing badges. Badge design includes magnetic stripe encoding, bar coding, signatures, and so on.

J. Bar Code: A method of encoding information using lines and blank spaces of varying size and thickness to represent alphanumeric characters.

K. Biometrics: A general term for the verification of individuals using unique biological characteristics (i.e. fingerprints, hand geometry, voice analysis, the retinal pattern in the eye).

L. Card and Card Holder: A card is an identity proof of a person and a card holder is a person who holds the card. Multiple cards can be assigned to a single card holder to provide different access.

M. Controller: A microprocessor based circuit board that manages access to a secure area. The controller receives information that it uses to determine through which doors and at what times cardholders are granted access to secure areas. Based on that information, the controller can lock/unlock doors, sound alarms, and communicate status to a host computer.

N. Communication Port: A hardware device that allows a computer to communicate with external devices.

O. Card Reader: A device that retrieves information stored on an access card and transmits that information to a controller.

P. Digital Video Recorder (DVR): A security system device that records the video from the surveillance cameras (IP and Analog) on a hard disk.

Q. Door: A generic term for a securable entry way. In many access control applications, a "door" may be a gate, turnstile, elevator door, or similar device.

R. Duress: Forcing a person to provide access to a secure area against that person's wishes.

S. Guard Tour: A defined route of a security guard.

T. Host Computer: The central controlling computer from which access control software applications are run.

U. Input: An electronic sensor on a controller that detects a change of state in a device outside the controller.

V. Keypad: An alphanumeric grid which allows a user to enter an identification code. A flat device which has buttons that may be pressed in a sequence to send data to a controller, and which differs from a typewriter-like computer board.

W. Online Help: A reference program within most software programs that provides basic descriptions and instructions on how to use that software program.

X. Output Relay: A device that changes its state upon receiving a signal from a controller. Typically, the state change prompts an action outside of the controller such as activating or inactivating a device. The auxiliary relays found in access control panels or NODES that control external devices.

Y. Reader: A device that "receives" an identification code from a card, key tag, magnetic stripe card, bar code card, or related item. Refers to the “front end” that a user must interact with to allow access. Readers can be keypads, card readers, proximity readers, and so on.

Z. RS232: A serial communication protocol used for connecting data terminal devices. RS-232 is the most commonly used communication protocol.

AA. Server: The host computer, which has the ISMS functions.

BB. Shunt Time: The length of time a door open alarm is suppressed (shunted) after a valid card access or free egress request. This time should be just enough to allow a card user to open a door or gate, pass through, and then close it.

CC. Time zones: "Schedules" that allow cards to function or not function depending on the time of day. This is used to limit access to the facility. The schedule may include not only time but which days of the week a card is valid.

DD. Wiegand Card: An access control card based on the Wiegand effect. Small bits of specially processed wire are embedded in the card in a pattern that uniquely identifies the card. This identification information can then be decoded by a Wiegand reader.

EE. Wiegand Reader: A reader capable of reading the information encoded on a Wiegand card.

FF. Video Management System (VMS): An enterprise-class video management and storage solution.

PART 2 PRODUCTS

2.1 MANUFACTURER

1. Integrated Security Management System Manufacturer: WIN-PAK Access Management System by Honeywell, www.honeywellaccess.com.

2.2 ISMS COMPONENTS

The ISMS shall be divided into six components: Database Server, Archive Server, Communication Server, User Interface, WIN-PAK API Server, and WIN-PAK Web. These components shall run on a single computer or on multiple computers, allowing flexibility in configuring a networked system.

a. Database Server: The database server is used for storing the database tables. This data is accessible to communication server and user interface for retrieving and generating the reports. The database server shall be installed on the client computer or any other computer connected to the network.

b. Archive Server: The archive server is used to obtain data from the archive database (the archive database consists of the backup details of the WINPAK main database).

c. Communication Server: The communication server routes user interface requests as well as the access transactions to the panel. The panel in-turn processes the transactions and sends the information to the database server as well as responses to the user interface through the communication server. When the communication server is sending information to the database server, it can also receive a request from the user interface. In this scenario, the communication server considers the user request as a higher priority and stops the panel-database server communication until the user request is processed. The communication server shall be installed on the client computer or any other computer connected to the network.

d. User Interface (ISMS Client): The user interface helps ISMS operators to communicate with the access control system. The user interface shall be installed on the computer where the database server or the communication server is installed or any other computer connected to the network. Several client computers can be run simultaneously and can access the single database server simultaneously. The number of client computers varies based on the licensing information of ISMS.

e. WIN-PAK API Server: The API server is used to obtain and set the details in the WIN-PAK database using the Application Programming Interface (API).

f. WIN-PAK Web: The WIN-PAK Web application is an extension of the WIN-PAK host application with limited operations. The 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.

In addition to above six components, ISMS include the following four components, also called as ISMS services.

g. Command File Server: A command file server provides text files containing device instructions that shall be stored in the command files database. The commands in the command files can be sent to the devices automatically on receiving, acknowledging, or clearing an alarm. Also, the command files can be manually executed.

h. Guard Tour server: A guard tour is a defined series of check points a guard must activate within a given amount of time. The check points are readers or input points where the guard presents the card or presses the button.

i. Tracking and Muster Server: A muster server is enabled in the event of an emergency and allows the card holders to swipe the readers. Muster areas are logical areas that contain readers to be used by the card holders, only if there is a call for muster (in the event of a disaster, for example).

j. Schedule Server: A schedule server schedules the list of events to be performed at a predetermined time and intervals such as hourly, daily, or monthly.

k. Video Management Server: A video management server provides interface to connect to various DVR's/NVR's. In addition, it also provides CCTV control with live monitor display, PTZ control of cameras, video playback operations, and so on.

