PACS A&E SPECIFICATION

REVISION 1.1

MAY, 2017

AccessNsite • 2520A Skyway Drive, Santa Maria, CA 93455 • 877.815.5511

SECTION 28 10 00
ACCESS CONTROL

PART 1 - GENERAL

1.1 SECTION INCLUDES

A. This Physical Access Control System (PACS) specification shall be inclusive of, but not limited to:
1. System Description
2. System Hardware
3. Graphical User Interface
4. Cardholder Management
5. Badge Creation
6. Access Control
7. Alarm and Event Monitoring
8. Event Photo & Video
9. System Administration
10. Graphical Maps
11. Video Management Integration
12. Software Support
13. Device Status
14. Automation Rules
15. Quick Launch
16. Help Assistance
17. Approvals
18. Video Interface
19. Web Clients
20. Database Import
21. Approved Manufacturers

1.2 SCOPE OF WORK

A. The Scope shall include a complete, operational electronic access control system supplied, installed, programmed and commissioned to deliver the features and functionality described in this Section. Services shall include engineering, procurement, installation and associated functions necessary to provide a fully operational PACS, as per manufacturer's guidelines and applicable building codes.

B. The PACS shall offer integrated Intrusion Detection System (IDS) functionality and a Badging Software module as described in this Section.

C. All necessary tools, equipment, hardware, software and software user licenses required as described in this Section shall be included for a complete installation of the PACS under this scope.

1.3 REFERENCES

A. The following reference standards and model code documents shall be used in estimating and detailing door hardware, and shall considered as a standard of quality, function, and performance, as applicable:
1. I.B.C. International Building Code – Edition noted as project basis of design.
2. I.F.C International Fire Code – Edition noted as project basis of design.
3. N.E.C. National Electrical Code – Edition noted as project basis of design.
4. I.E.E.E. Institute of Electronic and Electrical Engineers - Current 802.xx standards
5. U.L. Underwriters Laboratory - Current U.L. 294 standards listings
6. NFPA 80 National Fire Protection Agency - Fire Doors & Windows (edition is jurisdiction dependent).
7. NFPA 101 National Fire Protection Agency - Life Safety Code (edition is jurisdiction dependent).
8. NFPA 105 National Fire Protection Agency - Smoke Control Door Assembly. (edition is jurisdiction dependent)
9. ANSI 117.1 1992 Edition Providing Accessibility and Usability for Physically Handicapped People.
10. A.D.A.A.G Americans with Disabilities Act Accessibility Guidelines.

B. DEFINITIONS
1. DEFINITIONS
   a. PACS: Physical Access Control System
   b. IDS: Intrusion Detection System
   c. VMS: Video Management System

d.	ASIS:	American Society for Industrial Security
e.	PSP:	Certified Physical Security Professional
f.	API:	Application Programming Interface
g.	AVI:	Audio Video Interleave
h.	CA:	Certificate Authority
i.	CAC:	Common Access Card
j.	CE:	European Union Conformity
k.	CPU:	Central Processing Unit
l.	CSV:	Comma Separated Values
m.	DNS:	Domain Name Server
n.	DSM:	Door Status Monitor
o.	DVR:	Digital Video Recorder
p.	EPS:	Events Per Second
q.	FCC:	Federal Communications Commission
r.	FIPS:	Federal Information Processing Standard
s.	FIFO:	First In – First Out
t.	FTP:	File Transfer Protocol
u.	FRAC:	First Responder Authentication Credential
v.	GB:	Gigabyte
w.	HTML:	Hypertext Markup Language
x.	H.264:	Video Compression Standard
y.	IEEE:	Institute of Electrical and Electronics Engineers
z.	I/O:	Input/Output
aa.	IP:	Internet protocol
bb.	IS:	Integrated System
cc.	JPEG:	Joint Photographic Experts Group
dd.	LAN:	Local area network
ee.	LDAP:	Lightweight Directory Access Protocol
ff.	MB:	Megabyte
gg.	MJPEG:	Motion JPEG
hh.	MSATA:	Mini-Serial Advanced Technology Attachment
ii.	MTBF:	Mean-Time Between Failure
jj.	NAS:	Network Attached Storage
kk.	NBAPI:	NetBox Application Programming Interface
ll.	NFPA:	National Fire Protection Association
mm.	NVR:	Network Video Recorder
nn.	ODBC:	Open Database Connectivity
oo.	OS:	Operating System
pp.	OVID:	Open Video Integration Driver
qq.	PDF:	Portable Document Format
rr.	PIN:	Personal Identification Number
ss.	PIV:	Personal Identity Verification
tt.	PoE:	Power over Ethernet
uu.	PTZ:	Pan-tilt-zoom
vv.	RAID:	Redundant Array of Inexpensive Disks
ww.	RAM:	Random Access Memory
xx.	REX:	Request to Exit
yy.	RFID:	Radio Frequency Identification
zz.	ROM:	Read Only Memory
aaa.	RU:	Rack Unit
bbb.	SHA:	Secure Hash Algorithm
ccc.	SIO:	Secure Identity Object
ddd.	SMS:	Short Message Service (text messaging)
eee.	SSL:	Secure Sockets Layer
fff.	SUSP:	Software Upgrade and Support Plan
ggg.	TCP:	Transmission control protocol – connection to hosts via IP
hhh.	GUI:	Graphical User Interface
iii.	UPS:	Uninterruptible power supply
jjj.	UTP:	Unshielded Twisted Pair
kkk.	WAN:	Wide area network
lll.	Wi-Fi:	Wireless IEEE 802.11x Network

1.4 SUBMITTALS

A. Product Data: Provide a catalog cut sheet, clearly marked and identified, illustrating and describing each product included in the Physical Access Control System (PACS) Schedule.
1. Include construction and installation details, material descriptions, dimensions of individual components and profiles, and finishes.
2. Formulate catalog cut sheets into sets and include a set with each copy of the Equipment Schedule submitted.

