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

2. Underwriters Laboratories (UL):

a. UL294 – Access Control System Units

3. Electronic Industries Alliance (EIA):

~~a.~~ RS485 – Electrical Characteristics of Generators and Receivers for OSDP devices connection

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 a two year period for Owner's review.

1.6 QUALITY ASSURANCE

A. Manufacturer: A minimum of ten years' experience in manufacturing and maintaining Security Management Systems.

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, and smart/intelligent cards.

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

C. Access Level: The door or combination of doors and/or barriers an individual is authorized to pass through made up of zones and constrained by time periods.

D. Anti-Pass back: 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.

E. Alarm: A signal that indicates a problem.

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

G. Badge: Badge is a template or a design for creating a card. EBI 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.

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

I. 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).

J. 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.

K. Cardholder Management System: A database of the personnel and visitors stored in a relational database on the ISMS.

L. 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.

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

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

O. Digital Video System (DVS): A Closed Circuit Television (CCTV) security system that records the video from surveillance cameras (IP and Analog via digital encoders) onto a hard disk(s) located on a storage server and/or other storage media (NAS, DAS, SAN etc).

P. Door: A generic term for a securable entry way. In many access control applications a "door" may actually be a gate, turnstile, elevator door, elevator floor, or similar portal through which one controls or monitors passage.

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

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

S. Host Computer: The central controlling computer, typically a server class machine, from which access control software applications are run.

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

U. 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.

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

W. 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.

X. 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 physical device that a user must interact with to allow access. Readers can be keypads, card readers, proximity readers, and so on.

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

Z. Server: The host computer, which contains ISMS software and database and provides a centralized communication to and from field devices and user interface clients (stations).

AA. 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.

BB. Time periods: "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. Also used to limit when a card may access a particular zone within an access level.

CC. 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.

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

EE. Zone: a logical grouping of access controlled doors.

FF. Video Management System (VMS): Also commonly known as Digital Video System (DVS),An enterprise-class video management and storage solution.

GG. RS485: A serial communication protocol used for connecting readers, support long distances (up to 500ft generally supported)

HH. OSDP: Open Supervised Device Protocol (OSDP) is an access control communications standard developed by the Security Industry Association (SIA) to improve interoperability among access control and security products. OSDP V.2 enables encrypted communications

II. End-To-End Encryption: End-to-end encryption is intended to prevent data being read, other than by the true sender and the designed receiver. End-To-End encryption ensures that what is delivered is exactly what has been sent from card to host and vice-versa.

JJ. Feedback: It’s the ability to execute an action or a sequence of actions on some devices as a consequence of a status change on the same device or on other devices. Feedback can also be manually activated or scheduled.

PART 2 PRODUCTS

2.1 MANUFACTURER

1. Integrated Security Management System Manufacturer: Honeywell Enterprise Buildings Integrator (EBI) Version 600 or greater.

2. Honeywell s.r.l.

2.2 ISMS COMPONENTS

The ISMS shall be divided into three components: Database Server, Point Server(s), and User Interface (Client Stations). 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. Point Server: The point server routes data updates to the access panel(s), as well as, receives access transactions from the access panel(s). The point server shall be installed on the EBI Server computer.

c. User Interface (ISMS Client): The graphical interface helps ISMS operators to communicate with the access control system. The user interface is installed on the computer where the database server or the point server is installed and/or any other computer connected to the network. Many 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. Client connections are licensed by connection not by seat.

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, paging, digital video/CCTV integration 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 interoperable software suite and shall provide full integration of all components. It shall be alterable at any time depending upon facility requirements, subject to licensing 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 a message when the client is unable to communicate with the server. The operators on the network server shall have the capability to log on to workstations

and remotely configure the devices for the workstation via remote desktop. Standard operator permission levels shall be enforced, with full operator audit.

2. Operating Environment: The ISMS shall be a true 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 (64 bit),SQLServer 2017

3. Multiple Servers: The ISMS may consist of multiple servers including, but not limited to, database server, fire point server, building automaton point server, digital video manager point 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, known as a Distributed Server Architecture (DSA). The ISMS may support multiple database and/or point servers on a LAN/WAN via DSA, to provide distributed networking and load sharing capabilities, which significantly improve system performance. Server redundancy with automatic failover to provide fault tolerance is available as a licensed option.

4. 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.