NOTE TO SPECIFIER: The ISMS services are installed while installing the database server or the complete ISMS. The ISMS services start automatically after the installation of ISMS.

2.3 INTEGRATED SECURITY MANAGEMENT SYSTEM OPERATIONAL REQUIREMENTS

A. The ISMS shall be 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 ISMS 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 ISMS reconfiguration shall be accomplished online through system programming.

The ISMS shall include the following features:

1. Multi-User/Network Capabilities: The ISMS shall support multiple operator workstations via local area network/wide area network (LAN/WAN). The communications between the workstations and the server computer shall utilize the

TCP/IP standard over industry standard IEEE 802.3 (Ethernet). The communications between the server and workstations shall be supervised, and shall automatically generate alarm messages when the server is unable to communicate with a workstation. The operators on the network server shall have the capability to log on to workstations and remotely configure the devices for the workstation. Standard operator permission levels shall be enforced, with full operator audit.

2. Operating Environment: The ISMS shall be a true 32-bit or 64-bit, 3-tier client/server, ODBC compliant application based on Microsoft tools and standards. The ISMS application shall operate in the following environments: Microsoft Windows® Server 2016, Windows Server 2012 R2, and 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: The ISMS shall consist of multiple servers including, but not limited to, database server, communications server, and client workstation. The servers shall be capable of being installed on one or more computers across a network providing a distribution of system activities and processes. The ISMS shall support multiple communication servers on a LAN/WAN, to provide distributed networking capabilities, which significantly improve system performance.

5. Multi-level Password Protection: The ISMS application shall provide 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: The ISMS shall be fully compliant with Microsoft Graphical User Interface (GUI) standards, with the look and feel of the software being that of a standard Windows application, including hardware tree-based system configuration.

7. Online Help: The ISMS user interface shall include an Online Help which shall require only one click to activate. The standard 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. The tours shall not require the need for independent or dedicated readers.

9. Concurrent Licensing: The ISMS shall support concurrent client workstation licensing. The ISMS application shall be installed on any number of client

workstations, and shall provide the ability for any of the client workstations 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 shall 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.

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

    b. 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.

12. Relational Database Management System: The Security Management System shall support industry standard relational database management systems. This shall include relational database management system Microsoft SQL Server 2016 Enterprise Edition. The RDBMS shall provide edit, add, delete, search, sort, and print options for records in the selected databases.

13. Database Partitioning: The Security Management System shall provide the option to restrict access to sensitive information by user ID.

14. 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.

15. Encryption: The Security Management System shall provide multiple levels of data encryption.

    a. True 128-bit AES data encryption between the host and intelligent controllers. The 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.

    b. Transparent database encryption, including log files and backups.

c. SQL secure connections via SSL.

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

16. Industry Standard Panel Communication: The ISMS application shall communicate with the access control panels via LAN/WAN connections utilizing industry standard communication protocols.

17. Supervised Alarm Points: The system shall provide both supervised and non-supervised alarm point monitoring. On recognition of an alarm, the system shall can switch and displaying the video from the camera connected to the digital video recorder that is associated with the alarm point.

18. Multiple Account Support: The ISMS application shall allow support for multiple accounts 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.

19. 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.

20. Access Control Functions: The ISMS shall include the following access control functions: validation based on time of day, day of week, holiday scheduling, site code and card number verification, automatic or manual retrieval of cardholder photographs, and access validation based on positive verification of card, card and PIN, card or pin, pin only and Site Code only.

21. Digital Video Recorders (DVRs) Support: The ISMS shall support the ADPRO, MAXPRO NVR and Embedded Performance Series DVRs.

NOTE TO SPECIFIER: Live Video shall be streamed from the supported cameras connected to the corresponding DVRs.

22. Camera Functions: The ISMS shall include the following camera functions: pan/tilt, lens control, limits, and home.

23. Live Video Display: The ISMS shall provide an option to view live video from a camera connected to the digital video recorder on the computer screen. The live video window shall allow the user to change its size and location on the computer screen. Video controls (pan, tilt, zoom) shall be available to customize the display of live video to the user's requirements.

24. Global and Local Anti-passback: The Security Management System shall support the use of an optional anti-passback mode, in which cardholders are required to follow a proper in/out sequence within the assigned area.

25. Alarm Events: The ISMS shall include a feature where alarm events with defined priorities pop-up automatically in an Alarm event window for operator attention. The pop-up shall display the name of the 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 is displayed. An event counter shall also display the number of times the event was reported to the Alarm event monitor prior to Acknowledgement or Clearing the event. Event instructions shall be made available by double clicking on the event. The event shall also display an icon to indicate that video is available for events so programmed. The Alarm event window shall allow the operator to initiate a physical response to the event as well as a written response. Responses shall include but not be 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.

26. Manual Panel Control: The ISMS application shall allow manual control of selected inputs, outputs, and groups of outputs. Manual panel control shall 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.

27. Levels of System Operation: The ISMS shall include 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.

28. Hardware Configuration Changes: After installation of ISMS 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.

29. Distributed Processing: All the control components of the ISMS shall utilize "Distributed-Processing" concepts. The distributed processing shall include 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.