B. Access Control Schedule: Prepared by or under the supervision of a Certified Physical Security Professional (PSP) credentialed by the American Society for Industrial Security (ASIS). The schedule shall detail assembly of all hardware, as well as procedures, and diagrams. Coordinate with the final Door Hardware Schedule with doors, frames, and related work to ensure proper size, thickness, hand, function, and finish of door hardware.
1. Format: Comply with scheduling sequence and vertical format in DHI's "Sequence and Format for the Hardware Schedule."
2. Organization: Organize the PACS Schedule into door hardware sets indicating complete designations of every item required for each door or opening. Coordinate PACS Schedule with Section 08 7100. DO NOT DUPLICATE PRODUCT SHOWN AS SUPPLIED BY SECTION 08 7100.
3. Content: Include the following information:
   a. Type, style, function, size, label, hand, and finish of each PACS item.
   b. Complete designations of every item required for each door or opening including name and manufacturer.
   c. Fastenings and other pertinent information.
   d. Location of each door hardware set, cross-referenced to Drawings, both on floor plans and in door and frame schedule. Use same scheduling sequence and format and use same door numbers and hardware set numbers as in the Contract Documents.
   e. Explanation of abbreviations, symbols, and codes contained in schedule.
   f. Mounting locations for PACS product.
      i. PACS product sizes and materials.
      ii. Verify the Section 08 7100 Description of each electrified door hardware function, including location, sequence of operation, and interface with other automated building control systems. Notify Architect and Owner Representative if operational description does not meet the need and provide corrected solution.
4. Submittal Sequence: Submit the final PACS design at earliest possible date, particularly where approval of the PACS must precede fabrication of other Work that is critical in the Project Construction Schedule, such as door frame fabrication and raceways in cast and concrete block. Include Product Data, Samples, Shop Drawings of other work affected by hardware, and other information essential to the coordinated review of the PACS Schedule.
5. Designations: Requirements for design, grade, function, finish, size, and other distinctive qualities of each type of door hardware are indicated in Part 3 "PACS Schedule". Products are identified by using door hardware designations, as follows:
   a. Provide the materials or products indicated by trade names, manufacturer's name, or catalog number.
   b. Provide manufacturer's standard products meeting the design intent of this Specification, free of imperfections affecting appearance or serviceability.
   c. Hand of door: Drawings show direction of slide, swing or hand of each door leaf. Furnish each item of hardware for proper installation and operation of door movement as shown.

C. Wiring Diagrams: Verify with Section 08 7100 all electrified hardware items specified for this Project. Provide riser drawings and elevations, showing locations where such material is to be installed. Detailed Point-to-Point Wiring Diagrams will not be required for submittal *ONLY* if the equipment supplier is also the installing and commissioning contractor. Verify and coordinate with the electrical systems installer.
1. Operation Narrative: Describe the operation of doors controlled by electrified door hardware.

D. Keying: Verify with Section 08 7100 all keying will function properly with the PACS devices.

E. Credentials: The supplier shall hold a pre-Installation meeting to develop/discover the Owner Standard for credential technology, credential style, Facility Code, Bit Format, Sequential Numbering, and verification that all PACS devices will operate with a single credential.

F. Operation and Maintenance Data: Include each type of Access Control equipment in maintenance manuals. Provide latest, revised and updated schedule of PACS devices, cut sheets, and project schedule. In addition, furnish one (1) copy of maintenance and parts manuals for those items which are readily available and normally provided.

As-Built Drawings: During system installation, the PACS Contractor to maintain a separate hard copy rendering of the scope of work. This is to be kept up to date by the Contractor with all changes and additions to the PACS accurately recorded.

1.5 QUALITY ASSURANCE

A. Installer Qualifications: Minimum of two (2) experienced, trained and FACTORY certified installers who have completed previous PACS projects whose work has resulted in a record of successful in-service performance. Submit a minimum of three (3) project references of the same size and complexity and the specified system.

B. Provide proof of Dealer status and installer certifications. A copy of manufacturer(s) official certification document shall be provided indicating proof of status as a qualified and authorized provider of the primary access control components. The PACS contractor shall also provide written verification of installer's factory certifications.

C. Source Limitations: Obtain each type and all intelligent controllers from the same manufacturer providing the PACS software solution, unless otherwise indicated.

D. Fire-Rated Door Assemblies: Provide PACS hardware for assemblies complying with NFPA 80 that are listed and labeled by a testing agency acceptable to authorities having jurisdiction, for fire ratings indicated.

E. Electrified Door Hardware: Listed and labeled as defined in NFPA 70, Article 100, by a testing agency acceptable to authorities having jurisdiction, and marked for intended use.

F. The PACS contractor shall have a physical location within 100 miles of the project. Submit copies of State issued driver's licensed for at least two (2) local installation technicians.

1.6 WARRANTY

A. Refer to Division 1 of this Specification Manual for project warranty provisions.

B. The manufacturer shall warrant that the hardware product(s) are free from defect in materials and/or workmanship for a period of one year for door controllers and one year for Onsite Server Appliances. The PACS equipment shall be provided with one year product warranty from date of shipment or one year year from date of registration, whichever is shorter.

