SECTION 281300

ACCESS CONTROL AND SECURITY MANAGEMENT SYSTEM

Table of Contents

DATE	In Section…	This is added or deleted…
	Section 2.2	Subsection about dongles is deleted.
	(B) FIELD HARDWARE > 7.f Wireless Readers	ADDED "ASSA ABLOY APERIO Wireless Reader" and "SCHLAGE Wireless Reader"
	(B) FIELD HARDWARE > 7.f Wireless Readers	CHANGED "SALTO Wireless Reader" to "SALTO SALLIS Wireless Reader"
	(B) FIELD HARDWARE > Mercury Family Hardware	CHANGED "CASI Micro 5 Bridge" to "Mercury M5 Bridge"
	2.5 SYSTEM INTERFACES	ADDED F. Web Client (a. Web Alarms, b. Web Events)
	2.5 SYSTEM INTERFACES	ADDED G. Supported Web Browsers
June 2017	**Hardware Requirements > Mercury Family Hardware**	ADDED Mercury MS Bridge and Mercury iSTAR Controllers
June 2017	**Security Management System Operational Requirements > System Operations**	ADDED h. Identity Management Portal
June 2017	**Field Hardware > Biometric Readers**	ADDED Morpho Wave Reader
June 2017	**Security Management System Operational Requirements >Encryption, Page 7**	ADDED d. OSDP Support
July 2017	**Page 9, Item "h"**	CHANGED language.
July 2017	**Page 12, Item "IV"**	Added "REST"
July 2017	**Page 15**	Formatting corrections. Content same.
July 2017	**Page 16**	ADDED a new list of MS panels.
March 2018	**Page 15, Item 15.d**	ADDED "IRIS ID Reader" to list of Biometric Readers supported on Page 15 (15.d).
March 2018	**Page 7, Item 6**	ADDED "Microsoft Azure" support.
Nov 2018	**Security Management System Operational Requirements > System Operations**	ADDED Email notification
Nov 2018	**(B) FIELD HARDWARE > Mercury Family Hardware**	ADDED Suprema
Dec 2018	**(B) FIELD HARDWARE > Mercury Family Hardware**	DELETED Suprema
Dec 10, 2018	**OPERATIONAL REQUIREMENTS > 2. > m. ID Badging System**	ADDED list of "UNIFIED BADGING/IDENTITY MANAGEMENT"
Dec 10, 2018	**2.4 HARDWARE REQUIREMENTS > B. FIELD HARDWARE**	ADDED list of "UNIFIED PHYSICAL ACCESS CONTROL SYSTEM"

DATE	In Section…	This is added or deleted…
Dec 10, 2018	**SYSTEM INTERFACES**	ADDED list of "UNIFIED ALARM MANAGEMENT SYSTEM"

GENERAL

SECTION INCLUDES

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

RELATED SECTIONS

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

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

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

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

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

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

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

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

REFERENCES

I. 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)

SECURITY MANAGEMENT SYSTEM DESCRIPTION

J. The Security Management System shall function as an electronic access control system and shall integrate alarm monitoring, CCTV, digital video, ID badging and database management into a single platform. Email notification must be supported. A modular and network-enabled architecture shall allow maximum versatility for tailoring secure and dependable access and alarm monitoring solutions.

K. FIPS Certification: The system shall support FIPS 201 certification.

SUBMITTALS

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

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

N. 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.

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

P. 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.

QUALITY ASSURANCE

Q. Manufacturer: Minimum ten-years of experience in manufacturing and maintaining Security Management Systems. Manufacturer shall be Microsoft Silver Certified.

NOTE TO SPECIFIER: Specify minimum level of DSCP certification: Silver, Gold or Platinum. Refer to https://www.honeywellintegrated.com/documents/L_DLRSVCPB_D_DSCP.pdf for specifics of each level.

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

DELIVERY, STORAGE, AND HANDLING

S. Store products in manufacturer's unopened packaging until ready for installation.

WARRANTY

T. Manufacturer's Warranty: Submit manufacturer's standard warranty for the security management system.

PRODUCTS

MANUFACTURER

NOTE TO SPECIFIER: Select the appropriate version(s) of Pro-Watch software, or designate that the contract should select the appropriate version based on the size and configuration of the system for this project.