5. Graphical User Interface: The ISMS shall be fully compliant with Microsoft .NET, Internet Explorer and associated graphical user interfaces, with the look and feel of the software being that of a standard Windows application.

6. 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.

7. 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 as long as the maximum number of concurrent connections purchased has not been exceeded. Microsoft SQL CAL licensing required.

8. Access Control Software Suite: The ISMS shall offer a security management software suite to include ID Badging, Alarm Monitoring, Cardholder Management, Paging interface as well as options for Building Management, Energy Management, UL Fire monitoring and control and mobile applications supported on tablets and smart phones.

9. 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 2017.

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

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

    a. True 256-bit AES data encryption between the host and intelligent controllers. 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.

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

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

14. Multiple location (Facility/Organization) Support: The ISMS application shall allow support for multiple facilities/organizations allowing separate access to the card database, badge layout, operator access, and reporting. Physical hardware may be filtered by operator level into facilities. The system shall allow control of common areas between facilities/organizations. Administrators shall have the ability to move cardholders from one facility/organization to another.

15. Logical Representation of Hardware Devices: The ISMS shall use graphical representation of devices (icons/symbols/shapes) for representing physical hardware devices in the system. The icons/symbols/shapes shall be used in Floor Plans to provide the user interface to control and monitor the system.

16. 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.

17. Digital Video System (DVS) Support: The ISMS shall support the Honeywell Digital Video Manager, video management system

18. Camera Functions: The DVS shall include the following camera functions: pan/tilt/zoom (PTZ), iris control, tours, privacy zones, record on camera movement (PTZ) background recording, recording by schedule, record on motion detection, and archiving of video data.

19. Live Video Display: The DVS shall provide a live video from a camera connected to the DVS 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.

20. Alarm Events: The ISMS shall include a feature where alarm events with defined priorities shall be able to 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, facility, if a card event the card number, type of event and cardholder name. 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. 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.

21. 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 for output points and shunt/unshunt for input points. For entrances and readers manual control shall include but not be limited to Lock, Un-Lock, Unlock Single Transition.

22. 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.

23. Distributed Database: All the control components of the ISMS shall utilize "Distributed-Database" 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.

24. 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 transactions shall be saved in a retrievable file.

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

d. All transactions shall be saved in the event database.

e. Anti-pass back modes shall include: hard (no forgiveness), soft (allows access but generates an alarm event), in peer-to-peer within controllers.

f. 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.

g. 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.

h. 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.

i. 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.

j. Shall provide the ability for manual operator control of system output relays via defined group summary views or via graphical representation. The manual functions shall include the ability to energize, de-energize the output relay.

k. Shall provide the ability to automatically display stored cardholder ID photo, and switch real-time camera from CCTV or digital video server to card reader location for specific card usage.

l. 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. The size of the pop-ups shall be adjustable by the operator.

m. 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, mobile reading.

n. Shall support multiple reader communication technologies including: Wiegand, LON and OSDP.

o. Shall support daily scheduled automatic backups of all database and system files.

p. Communication from the access control communication server to the remote intelligent control panels shall be LAN/WAN using an IP address for direct connection to the intelligent controller via embedded network interface card. All commands and updates to the panels shall be verified and shall automatically retry if communications fail.

q. Shall provide the ability to initiate an email, SMTP message or page to a paging system based on a defined transaction state.

2. Cards

a. Shall provide a 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 and Photo Images.

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

c. Shall allow multiple cards per cardholder.

d. Shall allow unlimited behavior models to be assigned to a card, the limit is determined by the memory of the controller.

e. Shall provide unlimited user defined fields.

f. Each card holder note filed 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.

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), 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.

j. Shall provide the ability to store a written signature of the cardholder or other signatures such as family members.

k. Upon editing card information, the updated information shall be sent automatically to the appropriate access control panel, when hardwired, with no other user intervention.

l. Cards shall have the ability to be allowed to access one or selected facilities up to all available facilities controlled by access level(s).

3. Behavior Models

a. Shall provide specific access times as associated with readers, time periods and weekdays.

b. Shall provide the possibility to duplicate a behavior model, where changes can be made saved as a new behavior model.

4. Video Management Server

a. Shall support the following Digital Video Systems (DVS): Digital Video Manager from Honeywell.

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

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

d. The viewer windows shall allow at least 16 live videos to be displayed at one time.

e. 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.

f. 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 as defined in the automation rules section.

