Architectural and Engineering Specification for Video, Security and Access Control Software

Senstar Symphony™

This document is intended to provide performance specifications and operational requirements for the Senstar Symphony Common Operating Platform. It is written in a generic format. These specifications may be copied verbatim to form a generic procurement specification.

SECTION 28 13 00 ACCESS CONTROL SOFTWARE AND DATABASE MANAGEMENT

PART 1 GENERAL

1.1 System Summary

A. The contractor shall install an Access Control Software (ACS) solution that provides access control, alarm monitoring, graphical map or floor plan overlays, and security control functions.

1.2 Intent

A. It is the intent of this specification to identify a complete ACS for facility access and egress, alarm monitoring, facility control, and interoperation with other specified products with capabilities as indicated.

B. The purpose of this specification is to identify the required ACS features, capabilities, and functions. It is understood that terminology, system architecture, and application design can vary between system manufacturers. However, the design defined in this document is preferred. Any exceptions shall be viewed as non-compliant.

C. It is expected that the majority of the features requested will be provided in the manufacturer's standard product offering. Bespoke systems or those requiring extensive modifications shall be viewed as non-compliant.

1.3 References

The following acronyms and abbreviations are used in this document:

- ACS: Access Control Solution
- IP: Internet Protocol
- LAN: Local Area Network
- NFC: Near Field Communication
- ODBC: Open Database Connectivity
- OSDP: Open Supervised Device Protocol
- PIDS: Perimeter Intrusion Detection System
- REX: Request to Exit
- SMTP: Simple Mail Transport Protocol
- UPS: Uninterruptible Power Supply
- VMS: Video Management Software

PART 2 PRODUCTS

1.4 Electronic Access Control System

A. The contractor shall supply an IP-based Access Control Solution (ACS).

B. The ACS shall be used to provide scalable access control, alarm monitoring, graphical map/floor plan overlays, and security control functions.

C. The ACS shall support integration with Senstar Symphony Common Operating Platform, designed by Senstar Corporation.

D. Unless otherwise noted, the contractor shall provide all materials, equipment, hardware, software, modules, accessories, and other options required to deliver a complete turnkey solution.

1.5 Manufacturers

A. The Senstar Symphony Access Control software from Senstar Corporation (www.senstar.com) meets the software-specific requirements stated in this document.

1.6 System Architecture

A. The ACS shall have an Open Database Connectivity (ODBC) compliant design that facilitates the sharing of data with external databases and the integration of the HID® Aero™ Controllers

B. Operating system:

1. The ACS shall run as a native application on a current version of the Microsoft Windows® operating system and support its updates, patches, and hot fixes.

2. The ACS shall be able to work in a virtual server environment such as VMWare or Microsoft Hyper-V.

C. Database:

1. The ACS shall make use Microsoft databases such as Microsoft Access, Microsoft SQL Express, or Microsoft SQL Server.

2. The database shall be 'Open Database Connectivity' (ODBC) compliant to facilitate the sharing of data with external databases and the integration of a wide range of security hardware.

3. The ACS shall have the ability to import and export personnel information based on time schedules, TCP commands, and file date/time modification.

4. Import capabilities shall include:

a. The ability to import access control data including personnel, hardware, and time schedules.

b. The ability to import using an 'Open Database Connectivity' (ODBC), Text or CSV file.

D. ACS server computers:

1. The ACS server and operator workstations shall use industry standard computer hardware (PC) running a physical or virtual Microsoft Windows® operating system.

2. The ACS server shall provide centralized security control, alarm and event monitoring and response, as well as database configuration and management for all intelligent controllers and associated sub-controllers within the user's facility or facilities as specified.

E. The ACS shall support the use of a Common Operating Platform (COP) for the unified integration of video, security, and access control operator functions.

1.7 Intelligent Controller

A. The system shall support HID® Aero™ X1100 main controller and connection to X100, X200 and X300 sub-controller module.

B. The system shall support HID® Aero™ X1100 main controller configured in VertX dialect for connection to HID® VertX™ V100, V200 and V300 sub-controller modules.

1.8 Software Licensing

A. The ACS shall follow a flexible, per-door strike licensing model in which additional devices can be added to the system on a per-door strike license basis, without the need to purchase a group of licenses or other type of license.

B. All licenses shall be bound to the server, not to individual devices or device controllers. Replacing a door strike or other device shall not require a new license to be purchased.

C. Operator workstations shall not require a license and shall be available on an unlimited basis for licensed systems.

D. There shall be no cost for mobile devices connected to the ACS.

1.9 Administration Module Software User Interface

A. General requirements:

1. System shall allow authorized operators to define and modify system operating parameters, such as cardholder records, doors, time codes, monitor points, and alarm conditions.

2. The ACS shall be multi-user, multi-tasking, allowing the simultaneous use of multiple operator workstations. The ACS shall allow any number of operator workstations to be in use at the same time.

B. Language support:

1. The ACS administration software shall support the following languages: English, French, Portuguese, Spanish, Finnish, Spanish, German, Arabic, Swedish, Urdu and Chinese.

2. A trained dealer or integrator shall be able to customize the language by editing a text-based localization file.
3. The ACS software shall provide a standard Windows®-style graphical user interface that makes extensive use of graphical elements such as toolbars, icons, and pull-down list boxes. System commands and functions shall be available by using a mouse-type pointing device.