1.7 SUPPORT

A. On-site support shall be provided by the PACS security integrator of record. Contact the manufacturer for more details. Response has been defined in Part 3 of this Section.

Software version upgrades shall be available at no charge during the warranty period.

1.8 DELIVERY, STORAGE, AND HANDLING

A. Marking and Packaging: All items of hardware shall be delivered to the site in manufacturer's original cartons or boxes. Mark each door hardware box with the heading and door number according to approved schedule.

B. Deliver individually packaged hardware items at the proper times to the proper locations (shop or project site) for installation. Provide a complete packing list showing items, door numbers and headings with each shipment.

C. Store hardware in shipping cartons above ground and under cover to prevent damage. Provide secure lockup for door hardware delivered to the Project, but not yet installed. Control handling and installation of hardware items that are not immediately replaceable, so that completion of the Work will not be delayed by hardware losses both before and after installation

Aluminum Door Hardware: Coordinate with Section 08 4313 for all Access Control System hardware prior to Aluminum Door Hardware Delivery. Deliver hardware for aluminum doors as directed by the door supplier for installation by Section 08 4313.

1.9 COORDINATION

A. Templates: Obtain and distribute to the parties involved templates for doors, frames, and other work specified to be factory prepared for installing door hardware. Check Shop Drawings of other work to confirm that adequate provisions are made for locating and installing door hardware to comply with indicated requirements.

B. Electrical System Rough-in: Per local and national building codes, coordinate layout and installation of all raceways, back-boxes and drops as necessary for electrified hardware items. This infrastructure will be verified in trade coordination meetings prior to installation to support both power and data connections for: power supplies, fire alarm system I/O, detection devices, electrified locking hardware, auxiliary devices, cameras, controllers, network switches, PACS servers and workstations and any other required connections to other building automation functions, as applicable.

C. Pre-Installation meeting(s) are required with Electrical Contractor to determine the number of circuits, define cabling types and sizes and quantify the number of conductors required for the PACS. The Door Hardware Supplier (08 71000)

will be included to insure these connections and the wiring is coordinated with electrified locking hardware resulting in proper system functionality for the Owner.

PART 2 - PRODUCTS

2.1 SYSTEM DESCRIPTION

A. The Physical Access Control System (PACS) shall consist of Ethernet based, redundant, real-time host processors/servers, multiple workstations, and a hierarchy of Ethernet based intelligent controllers that interface with sub-controllers (reader and input/output) to connect specified readers, portal input devices, portal output devices, monitor, and control points.

B. The system shall be capable of handling multiple sites via Distributed Architecture, or Cloud based dependency. The software shall support individual sites as small as one (1) card reader to a virtual infinite number with alarm monitoring, video imaging, badging, digital video recorders and CCTV switching control. The system shall be scalable and allow for easy expansion or modification.

C. The system control at the Host location shall be under single software program control, shall provide full integration of all components, and shall be alterable at any time, depending upon the facility requirements. Reconfiguration shall be accomplished through system programming, without hardware changes.

D. The software program shall be a 3-tier client/server application based on modern operating system tools and standards and shall be offered in both 32-bit and 64-bit versions.

E. System controller options shall allow either a two (2) or one (1) tier configuration with master controllers at the card reader, or master panel and sub panels. The software shall be capable of supporting both system architectures simultaneously as part of a single site deployment.

F. The controller panels shall NOT be proprietary to a single brand of PACS software, but shall be compatible with a minimum of one dozen (OEM) manufacturers.

G. The system shall support multiple Client Workstations as well as Web Clients.

H. The system shall support Client Workstations running any mix of the supported operating systems simultaneously (e.g. running Windows, Linux, and/or Mac OS).

2.2 SYSTEM HARDWARE

A. Server
1. The Host Server shall communicate with the field hardware to configure the hardware, collect status (e.g. events and alarms), and execute commands (e.g. arm an area).
2. The Host Server shall communicate with Client Workstations to provide system status and accept configuration and command and control.
3. The Host Server shall be capable of utilizing a central database to store and retrieve hardware configuration data, badge and personnel records, business rules, and event and alarm data.
4. The Operating System shall be any currently supported Microsoft Windows (32/64 bit) server or workstation operating system; any compatible Linux operating system (32/64 bit); and OSX version 10.5 or newer.
5. The PACS shall support use of any of the following databases: Microsoft SQL Server, MySQL, MariaDB and Oracle.
6. Hardware Requirements: CPU, RAM, disk size, and peripheral hardware will be specified by the PACS Contractor following the manufacturer's recommendations for an appropriate robust network-based platform of the size and type necessary for the size and requirements of the system.
7. Support for virtualization: System shall support Microsoft Hyper V virtualization, VMware and or Citrix.
8. The contractor shall coordinate server requirements with an Owner Representative.

B. Client Workstation
1. Workstations shall have full personnel database editing capabilities, personnel image and badge production capabilities, and shall be capable of monitoring alarms and running database and history reports and queries.
2. The Operating System shall be compatible with Microsoft Windows 7 (32/64 bit) or newer desktop operating system; any compatible Linux operating system (32/64 bit); and OSX version 10.5 or newer.
3. Minimum Hardware Requirements: Intel Core i3 1.8 GHz, Minimum 8 GB RAM, 200 GB (minimum) Hard Drive, SVGA Color Monitor 17" (1024 x 768 minimum), Standard keyboard and two-button mouse and a minimum of four USB Ports.
4. Supported Hardware Platforms:
   a. Mercury Security Controllers, Sub-controllers and peripherals Series 1 thru current.