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

h. 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.

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

j. 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.

k. 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.

l. Shall provide for video wall integration and/or multi-monitor viewing and control via simple keyboard commands.

m. Shall provide for the option of dedicated alarm monitors for full screen viewing of live video triggered by motion or via automation rules as defined in the ISMS.

n. Shall provide the ability to start the recording, to change the camera preset and present the live camera image on a specific monitor via feedback, based on an alarm/event.

5. Camera control

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

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 a console window.

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

6. Alarm Monitoring – Alarms Only View

a. Shall report alarm point activity.

b. Shall provide color for each specific alarm point action, Low, high, urgent conditions.

c. Shall provide the ability to access the default floor plan graphic for any active alarm point.

d. Live video pop-up from the digital video server(s) shall follow the alarm event in the ISMS.

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 clip icon for events in the alarm and event history windows that have video associated with them. Double-clicking on video clip icon associated with the event shall allow the recorded video associated with the event to be viewed in a popup window. The stored video clip shall playback actual event without any adjustment. If pre-record was selected in the video setup, the operator shall have the ability to adjust the timeline to allow viewing of the events leading up to the alarm event.

j. Shall provide the ability for an operator to acknowledge and clear alarms from the alarm display window. 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.

k. Shall provide a display of the most current transactions in real time and filter events by day, date and or time.

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

m. Shall provide an alarm view filter allowing the operator to select: all facilities, individual facilities, and filter on screen data.

n. Shall provide a "System" alarm upon a communication failure.

o. Shall provide a "communications marginal and communications failed" alarm if communication to a panel is lost, value to be adjustable based on communications barometer settings.

7. Alarm Monitoring/System Control

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

8. 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 operator.

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

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

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

9. Access Control Panels

a. Shall provide the ability to program descriptions for all system alarm points.

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

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

d. 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.

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

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

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

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

i. Shall allow up to 20 different site codes/card formats to be used in the system.

j. Shall allow peer-to-peer communication within different Intelligent Controllers.

k. Shall allow end-to-end encrypted communication with automatic and randomic change of key every max 2 hours.

l. Shall support OSDP protocol with encrypted communication Version 2(2.1.7)

10. 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.

    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.

    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.

    d. Shall provide a feature to generate a history report for an alarm point(s) state.

    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 network communication.

    f. 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-Pass back Violation, PIN Violation, Time Zone Violation, Site Code Violation, or Expired card.

    g. 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.

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

    i. Shall provide an option to create report templates. Report templates shall include, but not be limited to, History and Card Holder information. The templates shall be able to be assigned to a schedule to run automatically per the schedule settings.

11. 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 24-hour (military) time or 12-hours (AM/PM)

c. The minimum time period that shall be assigned to a panel is 1 (always on).

d. The maximum time periods that shall be defined in a system is 32 per site.

e. The ISMS shall provide for Global Schedules that can be utilized in addition to time periods to schedule events system wide.

f. Holidays shall be defined in different time zones based on the site allowing different time schedule to be programmed for each holiday type.

g. Holidays shall be grouped in a Holiday Group (site calendar).

12. Floor Plan Graphics

a. Shall provide the ability to import floor plan graphics.

b. Shall provide the ability to associate all devices (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 provide a menu structure for direct selection of graphic pages.

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

13. Remote Locations

a. Shall provide the ability to place remote control panels in an offline mode. In the offline mode, the remote control panels shall retain panel history events. The amount of historical events shall be limited to the panels' buffer capacity.

b. Shall provide the ability to manage at least 99 remote locations per server.

c. Communication to all sites shall be customers LAN/WAN and accomplished through the use of password protection and AES 256 bit encryption. No commands or transactions occur until the communication link is verified.

14. 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 without the need to assign a behavior model or access control card number. Numbers and behaviour models may be assigned after the print process.

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

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

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

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

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

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

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

l. Shall provide video capture capability from a compatible USB camera

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

n. Shall provide badges in horizontal or vertical format.

o. Shall provide capability for printout of cardholder badge by industry standard dye sublimation printers or standard printers supported by Windows.

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

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

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

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

t. Shall provide signature capture or import capability for signatures that can be previewed in the cardholders badge or printed on the cardholder's card.

u. 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.

v. 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, direct to the ID printer.

w. 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.

x. System shall allow for integration to visitor management systems: Reception Manager, Easy Lobby, Right Crowd.