1.10 Access Control Features

A. The ACS shall provide card access control of doors, gates, elevators, and other portal control locations as defined herein.

B. All card readers shall read the credential information programmed in physical access cards as well as Mobile IDs, through Bluetooth and NFC, presented to a reader and pass verified information through an intelligent control processor for authorization. The intelligent controller shall maintain all card information locally and verify reader information received against stored criteria.

C. The HID® Aero™ controllers shall support multiple different biometric readers that may or may not be used in conjunction with an access card credential. These shall include but not be limited to fingerprint, face recognition, iris identification, and voice/hand geometry. These shall be supported via either dedicated servers or via the system controllers depending on where the template(s) are stored.

D. The ACS shall include door held and door forced conditions with configurable door held times up to 2048 seconds. The ACS shall be configurable to allow for masking of door forced and door held conditions. The ACS shall include the ability to configure an unlimited access grant time to be used in conjunction with Extended Grant Time Settings (American Disability Act mode). The Extended Grant Time Settings shall be configurable per portal or reader and card holder.

E. The ACS shall include the ability to configure up to 15 door de-bounce time settings of up to 255 milliseconds. The ACS shall contain the ability to assign up to 8 door reader modes including: disabled, unlocked, locked (no access, allow REX), correct facility code required, card only, pin only, card and pin, card or pin for use with the HID® Aero™ platforms.

F. The ACS shall include the ability to configure the offline reader modes to include: no offline mode, locked down (no access, no REX), unlocked, no access allow REX, correct facility code required for use with the HID® Aero™ platforms.

G. The ACS shall provide the capability for an authorized operator to assign an alphanumeric description (name) to each hardware hierarchical device. Description name fields shall allow for a maximum of 50 alphanumeric characters. The Description name field shall be used on System menus, displays and reports.

H. The ACS shall support up to 500 regionalized access levels per controller group with up to 1000 controller groups. The ACS shall support the ability to assign alphanumeric characters to each access level. The Access Level name shall allow a maximum of 50 alphanumeric characters. The ACS shall allow for Access Control Reader Groups or individual readers to be added to access levels using a drag and

drop method or selection by menu. The ACS shall allow for pre-defined time schedules to be associated with an individual reader or access control reader group. The ACS shall allow for a reader or access control reader group to be added to more than one access level with a different time schedule.

I. The ACS shall support 'Access Control Reader Groups', defined as a placeholder/folder to store one or more Readers. An Access Control Reader Group shall be an operator specified combination of one or more portals or doors associated to a time schedule. The ACS shall allow the assignment of portals or doors to the Access Control Reader Groups with a drag and drop function or maybe added from a menu selection. The ACS shall allow an operator to define Access Control Reader Groups as required without limiting System expansion.

J. The ACS shall provide the capability for an operator to assign an alphanumeric name to each Access Control Reader Group. The Access Group name shall be used on System menus, displays and reports.

1.11 Anti-Passback Feature

A. The ACS shall support deployments where card readers are used for both entrance (ingress) and exit (egress) and shall allow each card reader to be operator-defined as either an 'entry or 'exit reader'. The ACS shall require cardholders using a credential at an 'entry' reader to subsequently use the credential at an 'exit' reader before the credential can once again be used at an 'entry' reader, creating an Anti-Passback (or APB) condition. Cardholders attempting to use cards without first exiting the Anti-Passback area shall be denied access and shall cause a 'Passback Violation' message to be sent to the central System for operator notice. If so configured, Passback Violations shall create an Alarm Condition causing an immediate report generated for operator alarm response.

B. The ACS shall provide a Passback 'forgive' feature that can be activated by an authorized operator. The Passback forgive feature shall reset the Passback status of any card to a neutral condition (neither 'in' or 'out' of the anti-Passback area), allowing the Passback sequence to be restarted.

C. The ACS shall allow the Anti-Passback feature to be enabled and disabled upon authorized operator command,

D. The ACS shall allow the APB mode to automatically be "reset" by a Time Code without the need to use an "exit" reader.

E. A special Anti-Passback set flag shall be provided in the access control personnel record file that allows and authorized operator to specify a cardholder as Anti-Passback exempt. If a cardholder has the Anti-Passback exempt flag set, they may enter or exit any Anti-Passback area without causing an Anti-Passback event or alarm.

F. The ACS shall allow Anti-Passback by time such that a reader may not be used again before a pre-configured window of time has elapsed. This shall be supported on HID® Aero™ based controller hardware.

G. The ACS shall support “Nested Anti-Passback” such that readers may be used to require a user to enter and exit an area within a certain time frame. This shall be supported on HID® Aero™ based controller hardware

1.12 Elevator Control Feature

A. The ACS shall support elevator access control based on user controller group requirements and configuration. The supported access controller for Elevator Control shall ONLY be HID® Aero™ controllers.

B. The ACS shall allow outputs from elevator car floor selection buttons to be connected as monitor point inputs to the ACS to identify which floor was selected by each cardholder. Once a floor is selected the HID® Aero™ controller shall automatically reset all requests until another authorized cardholder selects another floor.

C. The elevator control feature shall provide a fully distributed functionality allowing managing access requests and activating floor selections, even when an intelligent controller is offline with regards to ACS server connectivity. The ACS shall not rely on the ACS server to provide elevator control functions. Systems that use a central computer for elevator control decisions shall be viewed as non-compliant.

1.13 Digital Keypad Features

A. The ACS shall provide two specific keypad control features, keypad for access control and display keypad for secure area access and management.