1) Mercury Security Interface for Aperio Family of locks
2) Mercury Security Interface for Schlage AD-300, AD-301, AD-400 and AD-401 utilizing the PIM interface.
3) Mercury Security Interface for Stanley Best IDH Max Locksets

b. HID EVO and Series 1 VertX and Edge controllers
c. DMP XR150 or XR500 Panels with peripherals
d. Allegion Gateway Interface – Live wireless connection to NDE and LE locksets
e. ASSA Abloy Door Service Router supporting the following locks
1) Aperio Solutions – Live wireless (I.e. IN100)
2) IN120 Wifi connected (Not a live lock)
3) IN220 PoE Intelligent Locksets - Live Wired Lockset
f. Best Lock WiQ solution - supporting the following locks
1) Wi-Q gateway
2) EXQ Locksets
3) 9KQ Locksets
4) 45HQ Locksets

C. Data Infrastructure and IP Network Capacity
1. The basis of design for network connectivity when provided by the PACS contractor shall be 10/100/1000 Ethernet LAN, unless the Owner's design standard defines other requirements.

D. Graphical User Interface
1. The interface and operator programming command structure shall be user friendly using standard Windows conventions such as dialog boxes, pull-down menus, menu trees, help prompts, and wizards where appropriate.
2. Competent system use shall be possible by personnel with PC experience commensurate with a commercial work environment and minimal training on the security management system application.
3. The graphical user interface shall execute as a single software program and shall provide full integration of all software modules.
4. Each functional element of the application (e.g. alarm monitoring, personnel management, hardware configuration, etc) shall run in its own window. Each window shall be movable and resizable.
5. The application shall remember the size and position of each window and which windows were open when the user logged out so that the layout can be restored at next user log-in.
6. The software program shall use graphical icons for representing hardware devices in the system. The graphical icons shall be used in graphic maps to provide the user interface to control and monitor hardware devices, and shall also be used in the hardware trees to help organize, display, and control system information.

E. Cardholder Management
1. Personnel records shall be separate and distinct from badge records. A personnel record holds information about a cardholder (e.g. name, SSN, address, etc). Any one user will normally have only one record in the system. A badge record holds information about a badge (e.g. card number, badge number, assigned access levels, etc). A badge is assigned to the user and a user can hold multiple badges with the ability to assign unique access levels to each badge.
2. A personnel record shall have the ability to store digital images of cardholder or other digital images such as a driver's license or passport. The number of images shall be limited only by the maximum size of the database.

F. Badge Creation
1. Provide a badge layout creation and editing module to allow for the creation of custom badge designs by the customer.
2. The badge editing module must be included in the PACS software natively and must not be an integrated third-party add-on.
3. The badge module shall support any industry standard thermal dye transfer ID card printer with an industry standard Microsoft Windows driver.
4. The badge module shall provide the ability to support multiple card enrollment and/or badging stations on a single networked system.
5. The badge module shall provide the ability to print a card in one step (requires suitable printer), without the need to reinsert the card.
6. The badging system shall support an advanced chromakey feature. Chromakey is the process of removing a solid background from a captured image. Chromakey photos are difficult to reproduce or falsify. The system shall be capable of removing the color residing in the top left corner of the crop window, or remove a color of the System Operator's choice. A tolerance setting shall be available for fine-tuning images of cardholders whose shirt, hair, etc. is close to the color of the background.

G. Access Control
1. Field Hardware Communications
a. The system shall communicate with the controllers by either EIA compliant RS-485, or IEEE 802.xx compliant IP addressable standards.

b. The system shall have the ability to communicate with master controllers by LAN/WAN connections utilizing TCP/IP communications protocol.

c. Upon losing and then restoring communications between the controller and the system database, database synchronization between the system database and the local database in each controller shall be fast and efficient.

d. When communications are restored, database synchronization shall occur immediately and without the need for System Operator intervention.

e. When required, Data security for encrypted connections between the system and controllers shall be provided by the full implementation of the Federal Information Processing Standard, FIPS-197, utilizing the 128-bit Advanced Encryption Standard (AES), a symmetric encryption algorithm. If utilized, the 128-bit AES encryption MUST be certified by the National Institute of Standards and Technology (NIST). Implementation of FIPS-197 shall solve the data security requirements for open network connections by providing a means to secure the data over the non-secure network by encryption.

f. Encrypted and open data transmission formats shall be supported for communication between system controllers and card readers. This shall include specifically Open Supervised Device Protocol (OSDP) AND 128 bit AES encrypted options and also, simultaneously in a **mixed system,** Wiegand open data format.

2. The PACS shall support the following Reader Technologies: Proximity, Biometrics, Magnetic stripe, Bar Code, Keypad, Card/keypad (PIN), High-speed Long-Range Vehicle ID, Smart Card and SEOS.

3. Access Features (Online connected panels or Live Online Locks Only)
   a. Support Anti-passback.

   b. Provide a latch mode of operation.

   c. Support a First Card Unlock feature.

   d. Provide a pre-alarm feature.

   e. Provide a host granted mode of operation.

4. Card Formats
   a. Support for ALL generally available open format commercial RFID credential technology. Backwards compatibility to magnetic stripe, Wiegand and other swipe technology shall be possible with special configuration.