30. Flexible Component replacement: The repair of hardware components associated to the ISMS shall be accomplished on site, by a new replacement, utilizing spare components.

B. The ISMS application shall have the major functional capabilities (considered essential for the system described in this specification) categorized as follows:

1. General

a. All the databases shall have the ability to add, delete, report, view, and edit information.

b. All the system transactions shall be saved in a retrievable file.

c. All the events shall be logged by date and time.

d. All the system transactions or selected system transactions shall be saved in a disk file.

e. The end-user shall have the provision 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.

f. Shall support "Global Anti-pass back", feature allowing cardholder to enter/exit any such defined card reader on the same intelligent control panel or RS-485 drop-line consisting of 2 and 4 door controllers.

g. Anti-pass back modes shall 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.

h. Shall support the "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.

i. Shall support the "Two card holder" rule, where two valid, non-identical "cards" must be used within a 20 second period to grant access.

j. Shall have the 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.

k. Shall support the "Latch mode" operation where the first card read unlocks the door and the second card read locks it.

l. Shall provide a mode of system operation that stores system commands not accepted by the hardware.

m. Shall provide a mode of system operation that requires the operator to enter a response to an event when acknowledging it from the alarm view window.

n. Shall provide a mode of system operation that allows acknowledged alarms to be automatically cleared.

o. Shall provide a mode of system operation where when an acknowledged, but not cleared event will be reissued requiring acknowledgement when the event changes to an alarm or trouble state.

p. Shall provide a mode of system operation that does not allow the operator to clear an alarm before prior to it being restored to normal.

q. Shall provide the ability for manual operator control of system output relays. The manual functions shall include the ability to energize, de-energize, return to time zone, or pulse the output relay. The pulse time shall be a programmable setting.

r. Shall provide the ability for manual operator control of system doors. The manual functions shall include the ability to Lock, Un-Lock, Disable, Card only, Card-Pin only, Pin only, exit only and site code only.

s. Shall provide the ability to 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.

t. 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.

u. Shall support 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).

v. Shall provide an option for taking scheduled automatic backups of any or all database system files. A means to restore these files from a simple menu shall exist.

w. Shall provide the ability to address up to 255 serial communication ports per communication server, where each port can be configured for either hardwired, or dial-up. When configured for dial-up, any one port can support multiple dial-up locations.

x. Communication from the access control communication server to the remote intelligent control panels shall be selectable. Communication options shall be 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. When using IP addressing it shall be un-acceptable 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.

y. All commands and updates to the panels shall be verified and shall automatically retry if communications fail.

z. Shall provide a system scheduler that shall automatically: Call 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 reader(s), 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.

aa. Shall provide drop boxes for all system-required information that the user has previously entered.

bb. Shall provide the ability to initiate an email (via SMTP using SSL and TLS services) or page to a paging system based on a transaction state. A transaction state shall be 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.

cc. Shall include a "host grant" mode of operation that requires the host computer to grant accesses 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.

2. SubAccounts

a. An extension of the Accounts feature, Sub-Accounts 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.

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

3. Cards

a. Shall provide 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.

b. Cardholder information shall include unique card number up to 20 digits and optional Personal Identification Number up to 10 digits.

c. Shall allow multiple cards, mobile access credentials or finger print enrollment per cardholder.

d. Shall 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.

e. Shall provide 40 user defined fields.

f. 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.

g. Provides special card options that shall 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.

h. Shall provide a card "Trace" function. The Trace function shall allow normal access control, but will provide a tracking alarm at the system monitor.

i. Shall provide the ability to store digital images of cardholder or other digital images such as property or family members. Up to 99 such images shall be associated with the cardholder.

j. Shall provide the ability to store a written signature of the cardholder or other signatures such as family members. Up to 99 such signatures shall be associated with the cardholder.

k. Shall provide the ability to prioritize specific card event types from 1 to 99 with separate priority options that shall include but not be limited to Anti-pass back, Trace, PIN Violation, Normal, Not Found, Expired, Host Grant, Site Code and Time Zone card activities or violations.

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

m. Upon editing 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 shall be updated when connection is made to the remote loop. If the scheduler is used, then card updates shall be sent based on scheduling.

n. 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.

o. Duplicate Card numbers shall not be 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.

p. Integrated biometric enrollment functions shall be managed directly inside the PAC UI without the need to use a 3rd party software.

q. 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.

4. Access Levels

a. Shall provide an option to define specific access times.

b. Shall provide an option to define specific readers for access.

c. Shall provide a template of a defined access level detail, where changes can be made to the template and saved as a new access level detail.

d. Shall provide an access control tree structure that allows groupings of entrances. User shall have the ability to group program all entrances on the branch or make specific changes to individual entrances.

e. Shall provide an 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 applications.

5. Video Management Server

a. Shall support the following Digital Video Recorders (DVRs): ADPRO, MAXPRO NVR, and ENVR.

b. Shall provide an option to configure the DVRs to a video management server.

c. Shall provide an option to configure the cameras, inputs, and outputs to the DVRs.

d. Shall provide an interface to a network of digital video servers.

e. Shall provide an option to discover all the cameras connected the DVRs.

f. Shall provide the ability to manually access live video from any camera on any defined digital video server.

g. The viewer windows shall allow at least 64 live videos to be displayed at one time.

h. The viewable size of the viewer salvo window shall be adjustable by using the common "click and drag" method. When adjusting height or width, the image shall retain the correct aspect ratio.

i. Shall provide the ability to automatically pop-up any camera in the system based on any alarm point, system alarm or cardholder video image pop-up.

j. Shall provide the ability to manually control the pan, tilt, and lens functions (zoom, iris, and focus) of cameras so equipped.