B. In access control application, the ACS shall permit the use of digital keypads as an alternate or supplemental access control devices. Keypads shall provide no fewer than twelve numeric keys. Operation of digital keypad shall require the entry of a valid Personal Identity Number (PIN). The PIN for each user shall be unique and definable by operator. These keypads may use fixed numeric keypads or scrambled keypads.

C. PIN Keypads shall be capable of different mode assignments with access control readers. An operator may change a PIN keypad mode by command or automatically by a pre-set time of day.

D. When in PIN Only Mode, entry of valid PIN number shall permit access. Use of an access card shall not be required in PIN Only Mode.

E. When in PIN Plus Card Mode, the entry of valid PIN number, plus use of valid access card shall be required to permit access. Use of access a card alone or use of a PIN number alone shall not permit access when in PIN Plus Card Mode.

F. When in Card Only Mode, the ACS will disable the PIN Keypad, allowing use of a valid access card alone.

G. In the alarm access applications, the ACS shall permit the use of digital keypads as an arm or disarm alarm access device as well as a user keypad command station. Alarm access Keypads shall provide no fewer than sixteen numeric and static keys with a two level 16-character LCD display for local user interaction and status.

Operation of digital keypad shall require the entry of a valid Personal Identity Number (PIN) or valid commands by the user. The PIN for each user shall be definable by an authorized operator.

H. Alarm access keypads shall allow an operator to configure secured areas and allow local users to 'Open and Close' secured areas based on pre-configured conditions. Open early, Open late, Close early and Close late. Alarm access keypad use shall allow the user to integrate alarm and access into a single integrated reporting and response System.

I. Alarm access keypads shall allow an operator to configure local controls to allow authorized users to active commands as well as Open /Close management. The ACS shall allow keypad commands to control any operator specified devices and controls by command code. Conditions such as open, close, lock, unlock, mask, un-mask, activate and de-activate shall all be assignable commands to a secured keypad area. Status and arm / disarm locations shall be displayed on the keypad LCD for pre-authorized users.

1.14 Definition of Access Privileges

A. The ACS shall use a flexible, modular method of defining "who, where and when" with regards to cardholder authorization to access or egress secured locations within a defined site.

B. As a cardholder is entered into the database the ACS shall automatically build a record and allow an authorized operator to assign access privileges. 'Who' shall be defined as the ACS defined cardholder.

C. Assigning an 'Access Level' to a cardholder record defines where and at what time (or when) that cardholder is permitted access within the facility or facilities.

D. The ACS shall allow multiple Access Levels consisting of a combination of Access Control Reader Groups, Temporary Access levels and General Access levels. The ACS shall allow for Time Schedules to be assigned to Access Levels in combination with Access Control Reader group(s).

E. The ACS shall allow for an automatic Temporary Access start and stop dates to be configured.

F. Assigning a 'Time Schedule' to readers and cardholders defines 'when' a cardholder will have access within the facility or facilities.

G. A Time Schedule shall be operator-specified combinations of Time Intervals and Days of the Week used to specify times that a card may be used to gain access throughout a facility or facilities. Each Time Schedule shall allow not less than twelve individual Time Intervals for each day of week for the Aero™ hardware. Holidays shall have multiple Time Intervals scheduled as well. The ACS shall allow for Holiday Time Schedule overrides by time schedule and interval.

H. Cardholder records, Access Levels and Time Schedules shall be definable by authorized System operators. To configure a Time Schedule the user shall select days of the week and hours of the day that will make up each Time Schedule. Time

Schedules shall also have 'Time Interval'. A 'Time Interval' shall be defined as a range of times that can be contained within a 24-hour day. (An example of a Time Interval would be: 00:00 - 22:00 and 22:15 – 23:59 / 12:00 AM – 10:00 PM and 10:15P M – Midnight). Time intervals shall maintain a precision of one minute (60 seconds) or less. The ACS shall allow an authorized operator to define as many Time Intervals as required by the installation with a maximum of twelve 'Time Intervals' per day for the Aero™ hardware. Time Intervals shall have the ability to be changed using a drag and drop graphic or by typing in the numeric time value.

I. A 'Holiday' shall be an operator-specified date treated by the ACS as a Holiday. A Holiday is defined as a single or multiple consecutive-day occurrence. On dates defined as a Holiday, the ACS shall use the time criteria specified for Holidays by a System operator. The ACS shall allow a System operator to specify Holidays as required by the site. The ACS shall provide for up to 8 holidays per time schedule. Systems that do not support 8 holidays per time schedule shall be viewed as Non-Compliant.

J. The ACS shall allow an authorized operator to assign an alphanumeric name to each Access Level, Time Schedule and Holiday. These names shall allow for a maximum of 50 alphanumeric characters. These names shall be used on System menus and reports.

K. The ACS shall allow an operator to establish an 'Activation Date' for each cardholder / card. The Activation Date shall be the date that access privileges associated with that cardholder / card shall take effect.

L. The ACS shall allow an unlimited number of cards to be assigned to a single cardholder/record

M. Cardholders attempting to use an access card before the Effective Date shall cause an Access Denied Time event condition message at the central System for operator response.

N. System shall allow the operator to establish a 'Deactivation Date' for each cardholder / card.

O. The Deactivation Date shall be the date that access privileges associated with that cardholder / card shall be denied upon usage of that card. Cardholders attempting to use an access card after the Expiration Date shall cause an Access Denied Time event condition message at the central System for operator response.