U. Security Management System Manufacturer: Pro-Watch® Security Management Suite by Honeywell, www.honeywellintegrated.com. Provide the following software system:

1. Pro-Watch® Lite Edition.
2. Pro-Watch® Professional Edition.
3. Pro-Watch® Corporate Edition.
4. Pro-Watch® Enterprise Edition.

SECURITY MANAGEMENT SYSTEM SOFTWARE REQUIREMENTS

V. Software Requirements: The Security Management System shall be a modular and network-enabled access control system. The Security Management System shall be capable of controlling multiple remote sites, alarm monitoring, video imaging, ID badging, paging, digital video and CCTV switching and control that allows for easy expansion or modification of inputs and remote control stations. The Security Management System 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. Security Management System reconfiguration shall be accomplished online through system programming. The Security Management System shall include the following:

1. Multi-User/Network Capabilities: The Security Management System 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 devices for the workstation. Standard operator permission levels shall be enforced, with full operator audit.

2. Concurrent Licensing: The Security Management System shall support concurrent client workstation licensing. The Security Management System 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.

3. Security Key: The Security Management System shall only require a software security key to be present on the application server for the Security Management System to operate. Security keys shall not be required at the client workstations. The Security Management System shall allow a user to read the information that is programmed on the server security key. The Security Management System shall support the installation, update, and termination of the security key.

4. Access Control Software Suite: The Security Management System shall offer a security management software suite available in four scalable versions: Lite, Professional, Corporate, and Enterprise Editions. The Security Management System platform shall offer a complete access control solution: alarm monitoring, video imaging, ID badging and video surveillance control.

NOTE TO SPECIFIER: Delete if Pro-Watch Lite Edition is not required.

a. Lite Edition: The Security Management System shall utilize the Microsoft SQL Express database for applications with one to four users and up to 32 controlled doors. The Security Management System shall operate in Windows 8.1/10 Professional/Enterprise as the host operating system.

NOTE TO SPECIFIER: Delete if Pro-Watch Professional Edition is not required.

b. Professional Edition: The Security Management System shall utilize Microsoft SQL Express (SQL 2012 or 2016 64-bit) database for applications from one to five users and up to 64 controlled doors. The Security Management System shall provide a set of tools to easily backup, restore and maintain the Security Management System database. The Security Management System shall allow for expansion to Corporate and/or Enterprise Edition without changing the user interface or database structure. The Security Management System shall operate in Windows 8.1/10 Professional/Enterprise as the host operating system.

Honeywell Internal

NOTE TO SPECIFIER: Delete if Pro-Watch Corporate Edition is not required.

c. Corporate Edition: The Security Management System shall operate in the Windows Server 2012 (64-bit), Windows Server 2012 R2 (64-bit), and Windows Server 2016 (64-bit) environment and support SQL Server 2012, 2014, and 2016 Standard (64-bit) as the database engine.

NOTE TO SPECIFIER: Delete if Pro-Watch Enterprise Edition not required.

d. Enterprise Edition: The Security Management System shall incorporate regional server architecture. Regional sites shall operate autonomously with all information required to maintain security locally. The enterprise server shall maintain any critical system information via synchronization with each regional site. A single enterprise server shall provide global management of all regional servers and shall act as a central collecting point for all hardware configurations, cardholder and clearance code data and transaction history. The enterprise server and regional server(s) shall support Windows Server 2012 (64-bit), Windows Server 2012 R2 (64-bit), and Windows Server 2016.

5. Terminal Services: The Security Management System shall support Windows Server 2008 Terminal Services. Terminal Services shall allow the Security Management System server application to reside on the Windows Terminal Server. Operating systems supporting a standard web browser shall be capable of utilizing the thin client architecture. The Security Management System shall support unlimited connections, based on concurrent licensing, to the Security Management System software. Full functionality shall be obtained through the intranet connection allowing full administration and monitoring without the need for a local installation.