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

l. Live views shall allow for the change in image resolution or aspect ratio to optimize the viewing quality to the native video.

m. The ability to change the size and location of the view shall exist.

n. The digital video server window shall also supply the ability to select a digital video server, camera, live, from stored video using user defined time and date.

o. A filter option shall allow the operator to define a date, time, transaction type, device(s), card holder, card number, note field, card event type and alarm status. Once filtered all events will be displayed in a listing. The listing shall include on the same event line if the event has an associated video clip. 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.

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

6. Camera control

a. Shall provide an option to configure the settings of cameras connected to the respective DVRs.

b. Shall provide an option to manually control the pan, tilt, and lens functions (zoom, iris, and focus).

c. Shall provide an option to automatically switch any camera in the system to any monitor in the system based on any alarm point or system alarm.

d. Shall display the live and recorded video in salvo window.

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

f. Shall provide an option to configure the Video Motion, Video Loss, and PTZ loss events to cameras associated to all the DVRs.

7. Alarm Monitoring – Alarms Only View

a. Shall report alarm point activity.

b. Shall provide color for each specific alarm point action, "Alarm", "Normal", and "Trouble", conditions.

c. Shall provide the ability to access the default floor plan graphic for any active alarm point by a right click option.

d. Live video pop-up from the digital video server(s) shall follow the alarm event pop-up. The number of live camera views in the pop-up window shall be no less than 16. The live pop-up window shall allow the user to define the quantity of views from 1 – 64. The ability to adjust the size of the live pop-up window shall exist.

e. Shall provide ability to bypass alarms in the system.

f. Shall execute alarm notification in all modes of operation.

g. Shall provide ability to acknowledge any intrusion alarm, event alarm, system alarm, card, or reader activity based on priority.

h. Shall provide 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.

i. Shall provide 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.

j. Viewable alarms shall include but not be limited to access control related events such as Door Normal, Door Alarm, Door Trouble, Door Ajar; Card events such as 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 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.

k. Shall provide the ability for an operator to acknowledge and clear alarms from display. Prior to acknowledgment, the user shall 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.

l. Shall provide a display of the most current transactions in real time.

m. Shall provide the ability for dynamic alarm monitoring of alarm points in real time on the system computer's video display terminal.

n. Shall provide an alarm view filter that is structured as a tree allowing the operator to select individual devices or groups of devices to be viewed.

o. Shall provide a "System" alarm upon a loop integrity violation.

p. Shall provide a "Panel Not Responding" alarm if communication to a panel is lost.

q. Shall provide 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.

8. Alarm Monitoring/System Control – Tree View

a. Shall provide the ability for dynamic alarm monitoring of alarm points in real time on the system computer's video display terminal.

b. Shall provide color and icon shapes for each specific alarm point action of "Alarm", "Normal", "Trouble", and "Shunted".

c. 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.

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

e. Shall provide an option to launch a Virtual keypad from an intrusion panel partition to monitor the physical keypad remotely and to administer programming changes via the Virtual keypad.

f. The control tree shall be created by the user and allow for manual of 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 & 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. 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.

9. Operator Database

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

b. Shall have the ability to view, edit, or delete cardholder sensitive information such as note fields, card number, and PIN shall be definable by field per operator.

c. Shall provide the ability to define the accounts that the operator has access to.

d. Shall provide the ability to log operator actions in the history files.

e. Shall provide the ability to select the default language during operator logon.

f. Shall provide specified time periods for the operator to logon

g. Shall provide the ability to select if access to the Web browser is allowed.

10. Access Control Panels

a. Shall provide ability to program Action Messages and assign an alarm event priority. A specific action message 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 shall include but not be limited to: Incorrect 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, VIP card Found. 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, 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.

b. Shall provide the ability to program descriptions, shunt times, and momentary shunt times for all system alarm points.

c. Shall provide ability to program descriptions, pulse times, and energize times for all system output relays used for door control and other auxiliary functions.

d. Shall provide the ability to program descriptions for all system card readers.

e. Shall monitor both 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.

f. Shall provide the ability to interlock any alarm point condition to an output relay.

g. Shall provide the ability to interlock any alarm point condition to another alarm point.

h. Shall provide the ability to interlock any alarm point to switch a camera to a system monitor.

i. Shall provide ability to program alarms and associate incoming alarms with related outputs.

j. Shall provide 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.

k. Shall allow 8 different site codes to be used in the system.

l. Shall support 32 readers per Intelligent Control Module.

11. Reports

a. Shall provide Card holder report capability with filter options to define door(s) that a card holder has access to, reporting card holder name, Card(s), Access Level/schedules, Activation/Expiration. Available in the Browser and workstation.

b. Shall provide 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.