P. The ACS shall support vacation start and stop dates to temporarily deactivate a cardholder card while they are listed as being on vacation and away from their normal work area. Systems that do not have and automated vacation set shall be viewed as Non-Compliant.

Q. The ACS shall support a temporary access level assignment selection with automated start and stop dates. This allows an administrator or authorized operator to assign additional access rights to an individual for a specific number of day and automatically cancel the exception. Systems that do not have an

automated temporary access level assignment set shall be viewed as Non-Compliant.

R. The ACS shall allow for the automatic deactivation of cardholder records if the card has not been used within the designated “Days of Non-Use before Card Deactivation” value. This value is shall be configurable by the operator. This feature shall have the ability to be disabled if the operator so decides.

S. The ACS shall support multiple world time zones such that a system that crosses time zones will report the local time based on its local server time rather than the “host”.

1.15 Cardholder Records

A. The ACS shall provide a ‘Cardholder Record’ to store data for each cardholder in the system. The ACS shall provide capacity for as many records as required by the operator.

B. The ACS shall provide data entry screen (form) allowing the creation, editing and deleting of Cardholder Records. The Cardholder Record shall contain the following fields and functions as a minimum:

1. Lock/unlock records from/for operator editing.
2. ADD a new card record
3. COPY an existing card record.
4. Save a record or data entered.
5. Delete a record.
6. Perform group edits and allow for Card Templates to be created allowing for predefined values to be assigned automatically to any card record assigned the Card Template. The Card Templates shall have permissions assigned by profile. The Card Templates shall automatically update any records with any values modified in the Card Template.
7. Print Personnel reports
8. Download all or selected database changes to the effected Controllers.
9. Display online help on pertaining to the software

C. Each Cardholder Record shall include support for the following general access control fields:

1. Enable/Disable Flag: Shall be used to activate / suspend card access to a record by an operator without deleting the cardholder record.
2. Card Record Count: The ACS shall display a filtered and actual card record count allowing an operator to move up and down records using an ascending and descending slide in left-hand side navigation window
3. First Name: Shall show 1 to 50 alphanumeric characters, first name field.
4. Initial Field: Shall show 1 alphanumeric character, initial field.

5. Last Name: Shall show 1 to 50 alphanumeric characters, last name field.
6. Card Template: The ACS shall support pre-defined data entry forms (ie, templates) and allow for each record to be assigned to one. This feature shall allow the operator to pre-define data fields shared amongst cardholders with similar roles, thus reducing error and data entry time.
7. Card Number: 1 to 12-digit number assigned to the card. Cardholder number entry shall support an automated entry of card number thru use of an Enrollment Reader or manual number entry. The ACS shall support an unlimited number of cards assigned to each record/cardholder. The card number shall contain information on:
    a. Card number
    b. Status: Active/Lost/Returned/Deactivated/Terminated
    c. Activation Date: Shall show the date when access privileges are to begin.
    d. De-activation Date: Shall show the date when access privileges are to expire.
    e. Card Format type: Shall display a dropdown list to identify the type of card issued
    f. Facility Code: Shall display a text field to input the facility code value of the card
    g. Card Re-Issue Code: Last card issued count. The ACS shall support a card issue count for each card re-issued to a cardholder.
    h. Hot Stamp Number: Shall show 1 to 12 numbers only.
    i. PIN Number: Shall show 4 to 8 digits user defined Personal Identification Number, if used.
    j. Vehicle ID: Shall show a text field to store auxiliary information such as Vehicle ID or License Plate
    k. Last Modified: Shall be used to show last modification data and log-on operator.
    l. Access Levels window: Shall provide a simple way for operators to assign door access t based on Access Levels and Access Group Reader Groups. Show all Controller Groups, access levels and groups associated with the cardholder record.

D. Each Cardholder Record shall include support for the following employee info fields:
    a. Company: Shall provide a dropdown list of “Company” name using 1 to 48 alphanumeric characters. This field can be customized
    b. Department: Shall provide a dropdown list of “Department” name using 1 to 48 alphanumeric characters. This field can be customized

c. Title: Shall provide a dropdown list of “Title” name using 1 to 48 alphanumeric characters. This field can be customized.

d. Social Security#: Shall provide a textbox to store Employee Social Security numbers. This field shall be customizable and renamed if required to provide another unique ID number if so desired

e. Employee#: Shall provide a textbox to store Company employee number 1 to 20 alphanumeric characters. This field can be customized.

f. Email Address: Shall provide a textbox to store 1 to 40 alphanumeric characters. This field can be customized.

g. Date of Birth: The ACS shall provide a right-click calendar display to select date.

h. Date of Hire: The ACS shall provide a right-click calendar display to select date.

i. Work#: 15 telephone alphanumeric characters

j. Home#: 15 telephone alphanumeric characters

k. Address-1, 2: 2 lines 50 alpha-numeric characters each for address information.

l. Last Print: Shall be used to show the last date the record was printed by an operator.

m. Notes box: Shall provide a text box to allow operators to enter notes. Quick click button will input the timestamp of the note

E. Each Cardholder Record shall include support at least 20 custom data fields, each storing up to 50 alphanumeric characters each.