15. 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 on a server class computer. The minimum hardware and software requirements to fulfill this installation are:

1. Processor: Intel® Xeon® E-2124G Processor or equivalent.

2. CPU: 2.2 GHz or faster.

3. RAM: 16 Gigabytes (GB)

4. Hard Disk: 3 x 250 GB, recommended configuration:

a. Disk 1 Mirror for OS Use,

b. Disk 2 Raid 5 for SQL Database,

c. Disk 3 Raid 5 ISMS system software and associated files.

5. Network Ports: 2 (gigabit preferred)
6. DVD – ROM Dual Layered
7. Monitor Display: Size: 15 Inches SVGA, Resolution: Minimum 1280x1024 pixels; 65K colors
8. Pointing Device: Mouse (USB preferred)
9. Operating System: Microsoft Windows® Server 2016.
10. Database: Microsoft SQL Server 2017

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.
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. Tema-Voyager Multi Controller
   b. Temaline TS2 controller
   c. Tema-Voyager Compact controller with display and reader embedded

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.
2. Intelligent Controller Board
   a. Honeywell Temaline Tema-Voyager Multi controller in any of below variations:
      - VMC-01xENNy: Tema-Voyager Multi-1: 1 reader, 4 inputs, 4 Outputs, 8 configurable I/O

- VMC-02xENNy: Tema-Voyager Multi-2: 2 readers, 4 inputs, 4 Outputs, 8 configurable I/O
- VMC-03xENNy: Tema-Voyager Multi-3: 3 readers, 4 inputs, 4 Outputs, 8 configurable I/O
- VMC-04xENNy: Tema-Voyager Multi-4: 4 readers, 4 inputs, 4 Outputs, 8 configurable I/O
- "x" stays for:
  - W= with plastic enclosure
  - N= bare board
- "y" stays for:
  - 2=SAM ready
  - 3= model embedding SAM plug-in

b. TS2: Honeywell Temaline TS2 controller, supporting up to 16 doors with reader on both sides of the door.

c. VCU-xyz7015EN1N01: Honeywell Temaline Tema-Voyager Compact controller with graphic display and reader embedded.

- "xy" stays for reading technology that can be:
  - 01: HID prox 125KHz
  - 02: Mifare
  - 03: HID and Mifare
  - 30: Multi reading technology supporting all the below:
    - HID prox 125 kHz
    - Prox Indala
    - Prox EMarine/Unique
    - Mifare Classic
    - Mifare DESFire
    - Mifare DESFire EV1
    - HID Mifare Classic SE
    - HID Mifare DESFire SE
    - HID Mifare DESFire EV1 SE
    - HID iClass standard
    - HID iClass Seos

- "z" stays for the type of mount
  - W = wall mount
  - T = turnstile mount
  - S = swivel mount

3. Intelligent I/O module for Multi controllers
   a. VMC-00xENN1: 4 Inputs, 4 Outputs, 8 configurable I/O
      - "x" stays for:
        - W= with plastic enclosure
        - N= bare board

4. Relay output board for Multi controllers
   a. VMA-06: Honeywell Temaline Tema-Voyager Multi Relay Output Board, to be plugged in to Tema-Voyager Multi-0/1/2/3/4 controllers
5. Emergency Relay output board for Multi controllers
   a. VMA-07: Honeywell Temaline Tema-Voyager Multi Emergency Relay Output Board, to be plugged in to Tema-Voyager Multi-0/1/2/3/4 controllers
6. SAM plug-in for Multi controllers
   a. VMA-08: Honeywell Temaline Tema-Voyager Multi SAM plug-in board, to be plugged in to Tema-Voyager Multi-1/2/3/4 controllers
7. Intelligent I/O module for TS2 controllers
   a. TK_C21P: Digital I/O module. 4 supervised inputs and 4 open collector outputs.
8. Intelligent PSU module for TS2 controllers
   a. TP_U01: Power supply for Temaline devices. 10Watt/12Volts output with battery (included). 4 hours autonomy.
   b. TP_U03: Power supply for Temaline devices. 60Watt/12Volts output with battery (included). 4 hours autonomy.
   c. TP_U04: LonWorks Intelligent power supply controller. Allows the usage of external power supply as Temaline devices.