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

d. Shall provide a feature to generate a history report for an alarm point(s) state. An alarm point state shall be defined as Normal, Alarm, Trouble, or Ajar.

e. Shall provide a feature to generate a history report of system alarms. A system alarm state shall be defined by panel and include any of the following information: communication, ground fault, power, panel reset, low voltage, panel tamper, and loop communication.

f. Shall provide a feature to generate an ADV actions report, which provides information on how the system ADVs are configured including detailed/advanced video configurations.

g. Shall provide a feature to generate a history report for a card(s) state. A card state shall be 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, Not Granted and filter the report with defined reader location(s). Available in the Browser and workstation. Additional search criteria shall be available at the workstation to include cardholders that meet up to at least 3-note field restrictions.

h. Shall provide a feature to generate a history report for system operator(s) activities. The report shall include time, date, operator name the device associated with the action and the type of action performed by the operator. Activities shall include but not limited to: acknowledged and cleared transactions, camera control, door mode, door and relay control such as unlock, lock; door and input control such as shunt, Unshunt; login, logout, panel initialization, panel buffer and panel Unbuffer.

i. Shall provide complete database reporting of all data programmed into the system data files.

j. Shall provide an option to define how long a card holder has been in a defined area. This report shall allow the time to be accumulated representing an attendance report. The definable filters shall include time/date range, reader(s) definition, card number, card holder and note field. The output of the report shall allow sort options to include First Name, Last Name, Event Time, and Card Number. The sorted data shall be selectable as Alpha or Numeric sorting and Ascending or Descending.

k. Shall provide feature to generate a report based on the frequency of usage of a card. The report shall allow the operator to 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. This report shall be available in the Browser and Workstation. Further a Workstation shall also provide a disposition function. The cards meeting the filtering criteria shall be acted upon based on the disposition setting. Disposition settings shall include but not be limited to: Report only, De-activate the card or Re-assign to a specified an access level. This report shall 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.

l. Shall provide an option to create report templates. Report templates available in the Browser and Workstation shall include, but not be limited to, Access Level, Card, Card History, Door, Holiday, Time Schedules and Card Holder information. The templates shall be able to be assigned to a scheduler to run automatically per the scheduler settings.

12. Tracking/Muster Report

a. A tracking feature shall allow the system operator to identify an area and the person(s) in that area.

b. Areas shall be defined by readers representing an IN or OUT read status.

c. Defined areas shall provide an automatic update of how many cardholders are in the area.

d. An area defined as an exit shall remove the person from the tracking area.

e. A view displaying all cardholders in a defined tracking or muster area shall have the ability to be sorted in columns where by 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.

f. A Muster area shall be defined by a reader(s) used to “muster” individuals in the event of an emergency.

g. Reports can be generated for the defined muster or tracking area. Available in the Browser and Workstation.

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

i. Tracking and Muster report template(s) shall be defined including whether it should be emailed and/or printed base on Event(s), Schedule(s) or assigned to a "Hot key" on the tool bar to be manually run when needed.

j. Reports shall be sorted 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.

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

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

m. 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.

13. Time Zones

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

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

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

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

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

f. Holidays shall be grouped in a Holiday Group.

14. Floor Plan Graphic

a. Shall provide the ability to import floor plan graphics stored in a WMF format.

b. Shall provide the ability to associate all ADV's (access, intrusion, and video) to floor plan graphics allowing the user to control and monitor the system.

c. Shall provide the ability to link floor plan graphics together in a hierarchy fashion.

d. Shall allow multiple floor plan views to be displayed simultaneously.

15. Remote Locations

a. Shall provide the ability to communicate to panels in real-time via encrypted Ethernet communication or support remote dial-up locations. Dial-up locations shall support the ability to place remote control panels in an offline mode. In the offline mode, the remote-control panels shall retain all panel history events. The number of historical events shall be limited to the panels' buffer capacity.

b. Shall provide the ability to place remote control panels in an offline mode where the remote panel will automatically call to the communications computer to report system alarms or upload buffered events.

c. Shall provide the ability to manage at up to 250 remote locations per communication server.

d. Shall provide a user-defined schedule that will automatically add cards to any number of sites.

e. For remote panels not configured for real-time communications, the ability shall exist to provide system time schedules that the computer will use to automatically start uploading or downloading information to the remote sites. Information to be sent to the panel shall include, but not be limited to, card database changes, time, date, and buffer condition. Information received from the panel shall include 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.

f. For remote panels not configured for real-time communications the remote site can also be supported via an auto dial schedule and shall allow the system to automatically dial the remote site at a predetermined time. The auto dial schedule is programmed with the ability to dial Once, Now, Hourly, Daily, Weekly, Two Weeks, Monthly, or Never to the remote site.

g. Shall provide the ability for an operator to program when the next scheduled update will occur, based on time and date.

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

i. The System shall be able to receive or send information to remote access control panels on demand.

j. Shall have the ability to configure how many redial attempts from the remote location shall be defined from 1 to 5.

k. Shall have the ability to pause between redial attempts shall be programmable from 1 to 120 seconds.

l. Shall have the ability to pause before disconnecting shall be programmable from 1 to 30 seconds.

16. Guard Tour

a. Guard Tour shall allow the operator to program a series of guard check points that must be activated to accomplish the task of a Guard Tour.

b. The check point shall be either reader points or alarm contact points or a mixture.

c. The Guard Tour shall be timed sequential allowing travel time between points with +/- tolerance. This type of tour shall allow alarms to be generated for early, missed, or late events.

d. The Guard Tour shall be un-sequenced with no time parameters.

e. The Guard Tour shall be started by two methods, Manual or Scheduled by the access control system scheduler.