F. The ACS shall allow for a date/time-stamped notes table in general data entry.

G. Each Cardholder Record shall include support for the following advanced fields:

1. Operator: Allow the cardholder record to be associated/linked to the ACS operator.

2. Card Use Limit: This shall define the number of times the card may be used for access in each time period.

3. Guard Tour Flag: Shall be used to identify the card as a guard tour card.

4. Vacation Start Date: The ACS shall provide a right-click calendar display to select date. Cardholder card shall be suspended from access on this date.

5. Vacation Stop Date: The ACS shall provide a right-click calendar display to select date. Cardholder card shall be re-activated for access on this date.

6. Temporary Access Level Start Date: The ACS shall provide a right-click calendar display to select date. Cardholder shall be assigned the temporary access level on this date.

7. Temporary Access Level Stop Date: The ACS shall provide a right-click calendar display to select date. Cardholder's temporary access shall be removed on this date.
8. Trigger Code 1: The ACS shall allow cardholder to be assigned a Trigger Code value to specifically actuate Triggers for I/O programming
9. Anti-Passback Flag: Shall be used to allow a card access or egress in an anti-passback area without activating an operator notice.
10. Anti-Passback Exempt Flag: Shall be used to allow free access or egress in any anti-passback area without activating an operator notice.
11. ADA (Uses the Extended Grant Time) Flag: Shall be used to set momentary time for ADA persons, extending door lock and held open timers.
12. PIN Exempt Flag: Shall be used to set all cardholder reader access to card only.
13. Do Not Alter Current Anti-Passback Location Flag: Shall be used to hold a current anti-passback status for a cardholder when access is granted.
14. Do Not Alter Current Use Count Flag: Shall be used to hold a current use count on a specific area when access is granted.
15. Watch Window button: Allow operator to view most recent card usage activity for a cardholder
16. Assign Last Used Reader button: Allow operator to manually assign a cardholder their last used reader
17. Personnel Access button: Shall provide operator the ability to view a list of cardholders who should have access to a selected reader

H. The ACS shall use the Cardholder Identification Number as the primary key to uniquely identify the record in the database. The ACS shall permit the use of access card numbers as a key but shall not use access card numbers as the primary key unless defined by an operator.

I. The ACS shall provide a sorted list of card holders per Controller Group selected on the Personnel Manager screen. Sort keys shall allow the list to be sorted and displayed for an operator.

J. The ACS shall permit the use of access cards encoded in Wiegand formats of varying bit lengths from 26 bit to 75 bit and MiFare cards and their derivatives (HID®, Legic etc.)

K. Note: Card bit format limitations and constraints are controlled by the field hardware. It shall be the responsibility of the bidder to ensure that the field hardware proposed can meet the standards as set forth in the specification/RFQ.

L. The ACS shall allow up to 10 different access card numbers/credentials to be assigned to each cardholder record. The ACS shall not require that a separate cardholder record be created for each access card number. The ACS shall allow each access card number on the cardholder record to use a separate format.

Systems that do not support a minimum of 10 cards per cardholder record shall be viewed as Non-Compliant.

M. The ACS shall permit the creation of a Cardholder Record without requiring that an access card number be assigned. This feature shall allow a Cardholder Record to be created for “PIN Only’ users who will be assigned a PIN number (1 to 8 digits) only and not require an access card.

N. The ACS shall provide a hierarchical tree showing access level assignment for each cardholder in the Cardholder Record. This tree shall permit an authorized operator to list, and select, through ‘pop-up and drop-down Windows®’, any access level or access group defined in the ACS. To view access levels and access group shall not require an operator exit from the Cardholder Record screen to perform this function.

O. The ACS shall allow the operator to identify the Access Levels, Access Groups, readers and Time Schedules associated with each cardholder without requiring the operator to exit from the Personnel Manager screen.

P. The ACS shall allow for the automatic disabling of card records based on the configured “Days of Non-Use before Deactivation” value.

Q. The ACS shall allow for the Personnel Manager heading tags to be modified to reflect headings based on the customer’s request.

1.16 Partitioned Database Feature

A. The ACS shall provide the ability to establish multiple ‘Logical Views’ of the access control system and cardholder database. Each Controller Group shall permit viewing and/or modification of only certain cardholder record fields, access levels, access groups, hardware configuration, and other such data. This capability shall allow the creation of ‘Controller Group’, logical Sub Systems. The ACS shall allow an authorized operator to create as many Controller Groups as required for a site or multiple sites. Systems that do not support a Controller Group management set shall be viewed as Non-Compliant.

B. Each Controller Group shall have full System capabilities; and shall appear to the operator and operate as if it were an independent access control System. The typical Controller

C. Group may consist of a single building or multiple building; or a single department in multiple buildings, or a single department within a building which houses multiple departments.

D. Creation of sub-Systems shall be accomplished through System configuration and software partitioning of the database.

E. The ACS shall allow operator profiles to view, create, or edit data in only certain Controller Groups. As an example, a operator who is assigned an operator profile for access to Controller Group 1 shall only be able to view and edit database records affecting Region 1. This operator would be restricted from viewing and modifying other portions of the ACS database based on his or her operator profile.

An operator profile shall allow the operator to assign one or more Regions for operator access.

F. The ACS shall allow the ability to partition the hardware down to the device level. The ACS shall allow operator profiles to view, create, or edit hardware data for only those devices designated to the Operators profile. Systems without the capability of partitioning hardware at the device level shall be viewed as Non-Compliant.