5. Access Levels
   a. The application shall allow the definition of access levels which shall be assigned an alphanumeric name using up to 255 characters and which combine card readers and time schedules.

   b. Within each access level, provide the ability to define groups of access points with specific times of access.

   c. Within each access level, provide the ability to define specific elevator access points which will enable the selection of specific elevator floor buttons according to each floor's specified time schedule.

   d. Provide the ability to specify an activation date and expiration date for an access level along with specific times of access.

6. Time Schedules
   a. Provide a number of Time Schedules limited only by the memory available onboard the controller, gateways or intelligent lockset.

   b. Time schedule definitions shall include an unlimited number of time intervals which define a starting time, ending time, days of the week, and holiday override.

7. Secured Areas
   a. Ability to define Special Secured Areas. Secured Areas shall be assigned an alphanumeric name using up to 255 characters. A Secured Area shall allow for the manual or automatic arming or disarming of a group of monitor points and/or access points.

8. Elevator Control
   a. The system shall provide elevator control using standard access control field hardware that will permit the restriction of cardholder access to certain floors while also allowing general access to other floors.

9. Triggers and Procedures (Mercury Panels Only)
   a. Provide the ability to react to the following triggered events without host intervention: DC Power Up Diagnostics, Door Contact Activity, Monitor Point Activity, Monitor Point Group Activity, Reader Activity, Schedule Activity and Authorized User Commands.

b. Provide the ability to perform the following actions at the Client Workstation, without host intervention, when a triggered event occurs: Change the mode of an access point; Disabled, Locked, Unlocked, Facility Code Only, Card, PIN Only, Card & PIN, and Card or PIN; Momentarily unlock a door; Arm or disarm a monitor point; Arm or disarm a group of monitor points; Activate, deactivate, or pulse a control point; Mask or unmask a door forced open or door held open alarm for a specific access point.

H. Alarm and Event Monitoring (Real time connected devices only)
1. Provide the ability to configure whether a specific event will be treated as an alarm.
2. Provide ability to configure whether a specific event or alarm will be stored to the database.
3. Provide ability to configure a specific background and foreground color for each type of alarm (e.g. monitor point active, door forced, tamper) and/or any alarm source (e.g. all alarms from devices in a specific building can be a specific color).
4. Provide the ability to configure a distinct alert sound for each alarm or alarm type.
5. Provide ability to show instructions, on a per alarm basis, for how to handle the alarm.
6. The system shall be capable of routing individual alarms to specific monitoring operators.
7. Provide ability to automatically show live video from a camera associated with an alarm.

I. Event Photos
1. Provide the ability to automatically display the stored photo image of a card holder for card usage at a specific location or locations.
2. The cardholder photo image shall be activated based on an alarm priority level, and/or cardholder attributes (e.g. personnel type) and/or device attributes (e.g. device address or type). Information shall include, but not be limited to the card holder's primary image, time, date, event description, device name, and cardholder name.

J. System Administration
1. Hardware Configuration.
a. Provide a hardware identification module where system hardware definitions shall be built using a graphical tree structure, similar to the typical folder tree used to represent a file system in window organized operating systems.

b. Provide functionality to execute commands appropriate for the device (e.g. start the driver, download firmware to the hardware device, unlock the door, etc)

c. Provide a wizard allowing standard access control panel configurations across multiple master and slave devices to walk an operator through configuration and to automatically build devices within the tree.

2. Profiles
g. Each authorized operator shall be assigned one or more operator profiles by the system administrator. Operator profiles determine which system software functions are available to the logged-on operator. Unavailable software functions or features shall be grayed out on the menus or shall not be visible to that operator.

3. Log-ins
a. Manual logon shall require an operator to enter their name and password to enable the software to become active.

b. Provide the ability to assign effective and expiration dates for a login.

c. Software modules, menus, and data shall be dynamically loaded based on the currently logged on operator profile.

d. Display language shall be selectable from the login screen.

4. Reports
a. Provide various types of reports to include the following: Card use reports, Manual operations reports, Alarm reports, Historical reports, Time & Attendance reports, Detailed reports, Summary reports, Statistical reports, etc.

b. Provide control over which fields will be displayed in the report, depending on the type of report.

c. Allow for filtering of the information to be included in the report (e.g. time range, locations, personnel, credentials, etc).

d. Provide control over who is allowed to run a report.

e. All reports shall be capable of display on-screen, printed, or sent by e-mail on a daily, weekly, or monthly basis. All event reports can be automated to be generated and sent at a specific time for a specific time frame.

f. The system shall support at a minimum the following report formats: PDF, CSV, Text (tab-delimited) and HTML.

K. Graphical Maps

1. The system shall provide Graphical Map Creation and Editing Software that must allow system administrators to import customized map backgrounds of their facility and to attach custom icons to those maps.
2. The system shall support real time graphical maps that can be configured to appear in the alarm monitoring client workstation, either on command, or when specified alarms are selected for acknowledgment.
3. Maps shall be dynamic so that the icons/maps do not have to refresh or repaint each time a new alarm arrives in the system. The system shall give operators the ability to acknowledge alarms from the graphical map without going back into the alarm monitoring window.
4. The maps shall provide the ability to import floor plan graphics stored as a scalable vector graphic (SVG), PNG, JPEG, PDF, TIF or in BMP format.
5. Map device icons shall have the ability to dynamically change color to reflect the current state of the device.
6. The maps shall be capable of linking floor plans together in a hierarchy fashion.
7. Provide the ability to click on an alarm to bring up live and/or recorded video.