17. ID Badging System/Video Image System

a. Shall allow any card data fields to be assigned to a badge.

b. Shall allow a stored cardholder image to be associated to any background. Each cardholder shall have any one of the background layouts associated to it.

c. Shall provide the ability to create temporary or permanent badges.

d. Badges shall be printed via the workstation without the need to assign an access level or access control card number. Numbers and access levels may be assigned after the print process.

e. Badges shall be printed via the browser after a card number has been assigned to the CardHolder.

f. Shall provide the image export capability. Image shall be exported utilizing the cardholder's name as the file name in .jpg format.

g. Shall provide unlimited custom badge layouts (only limited by the hard disk capacity).

h. Shall provide 24-bit (16.7 Million) color palette for background design or foreground text.

i. Shall provide the ability to implement all fonts supported by Windows.

j. Shall provide import capabilities of background information using video camera or BMP, JPG, or TGA files.

k. Shall provide import capabilities of video images from the compatible BMP, JPG, PCX, or TGA file formats.

l. Shall provide the ability to import multiple bitmap images to the badge layout.

m. Shall provide video capture capability from a compatible TWAIN device.

n. Shall provide video capture capability from a DirectX device.

o. Shall provide video capture capability from a compatible video capture device, such as a high-resolution color camera.

p. Shall provide badges in horizontal or vertical format.

q. Shall provide capability for printout of cardholder badge by video or standard printers supported by Windows.

r. Shall provide ability for multiple card enrollment/badging stations on networked system.

s. Shall allow text fields limited to a maximum of 255 characters per field.

t. Shall allow merging of data field from card database to text field.

u. Shall allow a field to be defined for bar code usage merging data from the card database.

v. Shall allow 99 different photos of the cardholder to appear on the same badge.

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

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

y. Shall provide the capability to have a front and back layout selected for a cardholder and the ability to print the card in one step (requires suitable printer) without the need to reinsert the card.

z. Shall provide the ability to encode a magnetic stripe with information from any of the card data fields to include, but not be limited to: First Name, Last Name, Card Number, Activation date, Expiration Date, or any data from the card holders note field.

aa. Information shall be encoded on track 1, 2, or 3 (requires suitable printer) without the need to reinsert the card. With suitable printer, each track shall be encoded with ABA, IATA, or TTS format.

18. Networking

a. Shall provide networking capabilities (LAN or WAN) as allowed by the computer's operating system license.

b. The access control software shall support two networking methods. By default, Domain controlled networks shall be the standard configuration providing secure networking communications. The ability to work on less secure peer-to-peer (Workgroup) networks shall be allowed for lower security installations. The functionality shall be one or the other and not run in both modes at the same time.

c. Shall provide the ability for a network system 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).

d. The workstation shall have the same user interface functionality as the Server, except the workstation shall not be able to perform database maintenance functions.

2.4 ISMS Hardware and Software Requirements

A. The ISMS shall be installed in 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; Workstation(s) 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 Microsoft Windows® SP1; Windows 10 (64-Bit) for workstations

12. Database: Microsoft SQL Server 2016 Express Edition

B. The ISMS shall be installed in 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 (60GB 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

C. The ISMS 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: 1TB 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

2.5 HARDWARE REQUIREMENTS

A. INTELLIGENT CONTROLLERS

1. Distributed architecture shall allow controllers to operate independently of the host. The architecture shall place key access decisions, event/action processing, and alarm monitoring functions within the controllers, eliminating degraded mode operation.

2. Flash memory management shall support firmware updates and revisions to be downloaded to the system. Upgrades to the hardware and software shall occur seamlessly without the 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:

a. Honeywell NetAXS Controller (NetAXS-123 and NetAXS-4 are the two types of NetAXS controllers)

b. Honeywell P-Series Controller (PRO-3200, and PW-6000 are the types of P-Series controllers – Legacy support for PRO-2200, PW-5000) PRO-3000 (APAC regional panel)

c. Honeywell N-1000 or PW-2000 Controller (Legacy support)

d. Honeywell Security NS2 or NS2+ (Legacy support)

e. Honeywell FIN-4000 Panels (HON-FIN4000MIK-100K, , HON-FIN4000AC-100K, , FIN4000K-10K, FIN4000-10K and FIN4000K-20K)

B. FIELD HARDWARE

NOTE TO SPECIFIER: Select the appropriate components and delete the others as necessary.

1. The security management system shall be equipped with access control field hardware required to receive alarms and administer all access granted/denied decisions. All field hardware shall meet UL requirements.

2. Intelligent Controller Board

    a. Honeywell Security PRO32IC

3. Single Reader Module (SRM)

    a. Honeywell Security PRO22R1

4. Dual Reader Module (DRM)

    a. Honeywell Security PRO32R2

5. Alarm Input Module (AIM)

    a. Honeywell Security PRO32IN

    b. 16 Inputs 2 Outputs

6. Relay Output Module (ROM)

    a. Honeywell Security PRO32OUT

    b. 16 Outputs 2 Inputs

7. Card Readers

    a. Proximity

    b. Magnetic Stripe

    c. Wiegand

    d. Barcode

    e. BLE

2.6 SYSTEM INTERFACES

A. Digital Video Recording Systems

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

2. WIN-PAK shall support the following Digital Video Recorders (DVRs).

    a. ADPRO

b. MAXPRO NVR

c. ENVR

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

3. Manufacturer(s) and part numbers:

a. Honeywell MAXPRO® NVR recorders

b. Honeywell ADPRO

c. Honeywell ENVR

B. Access Control Panels(Controllers)

a. Honeywell N-1000 or PW-2000 Controller, Honeywell NS2, NS2+ Controller, Honeywell P-Series Controller (PRO-2200, PRO-3000, PRO-3200, PW-5000, and PW-6000 are the types of P-Series controllers), Honeywell NetAXS Controller (NetAXS-123 and NetAXS-4 are the two types of NetAXS controllers), Honeywell FIN4000 Panels (HON-FIN4000MIK-100K, HON-FIN4000AC-100K, , FIN4000K-10K, FIN4000-10K and FIN4000K-20K), Honeywell MPA2 Panel + Controller.