G. Operator functions, which may be restricted by profile and Controller Group, shall include, as a minimum:

1. Adding, deleting, and modifying cardholder records
2. Locking and unlocking of doors
3. Arming and disarming of secure areas
4. Masking and unmasking of alarms
5. Printing reports
6. Configuration of access levels, time schedules, access groups, and other such system parameters.
7. Establishment of automatic door lock and unlock times.
8. Monitoring of alarm conditions from user defined doors and monitor points.

H. The ACS shall allow the assignment of any door, access group, monitor point, secured area, auxiliary output contact or other system element within a Controller Group.

I. It shall be possible to assign any door, access group, monitor point, secured area, auxiliary output contact or other system element to more than one region at the same time.

J. Operator access to specific Controller Groups shall be determined by the operator's username and password. The use of Controller Groups shall not prevent authorized system operators from making system-wide changes or generating system-wide reports.

K. As an example, it shall be possible for an authorized system operator to add/delete a cardholder from all sub-systems with a single entry. The ACS shall not require that a separate entry be made to add/delete a cardholder from each Controller Group. Systems that require data add/delete entries in multiple partitions within the application shall be viewed as non-compliant.

1.17 Interface to External Databases

A. The ACS shall be able to import information from existing data-compliant personnel databases. The purpose of importing this information is to minimize the need to manually enter data.

B. Import capabilities shall include:

1. The ability to import information from the databases for the initial load of the cardholder database; and for major loads of new information periodically.
2. The ability to update the cardholder database based on the import reflecting changes in employee status.
3. Import on updates/changes in the source database shall allow the ACS to automatically add cardholder records, delete cardholder records, modify access privileges, and change other information contained in the cardholder database.
4. The ACS shall allow said import to be scheduled by minute, hour or daily imports.
5. The ACS shall allow the import utility to be configured as a Windows® Service.
6. The ACS shall allow import of data from Open Database Connectivity (ODBC), CSV or text files.
7. The ACS shall allow for Human Resource (HR) Integration such as PeopleSoft HCM through the available API/SDK from the HR system for bidirectional updates
    a. New employee/user entered in the HR system will automatically add new record in the ACS thru the HR Integration
    b. Updates to employee/user in HR system will automatically download changes of the record in the ACS thru the HR Integration
    c. Deletion of employee/user in HR system will automatically disable/delete record in the ACS thru the HR Integration
    d. The system shall allow “pre-canned” pictures to be imported thus limiting the amount of re-work time that might otherwise be necessary for personnel data import utilities.
8. The ACS shall allow for direct Windows® Active Directory integration in real-time to populate Windows® AD accounts into the IS2000 Personnel database. Real-time updates to the IS2000 database will be triggered by information changes to the AD account on update/edits/status of the AD account

C. The ACS shall not require a System restart or ‘reboot’ for data imports or updates to the cardholder record database to take effect — updates shall be made automatically upon receipt of data, if so, configured by the user.

1.18 Door Control Features

A. The ACS shall be capable of unlocking and re-locking Doors and Door Groups upon command from an operator workstation.

B. The ACS shall automatically disable Door Forced conditions and ‘Door Open / Door Held’ conditions from doors that have been unlocked by an operator command.

C. The ACS shall be capable of automatically unlocking and re-locking Doors and/or groups of Doors based on Time Schedule and Intervals. The ACS shall be capable of

automatically disabling Door Forced conditions and Open-Too-Long conditions for Doors that have been unlocked by Time Schedule and Intervals.

D. The ACS shall provide the capability to selectively disable Doors upon command from designated operator workstations based on operator profile, username and password. Disabled Doors shall deny access to all cardholders.

1.19 Door Status Monitoring

A. The ACS shall monitor the status of each access-controlled Door to determine if a door is open or closed. If an access-controlled door is opened without the presentation of a valid card, the ACS shall generate a 'Door Forced' condition.

B. The ACS shall support an ADA (American Disabilities ACT) standard whereby a different shunt time can be set for a physically impaired person, so they can access with a longer held open / shunt time than other employees.

C. Where a card reader is provided only on the entry side of a door, the ACS shall allow the disabling of Door Forced monitor from the exit side of the door. Disabling of Door Forced monitor shall be accomplished using a request-to-exit input (REX). A REX input shall be a normally open dry contact input to the ACS, allowing connection of release buttons, motion detectors and other devices.

D. If the ACS is so configured, operation of a REX input shall disable the Door Forced monitor for a operator-specified period, allowing exit without causing a Door Forced condition. If the ACS is so configured, a REX input shall also be capable of unlocking the door. One REX input shall be provided for each access-controlled Door per door controller.

E. The ACS shall provide the capability to remotely disable REX features for each Door. Each REX shall be capable of being disabled automatically by Time Schedule, Triggers and Macros and upon command from an operator workstation.

F. The ACS shall support fully supervised End-Of-Line input circuits which are software programmable by the operator.

G. The ACS shall monitor the status of each access-controlled door to determine length of time a door is open after an authorized access grant. If the door is left open longer than an operator specified time period, the ACS shall generate a 'Door Open / Door Held' condition for operator notice.

H. The Door Open / Door Held timer shall be capable of being set for an operator-selected period of time between 1 to 4000 seconds. The Door Open / Door Held time period shall be individually selectable for each Door.

I. The ACS shall provide the capability to remotely disable the Door Open / Door Held monitoring feature for each Door. Feature shall be capable of being disabled automatically by Time Schedule, Triggers and Macros and upon a command from an operator workstation.