L. Video Interoperability

1. General

h. Provide ability to program descriptions and camera titles for all system cameras.

i. Provide the ability to show live, or recorded video manually or automatically based on an alarm, programmed trigger, or card access event.

2. Digital Video Server

a. Provide ability to interface to a network of digital video servers.

b. Camera functions such as pan/tilt, lens control, limits, and home position shall be supported by the system. Unless specific programming dictates otherwise, an operator shall be able to control these functions for all cameras so equipped.

c. A “live view”, the Digital Video Server shall be displayed on the system computer without the use of any add-in video capture card.

d. Upon recognition of an alarm, the system shall be capable of switching and displaying a view from either the CCTV camera or video from the digital video server camera that is associated with the point/event.

3. The PACS shall be compatible with the following video manufacturers: Dedicated Micros, March Networks, Salient, Exacq, Milestone, Mobotix, and Pelco. (Specific Models or Software version may require additional integration)

M. Software Support

1. The PACS software components shall be alterable and upgradeable at any time, depending upon system expansion requirements, without having to be discarded and replaced.
2. Completely new versions of the management system software intended to replace older versions of the system management software shall provide integral utilities to import all existing personnel records and image files, system hardware files, operator and historical log data files from previous software versions without requiring such data to be manually entered by system operators.

N. Device Status (Real time connected devices only)

1. The system shall support a real-time Device Status window that graphically depicts all field hardware devices that are configured in the system.
2. The Device Status window shall list all workstations, drivers, controllers, sub-controllers, secured areas, access points, readers, door contacts, door locks/strikes, REXs, monitor points, control points, DVR, and cameras.
3. Operators shall be able to sort any column in ascending or descending order. Operators shall also have the ability to choose what types of devices to display in the graphical system status tree or list window.

O. Automation Rules

1. Provide a means for automating one or more of the following actions on a periodic, manual, or event triggered basis:

a. Run any report that exists in the system.

b. Execute any driver or device command that can normally be executed from the hardware tree. As an example, execute a database backup for a driver, execute a “Set Time” command for a controller, or change the reader mode (e.g. Card Only) for an access point.

c. Perform a CSV import of Personnel/Badge records.

d. Perform a group edit of Personnel or Badge records. A group edit applies a set of specified field changes to a group of records that satisfy the criteria in a specified filter to a narrow set of records, such as: personnel type, badge expiration date, organization, access level, badge design, etc.

e. Execute an external command. An external command is any command that could be executed from the operating system command prompt.

2. Allow multiple actions to be executed within the same automation rule.
3. For event triggered rules, provide a filter that specifies the exact criteria for the type of event that will cause the automation rule to fire. The filter can specify, among other things, the exact log code of the event, the time window that the event must occur in, the source device of the event, specific cardholder information associated with the event, etc.
4. Provide the ability to e-mail, FTP, export to syslog server, or export to a file on the server selected events that occur within the system. Events shall include all events/alarms defined within the system software such as Monitor point active, Door forced open, and tamper alarms.
5. This capability provides the administrator the ability to support a global linkage feature whereby any input, output, or event could be linked to any other input, output, or event in the system. Input/Output linkages shall be able to span across controllers and across the system network.

P. Quick Launch
1. Provide an editor that allows you to build customized windows providing a central location for monitoring and executing various functions - on one screen, at individual workstation locations.
2. The editor shall allow the administrator to create any number of panels, where any one cell in the grid pattern can be populated with the status of a specific device, or with a button that will execute any one of multiple functions.
3. Provide a Quick Launch viewer that presents the panels that have been created by the administrator. The administrator shall be able to control which logins are allowed to see each Quick Launch panel.

Q. Help Assistance
1. The PACS shall provide a context sensitive help screen.

R. Approvals
1. The PACS shall be offer listings under UL-1076 and UL-294.

S. Web Clients
1. The PACS shall be accessible on a thin-client web application utilizing the following web browsers: Chrome, Firefox, Internet Explorer, Safari.

T. Database Import
1. Provide the capability to import Personnel, Credential and Access Level information from an existing PACS into the new system by using a properly formatted exported CSV file.

U. Prior Approvals
6. The PACS software shall be AccessNsite, or an equal that meets all requirements in this section, with a prior approval request submitted to the Architect a minimum of 14 days prior to bid date. Only PACS Contractors employing at least two (2) technicians with active factory certifications in the deployment and commissioning of an AccessNsite PACS (or equal) prior to the proposal request are eligible to submit a bid for this project.

2.3 MANUFACTURERS

	ITEM	SPECIFIED	APPROVED EQUIVALENT
1.	Software	AccessNsite	No Substitution
2.	Licenses	AccessNsite	No Substitution
3.	Panels	AccessNsite	No Substitution
4.	Cards/Fobs	aptiQ, HID	No Substitution
5.	Card Readers	aptiQ, HID	No Substitution
6.	Integrated Access Control Locks	Schlage, ASSA ABLOY, Best Lock	No Substitution
7.	Video Intercom Entry	AiPhone	No Substitution

2.4 SPECIAL REQUIREMENTS

A. Electrified Locksets
1. All locksets to be grade 1 heavy-duty mortise or cylindrical. Refer to Section 08 7100 and PACS below for electrified locksets.
2. Terminate, test, and commission all electrified locksets and PACS devices.
3. Provide all manufacturer recommended cable for Electrified Lockset and Intelligent Integrated Access Control Locks from PACS Panel to and through the door as necessary.