6. The Security Management System shall support on installation Microsoft Azure platform (IaaS – Infrastructure as a Service).

7. 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 2012, 2014, and 2016 Standard (64-bit).

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

9. Memory: Proprietary software programs and control logic information used to coordinate and drive system hardware shall be stored in read-only memory.

10. LDAP/ Microsoft Active Directory Services: The Security Management System shall provide support of Lightweight Directory Access Protocol (LDAP) for enabling the user to locate organizations, individuals, and other resources such as files and devices in a network, whether on the public internet or on a private intranet. The Security Management System shall provide a direct link to Microsoft Active Directory Services. The Security Management System shall allow the transfer of Active Directory users into the database via the Data Transfer Utility. Conversely, Security

Honeywell Internal

Management System users shall be capable of being exported to the Active Directory.

11. 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, Spanish, Portuguese, French, German and Simple Chinese.

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

    a. 256-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. OSDP Support

13. Supervised Alarm Points: Both supervised and non-supervised alarm point monitoring shall be provided. Upon recognition of an alarm, the system shall be capable of switching CCTV cameras that are associated with the alarm point.

14. Compliance and Validation: The Security Management System shall incorporate signature authentication where modifications to Security Management System resources will require either a single or dual signature authentication. Administrators will have the ability to select specified devices in the Security Management System where data manipulation will be audited and signatures will be required to account for the data modification. Upon resource modification, the user will be required to enter a reason for change or select a predefined reason from a list. All data will be securely stored and maintained in the database and can be viewed using the reporting tool. This functionality will meet the general requirements of Validation and Compliance through Digital Signatures with special attention to the case of Title 21 CFR Part 11 Part B compliance.

15. Clean Room Solution:

    a. Overview: The Security Management System shall provide a clean room solution which enables users to manage their “Clean Environments” or other areas requiring special restricted access through a process-oriented graphical user interface (GUI).

    b. Configuration: The user shall have the capability of adding, editing, or deleting clean rooms. Each “clean room” shall be capable of having a contamination

Honeywell Internal

level set. Entry to a higher level contamination area shall automatically restrict access to cleaner level areas. Individual cards shall be capable of being reset on an immediate one time, automatic, or per-hour basis.

OPERATIONAL REQUIREMENTS

W. Security Management System Operational Requirements:

1. System Operations:

a. Windows Authentication Login: The Security Management System shall use an integrated login method which accepts the user ID of the person who has logged on to Windows.

b. Password: The Security Management System shall use an integrated authentication method which utilizes Windows user accounts and policies.

c. Information Access: The Security Management System shall be capable of limiting operator access to sensitive information. Operators must have proper authorization to edit the information.

d. Shadow Login: The Security Management System shall allow users to login over a currently logged-on user without having the current user log off the Security Management System or out of the Windows operating system.

e. Graphical User Interface: The Security Management System shall be fully compliant with Microsoft graphical user interface standards, with the look and feel of the software being that of a standard Windows application, including hardware tree-based system configuration.

f. 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.

g. Secure Mode Verification (e.g., force guard to do a visual verify): The Security Management System shall provide ‘secure mode’ control from the verification viewer. This shall allow a user or guard to decide the access of an individual who presents his/her card at a designated secure mode reader.

h. Identity Management Portal: The Identity Management Portal shall provide a web-based portal to request and approve access for badgeholders who’d like to gain access to specific locations.

i. Database Partitioning: The Security Management System shall support dynamic partitioning. A Security Management System in which partitions are set up at installation and cannot be easily changed shall not be acceptable.

j. Status Groups: The Security Management System shall support a real-time system status monitor that graphically depicts all logical devices.