1. N-1000 Series Panels (Legacy) shall have the following capabilities:

a. Stores 5,000 cards/key codes, expandable to 25,000 with memory upgrade.

b. Supports ABA and WIEGAND card formats.

c. Stores eight format (software) commands, allowing use of cards with various bit structures and encoding schemes.

d. Supports an option to define 63 time zones. Each time zone shall include a start time, end time, day of week specification and holiday specification. Time zones may be assigned to cards via access levels to define when the card is allowed access. Time zones may be assigned to input points, to define when the input points are shunted (de-activated). Time zones may be assigned to output points (relays), to define when the output points are energized, for timed control of doors or devices.

e. Supports setting of panel options such as anti-passback, groups, and keypads for providing access for the readers, input points, and output points attached to the panel.

f. Supports the use of card readers in conjunction with keypads, in which users are required to enter a PIN, followed by a card, to gain access.

g. Supports an option to assign shunt times to input points, from 1-63 seconds, minutes, or hours, and debounce times to input points, from 1-255 seconds.

h. Supports an option to assign pulse times to output points, from 1-63 seconds, minutes, or hours.

i. Supports the option to interlock selected input and output points, in any combination. An interlocked input or output point shall act based upon a change of state from another input or output point.

j. Stores 32 relay group definitions. Each group may be controlled with the same options available for individual relays.

k. Supports an option to define 32 holidays, for override of normal system operation.

l. Supports the followings mechanical and electrical specifications:

(a) Mechanical specifications: Height: 14.6 inches (370mm), Width: 12.6 inches (320mm), Depth: 3.5 inches (89mm), Weight: 5.51 lb. (2.5kg).

(b) Electrical Specifications: 16.5VAC 50 VA or +24 VDC @ 1.25 Amps

2. NS2+ Series Panels (Legacy) shall have the following capabilities:

a. Stores 10, 000 cards/key codes. (NS2 = 2,000 cards/key codes)

b. Supports WIEGAND card format.

c. Stores eight format (software) commands, allowing use of cards with various bit structures and encoding schemes.

d. Supports an option to define 63 time zones. Each time zone shall include a start time, end time, day of week specification and holiday specification. Time zones may be assigned to cards via access levels to define when the card is allowed access. Time zones may be assigned to input points, to define when the input points are shunted (de-activated). Time zones may be assigned to output points (relays), to define when the output points are energized, for timed control of doors or devices.

e. Supports setting of panel options such as anti-passback, groups, and key pads for providing access for the readers, input points, and output points attached to the panel.

f. Supports the use of card readers in conjunction with keypads, in which users are required to enter a PIN, followed by a card, to gain access.

g. Supports an option to assign shunt times to input points, from 1-63 seconds, minutes, or hours, and debounce times to input points, from 1-255 seconds.

h. Supports an option to assign pulse times to output points, from 1-63 seconds, minutes, or hours. Output points can also report the change in state status in the same way an alarm point would. This provides added awareness of door operation in critical installations.

i. Supports the option to interlock selected input and output points, in any combination. An interlocked input or output point shall act based upon a change of state from another input or output point.

j. Supports an option to define 32 holidays, for override of normal system operation. Holidays shall be definable in two different holiday types thus allowing for different operational time definitions for each holiday type.

k. Supports the followings mechanical and electrical specifications:

(a) Mechanical specifications: Height: 14.6 inches (370mm), Width: 12.6 inches (320mm), Depth: 3.5 inches (89mm), Weight: 5.51 lb. (2.5kg).

(b) Electrical Specifications: 16.5VAC 50 VA or +24 VDC @ 1.25 Amps.

3. P Series Panels shall have the following capabilities:

a. Stores 50,000 cards/key codes for PRO-2200, stores 1 00,000 cards/key codes for PRO-3200/PW-5000/PW-6000.

b. Supports ABA and WIEGAND card formats.

c. Types of P-Series panels are: PRO-3200, PW-6000, and legacy PW-5000 and PRO-2200).

d. Eight SIO Boards are included in the PRO-2200 panel. A maximum of 16 SIO boards are supported by the PRO-3200 panel. 32 SIO Boards are included in the PW-5000 and PW-6000 panel. SIO boards enable extended input and output capabilities to the panel.

e. 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. The SIO Board types include 16-Zone Input/output (16 inputs, 2 outputs, and 0 readers), 16-Relay Output (0 inputs, 16 outputs, and o readers), 2-Reader I/O (2 inputs, 8 outputs, and 6 readers), and 1-Reader I/O (1 input, 2 outputs, and 2 readers).