B. Electrified Exit Devices
1. Refer to Section 08 7100 and PACS below for all electrified exit devices.

2. Terminate, test, and commission all electrified openings.
3. Provide all manufacturer recommended cable to electrified exit devices.

C. Card readers
1. Coordinate with Section 08 7100 for all card reader locations and proper operation. Card Readers may appear in Division 8, but are to be supplied by Division 28.
2. Mount readers per ADAAG and ANSI 117.1 handicap accessibility requirements for height above finished floor.
3. Provide all manufacturer recommended cable for card readers from PACS panel to card reader locations.
4. Terminate, test, and commission all card readers.

D. Integrated Access Control Locks
1. Coordinate with Section 08 7100 for all integrated access control lock locations and description of operation. These integrated locks with card readers onboard may be shown in Division 8, but are to be supplied by Division 28.
2. Supply, terminate, test, and commission all Integrated Access Control Locks.
3. Provide all manufacturer recommended cable for Integrated access control locks, unless connected to Owner Supplied Local Area Network (LAN) and then coordinate IP address(es) required from Owner Representative.
4. Provide all required Panel Interface Modules (PIMs) and Gateways (GWE) for a working system. PIM and GWE locations and quantities are the responsibility of this division. Wireless coverage test shall be conducted after building construction is 95% complete.

E. Biometric Reader Support
1. The PACS shall be capable of supporting Biometric Reader data via compatible interface. If specified on this project in the PACS Schedule, these devices shall be capable of storing biometric profiles onboard and offer a PIN function to minimize PACS latency.

F. Control Panels
1. Coordinate with General and Electrical Contractors for rack or wall space required for panel installation
2. Coordinate with Electrical Contractor for wire runs from panel location to all PACS devices.
3. Supply, install, and test all cable for PACS devices. PACS Contractor shall supply wiring paths, and wire types for Electrical Contractor.
4. **A minimum of an additional 10% capacity shall be built into the system controller architecture.**

G. Power Supplies
1. All electronic equipment within the PACS shall continue to operate for at least TWO (2) hours in the event of A/C power failure. The PACS contractor shall take into consideration traffic loads and point loads when determining the size of the Uninterrupted Power Supply (UPS) as backup power. Provision of the UPS shall be under this scope, unless the building design offers a centralized emergency power source and connectivity is made available to the PACS.
2. Coordinate with section 08 7100 for all power supplies. DO NOT DUPLICATE power supplies. Verify with section 08 7100 amperage and voltage required to operate PACS devices. Power supplies may appear in Division 8, but are to be supplied by Division 28.
3. Coordinate 110/120 VAC connections required for all power supplies with Electrical Contractor.
4. Terminate, test, and commission all PACS devices to power supplies in Section 08 7100. Notify in writing the Architect and Owner Representative if additional electrical infrastructure is required, but not shown in plans or drawings.

H. Software Licensing
1. All software related licensing, support agreements and control operational licenses to be provide for a period of Two (2) years.
2. Disclose all support agreements and costs associated with the agreements listed in G.1 above for years 3, 4, and 5 at the time of bid.

I. Credentials
1. This Scope of Work shall include a minimum of five hundred (500) Contactless RFID cards, unless instructed differently by the Owner representative and transmitted in writing.
2. The Credential format shall be 13.56 Mhz Smart format, unless a different Owner design standard is defined (required meeting in Paragraph 1.3.E). ONLY the secure sector may be used to read user and identity information. Any factory deployed Encryption Keys shall be under the complete control of the Owner. Any failure to share credential encryption keys with the Owner may constitute a breach of contract.
3. The Credential Format must be compatible with ~~both HID or aptiQ~~ wall mounted card readers.
4. The Credential shall have a 37 bit format, unless a different Owner design standard is defined (required meeting in Paragraph 1.3.E). The Facility Code and any Sequential Numbering requirements shall be provided by an Owner Representative prior to time of order.

2.5 MATERIALS

A. Screws and Fasteners: Provide all screws and fasteners of the proper size and type to properly anchor or attach the item of hardware scheduled. Provide all fasteners with Phillips heads, unless security type screws (spanner-head or torx-head) are hereinafter specified.

2.6 FINISHES

A. Hardware finishes as follows:
1. 626 – Satin Chrome-plated.
2. 630 – Satin Stainless Steel

2.7 CABLE

A. Cable shall comply with PACS and Door Hardware Manufacturer specified requirements and supplied, installed, and tested. Cable shall be in compliance with all local and national codes affecting cable types, locations and penetrations.

B. Section 28 10 00 is responsible for establishing all cable runs, termination, testing, and commissioning for all PACS devices.

PART 3 - EXECUTION

3.1 EXAMINATION

A. Examine doors and frames, with Installer present, for compliance with requirements for installation tolerances, labeled fire door assembly construction, wall and floor construction, and other conditions affecting performance.

B. Examine rough-in for electrical systems to verify locations of wiring connections, before electrified door hardware installation.

C. Proceed with installation only after unsatisfactory conditions have been corrected.

D. Verify all wiring paths for PACS devices.

3.2 PREPARATION

A. Coordinate with Owner Representative for all IP address, network switch ports and permissions, Firewall settings and other Owner Supplied LAN equipment and settings required for an operational PACS.

B. Coordinate rack space and/or wall space required for PACS devices.

C. Verify any Owner provided equipment, or network infrastructure meets, or exceeds manufacturer's requirements.

D. If Virtual LAN's or Virtual Machines provided by the Owner are used in deployment of the PACS, verify these system components are compatible with manufacturer's requirements.