Honeywell Internal

k. Keyboard Accelerators: The Security Management System shall allow the user to use a shortcut key to enable designated system commands.

l. Automatically Disable Card upon Lack of Use: The Security Management System shall allow system operators to set a predefined time period in which cardholders must swipe their card through a card reader in the Security Management System.

m. User Functions and ADA Ability: The Security Management System shall provide user functions and ADA (Americans with Disabilities Act) ability that provides the capability to trigger an event at the Security Management System intelligent controller when a defined card is presented.

n. Pathways: The Security Management System shall support the capability of programming pathways. A pathway shall be an object that combines input points to be masked (shunted) for a set duration, and an output point to be activated, when a particular card receives a local grant at a reader.

o. Database Audit Log: The Security Management System shall be capable of creating an audit log in the history file following any change made to the Security Management System database by an operator.

p. Operator Log: The Security Management System shall be capable of creating an action log in the history file following actions performed by an operator.

q. Alarm Routing: The Security Management System shall be capable of defining routing groups that determine what event information shall be routed to a user or class of users.

r. Global and Nested 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.

s. Two Person Rule: The Security Management System shall support a “two person rule” to restrict access to specific access areas unless two cardholders present two different valid cards to the reader one after the other within a period time defined by the door unlock time multiplied by a factor of 2.

t. Occupancy Restrictions: The Security Management System shall allow the user to define the minimum and maximum occupancy allowed in a designated area.

u. Multiple Sequential Card Swipes to Initiate Procedure: The Security Management System shall allow the user to define a logical device, quantity of consecutive identical events, a time period and a Security Management System procedure to trigger when the event occurs that quantity of times in the allocated time period.

v. Hardware Templates: The Security Management System shall include the ability to define hardware templates (door templates) in order to simplify the

Honeywell Internal

process of creating an access control system. Hardware templates shall allow a user to define a "typical" door configuration and then use that template over and over in the process of defining doors.

w. MRDT. Pro-Watch can accommodate Mercury Intrusion hardware like the Mercury MRDT ("Mercury Digital Terminal") with keypad. MRDT works with PW-6000 panel to provide intrusion functionality. Mercury Intrusion requires a special Pro-Watch license.

2. Access Control Functional Requirements: Functions shall include validation based on time of day, day of week, holiday scheduling, site code verification, automatic or manual retrieval of cardholder photographs, and access validation based on positive verification of card/PIN, card, and video. The following features shall be programmable and shall be capable of being modified by a user with the proper authorization:

a. Time Zones: Shall define the period during which a reader, card, alarm point, door, or other system feature is active or inactive. In addition to Monday-Sunday, there shall be at least one day of the week called Holiday.

b. Holidays: The application shall allow holidays to be entered into the Security Management System. Holidays shall have a start date plus duration defining multiple days. Holidays shall have a holiday type of 1, 2, or 3, which may be defined by the user.

c. Response Codes: The Security Management System shall allow the user to enter a predefined code to represent a response to an alarm occurring in the facility.

d. Clearance Codes: The Security Management System shall allow the user to establish groups of readers at a facility for the purpose of granting or denying access to badgeholders. Clearance codes shall be assigned to companies and individuals employed by the company, and may be modified for individual users in the badgeholder maintenance application.

e. Companies: Each badgeholder entered into the Security Management System shall be assigned a company code identifying the individual's employer. The company information dialog box displays and maintains information related to companies having access to the facility.

f. Group Access: The Security Management System shall allow a user or group of users via company selection, a temporary denial of access to specific readers or areas based on a preconfigured event. The group access function shall limit access to a group of cardholders, overriding all other access criteria.

g. Events: The event editors shall control processing done at the host computer that allows the user to associate nearly any input (trigger) with almost any sequence of outputs (actions) that the Security Management System is capable of executing.

h. Alarm Pages: Security Management System shall include the capability to create an unlimited number of customized alarm pages for the alarm monitor and each shall be assignable to users and user classes.

i. Event Types: Definitions shall be shipped with system software but shall be capable, upon installation, of being modified, added to, or deleted from the Security Management System.

j. Dynamic Graphical Maps: The Security Management System shall provide the user with the means to add maps and indicator icons to maps that shall represent input/output points, logical devices, or cameras located throughout the Security Management System. Security Management System maps shall display the state and condition of alarm points. The Security Management System shall also provide the ability to monitor the channels or panels.

k. Brass Keys: Shall maintain information related to assets that are issued in the facility, including brass keys, laptops, RSA keys, cell phones, company cards, etc.

l. ID Badging Client: The Security Management System Shall maintain information related to a badgeholder's card access privileges. Upon entering this application, a window shall appear on the screen and all actions (add, modify, or delete) involving badges and cards shall be initiated from this window. Access privileges shall be linked to the cards used to gain access to doors in the facility. Modifications shall be made by adding or deleting clearance codes, or by door types assigned to the cards or to a badgeholder.

m. ID Badging System: The Security Management System shall include seamlessly integrated ID badging system.