4. NetAXS Panels shall have the following capabilities:

a. Types of NetAXS panels available are: NetAXS-4 panel and NetAXS-123 panel.

b. Panels (NetAXS-123 and NetAXS-4) are called as Gateway panels when added directly to the communication server.

c. NetAXS-4 Gateway panel supports the downstream devices feature. This feature shall extend the input and output capabilities of the NetAXS-4 panels.

d. NX4IN and NX4OUT

1) NX4IN is a 32 input and 0 output downstream add on device

2) NX4OUT is a 2 input and 16 output downstream add on device

e. Supports only the WIEGAND card format. The NetAXS panel allows multiple sets of card numbers and site codes embedded in a card format. These multiple embedded sets will be represented as A, B, C, and D sets of card numbers and site codes. The A set shall be used as the default / primary card and site code numbers. The resulting maximum length of the card number will be 64-bits in length (20-digit card number). This is the reason that the system defaults will incorporate the ability to select a 20-digit card number size in addition to the existing 5, 12 and 16 digits

f. Supports 128 time slots and 255 holidays (per holiday group). Holidays shall be definable in three different holiday types thus allowing for different operational time definitions for each holiday type. The NetAXS panels shall have a provision to add a new time zone while within the panel database. After creating the new time zone, it shall be added to the Time Zones database and applied to the panel's database.

g. 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 NetAXS panels.

h. NetAXS-4 panel shall allow configuring of 14 inputs with default values. NetAXS-123 panel shall allow configuring 17 inputs with default values.

i. NetAXS-4 panel shall allow configuring of 16 inputs with default values. NetAXS-123 panel shall allow configuring 14 inputs with default values.

j. NetAXS-4 panel shall support 4 readers. NetAXS-123 shall support 6 readers controlling 3 doors where the "A" reader is the primary reader for the door and the "B" reader is the Out reader for the door when so used. The B Reader can be programmed separately regarding name, Advanced Options, Anti-Passback configuration, and Intrusion support. The B Reader cannot work alone as a Reader only. When used, the B reader will be tied to the A reader in terms of the interlock relationships pertaining to Door operation. The Advanced Options selection shall provide several advance features not normally used in the typical system and thus the reason they are accessed separately to reduce confusion for typical installations. For the NetAXS-123, Reader A and Reader B shall support their own settings.

k. The Groups option shall be supported only by the NetAXS-4 panels. A maximum of 64 groups shall be defined with a maximum of 76 relays.

5. HON-FIN4000 Panels shall have the following capabilities:

a. Type of HON-FIN4000 panels available are: HON-FIN4000MIK-100K, HON-FIN4000AC-100K, and legacy FIN4000K-10K, FIN4000-10K and FIN4000K-20K Panels

b. HON-FIN4000 work as standalone or as an access control panel/biometric reader directly supported by the PAC (WIN-PAK software) or as a biometric reader using the Wiegand interface to other supported access control panels.

c. HON-FIN4000AC-100K supports 125kHz EM, HID Prox & 13.56Mhz MIFARE, MIFARE Plus, DESFire/EV1, FeliCa, iCLASS SE/SR/Seos card technologies; 500,000 users (1:1) or 100,000 users (1:N)

d. HON-FIN4000ACK-10K supports 125kHz EM, HID Prox & 13.56Mhz MIFARE, MIFARE Plus, DESFire/EV1, FeliCa, iCLASS SE/SR/Seos card technologies; 10,000 users (1:1) or 10,000 users (1:N); 1.77" color TFT LCD; 160 x 128 pixels

e. Supports 128 time slots and 255 holidays (per holiday group). Holidays shall be definable in two different holiday types (H1 and H2), thus allowing for different operational time definitions for each holiday type.

f. Panel options such as Anti-passback, Groups, Forgiveness, Host Grant, Site Codes, and Command File can be set for providing access to the readers, input points, and output points attached to the panel.

g. HON-FIN4000 shall allow configuring of 3 inputs with default values.

h. HON-FIN4000 panel shall support an additional Wiegand reader for in/out management.

6. MPA2 Panels shall have the following capabilities:

a. MPA2 Panel is called as Gateway panels when added directly to the communication server.

b. MPA2 Panel supports the downstream devices feature. This feature shall extend the input and output capabilities of the MPA2 Panel.

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

d. Supports 128 time slots and 255 holidays (per holiday group). Holidays shall be definable in three different holiday types thus allowing for different operational time definitions for each holiday type. The MPA2 panels shall have a provision to add a new time zone while within the panel database. After creating the new time zone, it shall be added to the Time Zones database and applied to the panel's database.

e. 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.

f. MPA2 panel shall allow configuring of 24 inputs with default values.

g. MPA2 panel shall support 4 readers.

C. Intrusion Detection Panels:

1. Honeywell VISTA-128FBPT, VISTA-250FBPT, VISTA -128BPT and VISTA-250BPT

a. General Requirements: The Security Management System shall 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:

1) Disarm and unlock a door on card swipe.

2) Arm and lock a door on card swipe.

3) Common area arm/disarm.

4) Access denied if intrusion system is in alarm or armed.

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

6) Associate intrusion system events and alarms to video surveillance integrations.

2. 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.

   a. 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:

      1) Disarm a zone on a card swipe.

      2) 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.

      3) Security Management System supports linking of intrusion panel users with Security Management System cardholders.

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

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

      6) Security Management System stores and reports on intrusion events.

PART 3 EXECUTION

3.1 EXAMINATION

A. 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.

3.2 INSTALLATION

A. Integrated Security Management System, including but not limited to access control, alarm monitoring, CCTV, and ID badging system shall be installed in accordance with the manufacturer's installation instructions.

B. 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 Security Management System.

3.3 FIELD TESTING AND CERTIFICATION

A. Testing: The access control, alarm monitoring, CCTV, and ID badging system 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 Security Management 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.

END OF SECTION