9. Card Readers

a. Temaline LON readers directly connected to TS2:

1) TK_L30: mullion style reader with multi reading capabilities.

2) TK_C30: compact style reader with multi reading capabilities, with 2 lines display and keypad.

3) TK_S014M: wiegand module to connect any wiegand reader.

b. Proximity, Low frequency Digi Reader, HID low frequency 125K, HID iCLASS SE SEOS 13.5Mhz or equal.

c. Magnetic Stripe

d. Wiegand

e. Barcode

f. Biometric

g. Mobile credential BLE.

h. Any combination of the above via multi-technology readers.

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 (DVS). The DVS shall record, search and transmit video, and shall provide users with live, pre and post-event assessment capabilities. The DVS shall be seamlessly integrated with existing video equipment and incorporated into any TCP/IP network. The DVS shall provide multiple levels of integration with the Security Management System software, providing control of the digital video system from the access control application.

B. Access Control Panels(Controllers)

1. Tema-Voyager Multi Panels shall have the following capabilities:

a. Shall allow wall or DIN rail mounting

b. Shall allow connection via POE or POE+ or 10-30Vcc external power supply

c. Support for WIEGAND card format.

d. A maximum of 4 readers supported

e. Shall allow to purchase the exact amount of access control doors immediately required, and to easily add more readers in the future, for a total of 4.

f. Shall support peer-to-peer communication with other Tema-Voyager Multi controllers, TS_AC01 and TS2 controllers, Tema-Voyager Compact controllers.

g. Shall support for 250,000 cardholders fully configurable

h. Shall support for 250,000 transactions fully configurable

i. Shall support for 65.000 events/alarms fully configurable

j. Shall support up to 32 Card Formats per controller

k. Shall support AES 256-bit encryption on LAN connection to host.

l. Shall store encryption-keys in Flash memory in encrypted mode

m. Shall support automatic and random change of encryption-keys within a timeframe that varies from 1 to 3 hours.

n. Shall support AES 256-bit encryption on peer-to-peer LAN connection to other Multi controllers

o. Shall support connection to readers via Wiegand or OSDP V1, or OSDP V2 secure channel, or OSDP V2 without encrypted communication.

p. Supports AES 128-bit encryption to OSDP V2 readers

q. Shall be ready to support mutual authentication communication with smart cards via OSDP transparent readers.

r. Shall allow optional SAM plug in with 3 tampers to detect:

    1) Multi controller opening

    2) SAM plug-in dismount

    3) SIM extraction

s. Shall support optional relay board to empower 4 outputs and directly manage the unlock of up to 4 doors depending from the current required by the locks.

t. Shall support optional emergency relay board to empower 4 output, to physically manage the unlock of doors in case of an emergency.

u. Shall support Threat management of up to 5 levels

v. Shall support Access control and T&A transits

w. Shall support end-to-end encryption, fully encrypted chain of communication from card reading up to supervisory level via OSDP-V2 secure protocol.

    1) All the keys used for encryption of communication or for data at rest encryption, are themselves stored in encrypted mode.

2) Every Multi controller has a different encryption-key to communicate with the supervisory level.

3) Every reader can have a different encryption-key to communicate with the controller.

4) The encryption-keys for communication between supervisory level and Multi are automatically and randomly changed within a timeframe of max 3 hours.

5) The encryption-keys for communication between Multi and readers can be regularly changed by the operator.

6) The system is protected from any unauthorized data capturing.

7) Each Multi defines its own encryption key to communicate to each reader, so in the worst option the breach is limited to max 1 door.

x. Shall support certified interface to SAP R/3 HR-PDC module

y. Shall support intrusion detection features on same controller of Access control, minimum the following ones:

1) To manage detectors with 4 different states: short, cut, normal, alarm.

2) To manage normal field point detectors.

3) To manage manual and automatic zones.

4) To allow arming and disarming a zone from supervisory center or in automatic based on a scheduled plan.