NOTE TO SPECIFIER: Select the appropriate version(s) of Pro-Watch's Unified Badging software, or designate that the contract should select the appropriate version based on the size and configuration of the system for this project.

A. Unified Badging Management System Manufacturer: Pro-Watch® Badging software by Honeywell, www.honeywellintegrated.com. Provide the following software system:

1. Pro-Watch® AP Edition.

2. Pro-Watch® Standard Edition.

I. **Unified Badging/Identity Management – Standard Edition**

1) **Reporting Module** (Standard, Wizard, Scripting)
2) **Unified Biometric Integration (Morpho)**
IDMS shall be able to enroll Morpho fingerprints or wave hand prints within the same in-process application without using another 3rd party application or biometric manufacturers enrollment application. All biometric data is stored and maintained in the Pro-Watch database. IDMS can push templates

to biometric readers (1 to many matching) or encode to smart card (1 to 1 matching).

3) **Certifications/Training Module**
IDMS shall be able to maintain certifications/training for a badge holder. A certification may be linked to access groups with expiration dates. When a certification, associated to an access group, has expired and the badge holder has an active credential, the access group will be removed from the credential without affecting the status of the credential.

4) **Assets Module**
IDMS shall be able to keep track of any type of asset (keys, phone, computer, etc.) assigned to a badge holder. Asset should be tracked for assignment, returned, lost or stolen. A report of assets assigned to a badge holder that be available on demand.

5) **Company/Employer Module with Authorized Signatory**
IDMS shall be able to maintain all aspects of companies/employers doing business on the property. Data maintained for companies shall include: authorized signers, company web portal access, sponsor companies, default access groups for badge holders, defined badge types, company documents, company vehicles.

6) **Document Management Module**
IDMS shall be able to maintain any number of documents for a badge holder or company. Stored documents shall be any paper, electronic on a file system or a link such as a web page. Paper documents should be able to be scanned as images or PDF's. PDFs should be scanned as a single or multiple documents. Documents can be viewed and printed at any time for any badge holder.

7) **Vehicle Permits and Tracking Module**
IDMS shall support vehicle permit issuance to a badge holder or companies. Vehicle permit will be issued to associated vehicles and maintain items such as vehicle model, license plate and insurance information. Vehicle permits will be issued, expired, lost and stolen.

8) Badge Design Wizard

II. **Unified Badging/Identity Management – AP Edition**

1) **Channeling Integration (TSC, Telos)**
IDMS system shall integrate to Telos and TSC backend web services to automatically push data for STA, CHRC and RapBack integration. Results will be received from TSC and Telos web services and will update individual badge holder records.

2) **Livescan Integration (Greenbit)**
IDMS shall integrate to the GreenBit Livescan DactyScan84c

Honeywell Internal

machine. Slap fingerprints are captured to be sent to the channeler and onto the FBI for CHRC adjudication.

3) **Billing Module**
IDMS shall be able to maintain billing transactions for badge holders. Billing transactions can be specifically defined, but will include transactions for a new badge, lost or stolen badge and any type of revenue transaction pertaining to badge holder actions.

4) **Violations Module**
IDMS shall maintain violations issued to badge holder population. Violations will be tracked with violation fine amounts, location, time and status. An adjudication process is also tracked with hear date, hearing office and verdict.