J. Door Forced and Door Open / Door Held conditions shall be immediately processed based on parameters pre-configured by the operator. If so configured, Door Forced and Door Open / Door Held conditions shall create an Alarm Condition; causing an

immediate report to be sent to a designated operator workstations through Alarm Manager for alarm acknowledgment; and causing other operator-specified System operations to occur.

K. The system shall support a minimum of three different states for any access control door/portal.

1. Door open
2. Door closed
3. Door closed, locked and secure

L. Any system that does not record the position of the door locking hardware shall be deemed non-compliant.

1.20 Alarm Monitoring Features

A. The ACS shall provide monitoring of contact inputs from door switches, motion detectors, and other sensors located at field locations. Each input shall be defined as an individual 'Monitor Point'. The ACS shall provide the capacity for a maximum of 10,000 Monitor Points.

B. Monitor Point inputs may utilize a supervised circuit requiring the use of an End-Of-Line (EOL) resistor circuit. The ACS shall allow an authorized operator to specify, through the ACS software, the EOL circuit requirements of each individual input.

C. Monitor Point inputs shall accept both normally-open and normally-closed dry contact input signals. Monitor Point inputs shall provide a minimum of three distinct states, including 'normal' (input is in normal or inactive condition), 'alarm' (input is in alarm or active condition), and 'trouble' (input is in fault or tamper condition).

D. Each Monitor Point shall be identified on System displays by a unique Monitor Point number. In addition, the ACS shall provide the capability for the operator to assign an alphanumeric name to each Monitor Point. Monitor Point name shall be a maximum of 50 alphanumeric characters. The Monitor Point name shall be used on System menus, displays and reports.

E. The ACS software shall provide an 'A Virtual Door Monitoring Feature'. The virtual door monitoring feature shall permit a REX input point to be logically associated in software with a Monitor Point and Auxiliary Output to create a 'Virtual' access door. This feature shall allow non-card reader doors to be monitored for both Door Forced and Door Open / Door Held conditions without requiring a card reader or card reader sub-controller.

F. Monitor Points shall be capable of being grouped for the purpose of alarm management. A Secured Area shall be an operator-specified group of Monitor Points.

G. The ACS shall provide the capability for the operator to assign an alphanumeric name to each Secured Area. Secured Area name shall be a maximum of 50

alphanumeric characters. The Secured Area name shall be used on System menus, displays and reports.

H. The ACS shall provide the capability to Arm (enable) and disarm (disable) secured areas by command from operator workstation. Time Schedule and Interval. Arm and Disarm commands shall be capable of being executed from pull-down menus, icons on status screen, through triggers and macros and icons on Custom Map Displays.

I. The ACS Operator shall be able to enable a Monitor Point allowing the Monitor Point to cause an Alarm Condition for operator notice, if point is activated or activates after enabling. The ACS Operator shall be able to disable a Monitor Point allowing the Monitor Point to activate without causing an Alarm Condition for operator notice. Monitor Points shall be capable of being armed and disarmed individually, and by Secured Area.

J. The ACS shall have a capability to automatically Arm and Disarm Monitor Points and Secured Areas by Time Schedule and Interval.

K. Triggers and Macros shall be capable of locking and unlocking any number of access-controlled Doors and Door Groups, change any number of card reader modes, enable and disable any number of Monitor Points and activate and deactivate any number of output points based upon a Monitor Point status change. Triggers and macros shall be operator configurable and shall use any Monitor Point status change, access condition change, keypad commands and/or cardholder trigger codes for conditions of change. Triggers and Macros conditions shall be stored at the controller level and function independently of the host, provided the download to the controllers is completed

L. The ACS shall allow the disassociation of hardware points for use as another device. This option shall be available with the Aero™ controllers only.

1.21 External Control of Secured Areas

A. The ACS shall allow Secured Areas to be Armed and Disarmed using card readers designated as ‘Arming Readers’. Presenting a valid access card to an Arming Reader shall toggle Secured Areas from armed state to disarmed state and vice versa.

B. The ACS shall allow Secured Areas to be managed for access into such areas using a ‘Keypad Display Terminal’. The ACS shall be capable of managing up to 64 secured areas from a single Keypad Display Terminal or up to 64 secured areas across multiple Keypad Display Terminals.

C. Keypad Display Terminal alarm management shall support secured area Open / Close conditioning, tracking operator defined secured area early and late open and early and late close status for each defined area.

D. The ACS shall allow Secured Areas to be Armed and Disarmed through the use of external hardwired controls (such as a key-operated shunt switch.) The ACS shall permit Monitor Points to be defined as a trigger to run a macro assigned to Arm or Disarm a Secured Area. As an example, when Monitor Point trigger / macros are activated, the Secured Area which it controls shall be disarmed. When a Monitor

Point trigger / macro is normal (inactive), the Secured Area which it controls shall be armed.

E. The ACS shall allow Auxiliary Output Contacts to function as Secured Area status outputs. Two types of outputs shall be capable of being defined:

1. Armed Status Output: Output contact operates when Secured Area is in Armed Condition (typically used for 'armed-status' indicator lights).
2. Secure Status Output: Output contact operates when all Monitor Points assigned to Secured Area are in normal condition (typically used for 'ready-to-arm status' indicator lights).

1.22 Activation of Output Upon Alarms

A. Through Triggers and Macros, all Alarm conditions, including Door Forced conditions and Door-Held-Open conditions, shall be capable of activating one or more Auxiliary Contact Outputs to enable operation of audible sounders, door alarm horns, and other such devices.