E. Verify Owner supplied servers, workstations and laptop PC's are compatible with all PACS devices and software.

3.3 INSTALLATION

A. Installation shall be by a qualified installer with a minimum five (5) years' experience in the installation of commercial grade PACS devices. Manufacturer's instructions shall dictate templating and installation.

B. Door Hardware Supplier (08 7100) shall provide all necessary mounting brackets, special templates, shoe supports, spacers or other special items required to make mechanical door hardware function together. If shim kits or drop brackets (etc.) are required for proper door function, these will be the responsibility of the Door Hardware Supplier (08 7100) for a complete installation.

C. Mounting Heights: Mount Integrated Access Control Lock units at heights indicated in following applicable publications, unless specifically indicated or required to comply with governing regulations:
1. DHI's "Recommended Locations for Architectural Hardware for Standard Steel Doors and Frames."
2. Wood Doors: DHI WDHS.3, "Recommended Locations for Architectural Hardware for Wood Flush Doors."

D. Prior to hardware installation, the General Contractor shall setup a meeting with the Door Hardware Supplier, Installer and the PACS Contractor to ensure all understand the manufacturer's installation requirements for all items.

E. PACS equipment shall be installed to comply with manufacturer's written instructions. Where cutting and fitting are required, the PACS contractor shall insure that all such preparation is done to minimize cosmetic impact. If installation requiring cutting onto or into surfaces that are later to be painted or finished, the PACS contractor shall coordinate removal, storage, and reinstallation of surface protective trim units (trim rings, etc.), as required. Do not install surface-mounted items until finishes have been completed on substrates involved.
1. Set units level, plumb, and true to line and location. Adjust and reinforce attachment substrates as necessary for proper installation and operation.

2. Drill and countersink units that are not factory prepared for anchorage fasteners. Space fasteners and anchors according to industry standards.

F. Boxed Power Supplies: Coordinate with Section 08 7100 and Electrical Contractor to locate power supplies as indicated or, if not indicated, above accessible ceilings. Verify location with Architect prior to installation.

G. Work with all other trades to establish wiring paths for all PACS devices.

H. Elevator Control. Supply, install, terminate, and commission Card Readers as shown in PACS hardware sets mounted inside Elevator Cab for Elevator Floor Control. The General Contractor shall coordinate with the Elevator Contractor to provide the proper size and number of conductors to be installed in the carrier cable. I/O shall be provided by the PACS contractor to accommodate the functionality defined by the PACS design. Coordinate all activities with the Elevator Contractor.

I. Wireless Integrated Locksets. Supply, install, terminate and commission Wireless Integrated Locksets using the appropriate Wireless Access devices: PIMs, GWE's or WiFi Access Points. Coordinate with Owner's LAN/WAN support for all Network Switch and POE connections. Ethernet and other associated cables for the Wireless Integrated Locksets shall be the responsibility of the Division 28 contractor.

3.4 FIELD QUALITY CONTROL

A. Perform final inspection with hardware installer and hardware supplier present to ensure correct installation and operation, and check for damaged or defective items before installing additional PACS devices. Observe and inspect that all hardware has been installed to its correct destination in proper working order.

B. The PACS contractor will perform at least one test of the system after commissioning with the Owner and General Contractor present to confirm problem-free operation and compliance with the design specifications in this Section.

C. Install, terminate, test, and commission all devices listed in section 28 10 00. Coordinate with Operational Description, Section 08 7100 supplier and Owner Representative. Use operational description and drawings as a guide to verify turn-key PACS operation.

D. Independent PACS Consultant: Owner reserves the right to engage a qualified independent PACS Consultant to perform a separate independent inspection and to prepare an inspection report.

3.5 ADJUSTING

A. Initial Survey: Check each operating item of door hardware and each door to ensure proper operation or function of every unit. Report items out of adjustment, or that do not operate as intended to General Contractor.
1. Ensure all PACS openings have been adjusted properly prior to commissioning and system testing.

B. At completion of the installation and prior to Substantial Completion, final adjustments should be made to all PACS devices. Leave all hardware clean and fully operable. Should an item be found to be defective, it shall be repaired or replaced as directed.

3.6 CLEANING AND PROTECTION

A. Clean adjacent surfaces soiled by PACS installation.

B. Clean operating items as necessary to restore proper finish.

C. Provide final protection and maintain conditions that ensure all hardware is without damage or deterioration at time of Substantial Completion.

3.7 DEMONSTRATION & TRAINING

A. Provide a minimum of four (4) hours of software instruction to Owner's Personnel in proper setup and operation of the PACS at final installation.

B. In addition to instruction, after PACS is installed and adjusted, the PACS contractor shall demonstrate the functionality and proper use to Owner's Personnel of the PACS and its Graphical User Interface (GUI).Warranty

C. Refer to Division 1 of this Specification Manual for project warranty provisions.

D. The PACS Contractor shall provide One year of warranty support service as part of this scope. Maximum response time will be two (2) business days. As part of the Owner turn-over process, the PACS Contractor shall discuss extended and/or faster response alternatives available beyond the scope of this work. All such agreements shall be direct with the Owner and outside of the scope of this Project.

3.8 PACS EQUIPMENT SCHEDULE

A. The hardware sets listed represent the design intent and direction of the owner and architect. They are a guideline. Discrepancies, conflicting hardware, operational gaps and missing items should be brought to the attention of the architect with corrections made prior to the bidding process.

HARDWARE AND EQUIPMENT SCHEDULE

TBD

END OF SECTION