2. Temaline TS2 Panels shall have the following capabilities:

a. Support for WIEGAND card formats.

b. A maximum of 16 doors supported, with reader on both sides of the door

c. Shall support up to 16 doors via LON connection

d. Shall support for 250,000 cardholders fully configurable

e. Shall support for 250,000 transactions fully configurable

f. Shall support for 65.000 events/alarms fully configurable

g. Shall support IPSEC-3DES encryption on LAN

h. Shall support up to 32 Card Formats per controller

i. Shall support peer-to-peer communication with other Temaline TS_AC01, TS2, Tema-Voyager Multi and Tema-Voyager Compact controllers.

j. Shall support shared load: redundant paired controller to share the load of LON devices.

k. Shall support Threat management up to 5 levels

l. Shall support up to 64 I/O via LON

m. Shall support Access control and T&A transits

n. Shall support certified interface to SAP R/3 HR-PDC module

o. Shall support intrusion detection features on same controller of Access control, minimum the following ones:

1) To manage detectors with 5 different states: short, cut, normal, alarm, tamper of the detector.

2) To manage normal field point detectors.

3) To manage manual and automatic zones.

4) To allow arming and disarming a zone via a feedback initiated by a transit with associated reason, via a TK_C (LON reader with keypad and display).

5) To view zone status via an enquiry to a TK_C (LON reader with keypad and display) and arm/disarm the zone

p. Shall allow lift management of any lift brand via I/O, max 64 floors, suggested max 16.

q. Shall allow lift management via IP protocol to the following lift brand:

1) Kone GCAC Ver1.0

2) Kone encrypted protocol GCAC Ver3.0

3) Mitsubishi ELSGW

r. Shall allow high level lift management in one or more of below situations:

1) Management of car-lift panel for authorizing lift only to enabled floors for specific cardholders

2) Management of destination panel to optimize the personnel flow for a better user experience

3) Management of lift in conjunction with access turnstile to direct the employees on most appropriate lift

3. Tema-Voyager Compact controller shall have the following capabilities:

a. Shall allow connection via POE or to power supply

b. Shall embed in single device a fully autonomous controller, reading capability and graphic display.

c. Shall comply with IP65 for challenging environment

d. Shall support up to 4 languages on single controller

e. The display shall support oriental languages

f. Shall allow mounting in vertical or horizontal with possibility to adapt optimally the vision.

g. Support for ABA card formats to connect an external magnetic reader.

h. Shall support for 250,000 cardholders fully configurable

i. Shall support for 250,000 transactions fully configurable

j. Shall support for 65.000 events/alarms fully configurable

k. Shall supports IPSEC-3DES encryption on LAN

l. Shall support peer-to-peer communication with other Temaline TS_AC01, TS2, Tema-Voyager Multi and Tema-Voyager Compact controllers.

m. Shall have on board 2Inputs and 2Outputs to manage door.

n. Shall support external I/O module to extend number of I/O managed and to drive door management from secure area.

o. Shall support up to 32 Card Formats per controller

p. Shall support Access control and T&A transits

q. Shall support certified interface to SAP R/3 HR-PDC module

r. Shall support intrusion detection features on same controller of Access control, minimum the following ones:

    1) To manage detectors with 4 different states: short, cut, normal, alarm.

    2) To manage normal field point detectors.

    3) To manage manual and automatic zones.

    4) To allow arming and disarming a zone from supervisory center or in automatic based on a scheduled plan.

    5) To manage arm/disarm via the graphical display.

s. Shall support Muster functionality

1) Shall be independent from host availability

2) Shall be suited to be placed in outside area

3) Shall identify in real time the presence of zone of people in risk areas for a prompt rescue intervention

4) Shall allow identification of personnel in safe zones

5) Shall apply to employees, contractors and visitors

6) Shall allow to move cardholders in safe zone also without the need of the card.

t. Shall support interactivity

1) Shall be able to display customer logo

2) Shall support local and remote enquiries transits and on free data.

3) Shall support bulletin board

4) Shall allow to configure the format of date and time, (small/large characters, 12/24 hours, day/month)

5) Shall support Spontaneous Messages prompted to cardholders at transits.

6) Shall support Additional Data List to associate info to transits

u. Shall support T&A transits

1) Shall show date and time

2) Shall allow double direction on the same device

3) Shall allow change of the direction based on:

(a) Manual selection via function key

(b) Automatic change via time-plan

(c) Automatic change via an event

(d) Automatic direction via a reason

4) Shall allow full configuration of tool bar within a predefined set of icons

5) Shall allow simple transits as well as well as transits with associated reasons.

C. Intrusion Detection Panels:

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

a. General Requirements: The Security Management System shall support hardwired and TCP/IP communication for the VISTA 128BPT/VISTA-250BPT 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.

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