III. **Unified Badging/Identity Management – Optional Modules**

1) Vendor Management Portal

2) Identity Management Portal

3) **Smart Card Encoding and Printing**
IDMS shall be able to securely encode a smart card either through a USB/network encoder or via a printer. Using a printer, the smart card will be encoded and printed in a single step. Data written to the smart card will be credential information and may include biometric data and time clock applications.

4) **Vehicle Gate Control Software**
Credential holders entering perimeter vehicle gates shall be shall be monitored for driver and escort privileges via the Gate Control software. Drivers of vehicles must have driver designations on their badges and in the database. Vehicle passengers must have access to vehicle gate and will be associated in vehicle with the driver. If the driver is escorting a vehicle, the driver must have escort privileges. A guard will monitor transactions and swipe credential to validate driver and passengers and open the vehicle gate.

a. Users: Information related to the users of the Security Management System software shall be stored in the database. Users entered into the Security Management System shall be assigned the access privileges of the class to which they are assigned.

b. Elevator Control: The elevator control shall be of the Security Management System intelligent controller-based line of devices. The elevator control shall include the following functional features:

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

Honeywell Internal

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

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

c. Data Transfer Utility (DTU): The DTU enables data to be imported from an external system directly into the Security Management System database **as well as** exported from Pro-Watch to an external system.

I. Insert only: If a "data file key column #" shall be provided, the DTU will only insert a new badge record if the key column value is not found. An error shall be displayed in the log file if an existing badge record is found. If no "data file key column #" is provided, every record will be inserted into the Security Management System.

II. Updates only: The DTU shall use the "data file key column #" to look for the matching Security Management System record. An error shall be logged in the log file if the badgeholder is not found in the Security Management System database.

III. Inserts, updates: The DTU shall use the "data file key column #" to look for the matching Security Management System record. If a matching record is not found, the DTU shall insert the data. If a matching record is found, the record shall be updated.

IV. DTU shall support SOAP and REST web services.

d. Generic Channel Interface: The Security Management System shall provide the ability to define generic communications channels over serial port or TCP/IP network socket including IP address and port/socket, to support custom integration of external foreign devices. The Security Management System shall generate events based on data received from the channel matching operator pre-defined instructions.

3. Application Localization: The Security Management System shall support at least seven languages including English. The languages available must include German, French, Spanish, Italian, Chinese (simplified), Portuguese (Brazil), Norwegian, Chinese (Traditional), Danish, and Dutch, All database resources will be localized, and will include a standard U.S. English help file.

4. Event Manager: The Security Management System shall utilize an event manager as a component of system administration and offer the ability to have users control the amount of data stored as well as a quick snapshot of the logged data in the system. Using the various logs in event manager, the user will be able to gather information about events, auditing, and operator actions. The logs are defined as follows: Event log, audit log, unacknowledged alarms.

Honeywell Internal

HARDWARE REQUIREMENTS

INTELLIGENT CONTROLLERS

5. 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.

6. 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.

7. Manufacturers: Subject to compliance with requirements, provide Field Controllers or comparable product by one of the following:

    a. Honeywell Security Star II (Legacy support only)

    b. Honeywell Security PW-2000

    c. Honeywell Security PW-3000 (Legacy support only)

    d. Honeywell Security PW-5000

    e. Honeywell Security PW-6000

    f. Honeywell Security PW-6101ICE

8. Cardkey Controllers: The Security Management System software suite shall provide functionality to Cardkey Controllers using Nodal Protocol B, the Cardkey Controllers D620 (Firmware revision PS-143D or PS143-E), and the Cardkey D600AP (Firmware Revisions PS-155A or PS-155B). Supported interface is currently, but not limited to, standard STI and STIE devices. Minimum functionality to be supported:

    a. Controller to host communications.

    b. Downloading of cards.

    c. Downloading of Security Management System parameters.

    d. Downloading of reader parameters.

    e. Downloading of input point parameters.

    f. Downloading of relay output point parameters.

FIELD HARDWARE

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

9. 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.

10. Intelligent Controller Board

a. Honeywell Security PW3K1IC (Legacy support only)

b. Honeywell Security PW6K1IC

c. Honeywell Security PW6K1ICE

11. Single Reader Module (SRM)

a. Honeywell Security PW6K1R1

b. Honeywell Security PW6K1R1E

12. Dual Reader Module (DRM)

a. Honeywell Security PW6K1R2

13. Alarm Input Module (AIM)

a. Honeywell Security PW6K1IN

14. Relay Output Module (ROM)

a. Honeywell Security PW6K1OUT

15. Card Readers

a. Honeywell Security

I. OmniProx

II. OmniAssure

III. OmniClass

IV. DigiReaders

b. HID

I. ProxPro

II. MiniProx

III. MaxiProx

IV. ThinLine II

V. ProxPro II

VI. ProxPoint Plus

c. Indala

I. FlexPass

II. FlexPass Linear

III. FlexPass Arch

IV. FlexPass Curve

V. FlexPass Long Range

VI. FlexPass Wave

d. Biometric Readers

I. BioScrypt

II. Recognition Systems

III. Morpho Wave Reader

IV. IRIS ID Reader

e. WSE Readers (SNET Protocol) – Star I, Star II, PW-6000

I. DR4201

II. DR4203

III. DR4205

IV. DR4205K

V. DR4208

VI. DR4208K

VII. DR4220

VIII. MSR42-GW

f. Wireless Readers

I. IR Wireless Reader

II. AD-400 Wireless Locks

III. SALTO SALLIS Wireless Reader

IV. ASSA ABLOY APERIO Wireless Reader

V. SCHLAGE Wireless Reader

16. Mercury Family Hardware

I. EP-1501

II. EP-1502

III. EP-2500

IV. MR-16IN (16 Input Board)

V. MR-16OUT (16 Output Board)

Honeywell Internal

VI. MR-50 (Single Reader Board)

VII. MR-51E (Single Reader Board ETHERNET)

VIII. MR-52 (2-Reader Board)

IX. SCP/SCP2

X. Mercury M5 Bridge

a. M5-IC (Controller)

b. M5-2RP (Dual Reader Module)

c. M5-2SRP (Supervised Dual Reader Module)

d. M5-8RP (Eight Reader Module)

e. M5-2K M2000 Reader Module)

f. M5-20IN (Input Panel)

g. M5-16DO (Output Module)

h. M5-DOR (Output Panel)

i. M5-COM (Communication Board)

XI. Mercury MS Bridge

a. MS-ICS

b. MS-ACS

c. MS-I8S

d. MS-IRS

17. Lenel Family Hardware

I. LNL-1000 with Wiegand Reader

II. LNL-1100 (16 Input Board)

III. LNL-1200 (16 Output Board)

IV. LNL-1300 (Single Reader Board)

V. LNL-1320 (2-Reader Board)

VI. LNL-2000 with Wiegand Reader

VII. LNL-2210

VIII. LNL-3300

IX. LNL-8000

Honeywell Internal

18. SALTO Locksets

    Locksets compatible with SVN - Salto's Virtual Network.

19. MRDT – Mercury Intrusion Display Terminal

UNIFIED PHYSICAL ACCESS CONTROL SYSTEM

1. PW Series Panels
2. Mercury Panels
3. Mercury Bridge Hardware (Casi-Rusco, Software House)
4. OPTIONS:
   - Readers (DesFire, Seos, Proximity, etc.)
   - Pro-Watch API
   - Data Transfer Utility
   - Biometric Unified (Morpho)
   - Intrusion (Galaxy, Vista, Mercury)
   - Intercom Interface (Commend or Stentofon)
   - IP Based CCTV Interface (Honeywell MaxPro VMS)
   - Analog Switch Interface (Burle Allegiant, Pelco, Integral Technologies)
   - IP/Wireless Readers (Aperio, Salto, Allegion, Assa Abloy)
   - Visitor Management (Honeywell LobbyWorks, EZ Lobby)

SYSTEM INTERFACES

B. 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. Manufacturer(s) and part numbers:

   a. Honeywell MAXPRO® VMS

   b. Honeywell Fusion III series digital recorders

   c. Honeywell Rapid Eye Multi-Media series digital recorders

C. Video Management Systems (VMS):

1. With integration to VMS, Security Management System shall control multiple sources of video subsystems in a facility to collect, manage and present video in a clear and concise manner. VMS intelligently determines the capabilities of each subsystem across various sites, allowing video management of any analog or digital video device through a unified configuration and viewer. Disparate video systems are normalized

and funneled through a common video experience. Drag and drop cameras from the Security Management System hardware tree into VMS views. Leverage Security Management System alarm integration and advanced features such as pursuit that help the operator track a target through a set of sequential cameras with a single click to select a new central camera and surrounding camera views.

2. Manufacturer(s) and part numbers:

    a. Honeywell Security MAXPRO VMS

D. Intercom Interface:

1. The interface shall provide control of both remote and master intercom stations from within the Security Management System application. The Security Management System shall allow the user to define the site, channel, description, and address as well as provide a checkbox for primary station.

2. Administrators shall have the capability to program a list of intercom functions that report to the alarm-monitoring module as events. These functions shall coincide with the intercom functions provided with the intercom system. For each intercom function, Security Management System administrators shall be able to define an alphanumeric event description 1 to 40 characters in length and shall also be able to set the parameter value of that function.

3. The intercom interface shall allow for secondary annunciation of intercom calls, events, and alarms in the alarm-monitoring window. Intercom reporting to the alarm monitoring window shall report as any other access control alarm and shall have the same annunciation and display properties as access control alarms.

4. All intercom calls, events, and alarms that report into the Security Management System shall be stored in the system database for future audit trail and reporting capabilities. Intercom events shall include but not be limited to: Station busy, Station free, Intercom call to busy station, Intercom call to private station, Station disconnected, Function dialed outside connection, Intelligent station ID, Station reset, Station lamp test, Audio program changed, Group hunt occurred, Mail message, Digit dialed during connection, Direct access key pressed, Handset off hook, M-key pressed, C-key pressed

5. Manufacturer(s) and part numbers:

    a. Stentofon/Zenitel Alphacom series intercoms

    b. Commend series intercoms

E. Intrusion Detection Panels:

1. Honeywell VISTA-128FBP, Vista 128BPE, Vista 128BPT, VISTA-250FBP, Vista 250BPE, and Vista 250BPT Controllers:

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

Honeywell Internal

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:

I. Disarm and unlock a door on card swipe.

II. Arm and lock a door on card swipe.

III. Common area arm/disarm.

IV. Access denied if intrusion system is in alarm or armed.

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

VI. Associate intrusion system events and alarms to video surveillance integrations.

2. Honeywell Galaxy Dimension GD264 and GD520 Controllers:

a. Security Management System users are able to 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, a 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:

I. Disarm a zone on a card swipe.

II. 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.

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

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

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

VI. Security Management System stores and reports on intrusion events.

F. Software Development Kit (SDK)

1. Security Management System shall permit custom integration with other third party systems through an SDK. SDK shall support the OBIX communication protocol and interface directly with the Niagara Framework for support of additional communications protocols.

Honeywell Internal

2. Manufacturer(s) and part numbers:

a. Honeywell Security HSDK

G. Web Client

a. Web Alarms

b. Web Events

c. Web Badging

d. Web Reports

H. Supported Web Browsers

a. (Windows) Internet Explorer 11

b. (Windows) Google Chrome Version 42

I. Unified Alarm Management System

a. OPTIONS:

- Video Integration
- Intrusion (Galaxy, Vista, Mercury)
- Intercom Interface (Commend or Stentofon)
- Direct CCTV Interface (Burle Allegiant, Pelco, Integral Technologies, Honeywell MaxPro VMS)
- Notifier Fire Alarm Interface

b. FACTORY DIRECT SERVICES:

- On-Site Technical Support
- Professional Services (On-Site, Remote)
- Database Services
- Training and Certification
- Custom Development

EXECUTION

EXAMINATION

J. 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.

Honeywell Internal

INSTALLATION

K. 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.

L. 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.

FIELD TESTING AND CERTIFICATION

M. 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

Honeywell Internal