B. System shall permit the global relationship of Alarm Conditions to Auxiliary Outputs, where conditions occurring at one intelligent controller shall be capable of causing outputs to occur at any intelligent controller in the ACS. This will be configured/implemented through custom scripting using command/ini files.

C. The ACS shall allow operator to define how each output is to operate during each Alarm Condition. As a minimum, the ACS shall permit the following operating conditions all configured in a separate software module, Triggers and Macros. Systems that do not support fully configurable Triggers and Macros based on any System event/alarm shall be viewed as Non-Compliant.

1. Output tracks Alarm Condition / Event / Activity: Output activates when Alarm Condition is active and deactivates when Alarm Condition clears.
2. Output tracks acknowledgment: Output activates when Alarm Condition is active and deactivates when Alarm Condition is acknowledged by operator, even if Alarm Condition has not yet cleared.
3. Timed output: Output activates when Alarm Condition is active, and deactivates when Alarm Condition has cleared, or after a preset time period, whichever occurs first. Time shall be definable by operator for periods of between 1 and 300 seconds.
4. Access Events: Output activates or de-activates based on any access event/status change with time of day and other event conditioning.
5. Cardholder Event: Output activates or de-activates based on a cardholder trigger code and access event (granted or denied).

1.23 Trace Feature on Cardholder Access History

A. System shall provide a special Trace feature (Watch Window) that can be set individually for each cardholder. The Trace feature shall allow special real-time tracking of operator-specified cards. Use of a card that has been set for Trace shall be automatically logged, and if so configured, shall cause a special report to be displayed at operator workstation. Trace reports are special and are in addition to any regular report as the result of card activity, such as Valid Access or Invalid Access Attempt.

B. An automatic cardholder activity report and reader access report shall be standard selection in the cardholder file. Reader access reports shall be selected from the Event Manager display, cardholder file and graphic map icons.

1.24 System Reporting and Logging Features

A. The ACS shall provide an electronic log of events, recorded on a real-time basis as they occur. Events shall be recorded with date and time.

B. When intelligent controllers are in an ‘on-line (in communication with ACS server) status condition, System events shall be immediately sent to ACS server and written to the host database

C. When intelligent controllers are in an off-line status (i.e. not in communication with the ACS server), the intelligent controllers shall store (buffer) system events in controller memory. Events will be stored in memory to its capacity overwriting as needed in first-in/first-out mechanism. Each intelligent controller shall be capable of storing a minimum of 20,000 events in memory.

D. In addition to being stored, System events shall also have the capability to be immediately displayed at designated operator workstations, providing real-time reporting of all System events.

E. The ACS shall support standard network printing facilities to allow the use of any printer connected to the user’s local computer or network. The use of specific printers for specific types of reports shall not be required.

F. The ACS shall allow events to be selectively reported to operator workstations and Printers. As a minimum, the ACS shall allow the selective reporting of the following events: Alarm Condition, Monitor Point activity, Forced Door, Door-Held, Invalid Access Attempt, Passback Violation, Trace, Hardware Failure, Communication Failure, Tamper, Power Fail, etc.

G. The ACS shall provide the capability to generate a current System status report upon command from operator workstation. Status reports will indicate: current status of Doors, Monitor Points, and Alarm Conditions; current status of operator imposed commands such as Disarm, Unlock, Disable and the like; current status of timed System operations, such as timed Unlock, timed Disarm and the like; and the current status of equipment, communications, and power failure conditions.

H. All card access activity shall be logged at a minimum data retention period definable by the system operator. For Valid Access, Invalid Access Attempt, and

Trace conditions, the ACS shall be capable of logging the following information as a minimum: Door name and number; card number; and cardholder name (If truncated, shall be 12 characters minimum). For Invalid Access Attempts, the ACS shall display and log reason for rejection.

I. The ACS at a minimum shall log all Monitor Point and Alarm Condition activity.

J. All operator commands from operator workstation shall be logged, including Unlock, Re-lock, Arm, Disarm, Disable, Silence, Acknowledge, Reset, and other such operator commands. Log of Operator commands shall identify the operator who issued each command. The ACS shall log unauthorized attempts to gain access to the ACS, such as the use of an invalid password, including the terminal node and/or network address from which the attempt was made.

K. The ACS shall log all automatic System operations that occur by Time schedules, including Unlock, Re-lock, Arm, Disarm, and other such timed operations.

L. All System failures shall be logged including Hardware Failure, Communications Failure, Power Fail, and other such System conditions.

M. All operator configuration activity, such as modification to card/credential numbers, Time Schedules, Access Levels, Monitor Points, Cardholder Records, and other System data, shall be recorded to an Operator audit log. As a minimum, the operator audit log shall identify the type of data that was modified, old data, new data and identify the operator who modified it. The ACS shall allow the Audit report to be filtered by date and by operator.

N. System shall be capable of selectively displaying all System configuration data at an operator workstation screen, allowing the viewing of Cardholder Records, card/credential numbers, Doors, Time Intervals, Time Codes, Monitor Points, Door Groups, Secured Areas, and other configuration data. System shall provide ability for operator to selectively view specific types and numerical ranges of data all based on their user assigned operator profile.

O. System shall be capable of printing all System configuration data to printer, allowing print-out of Cardholder Records, Clearance Codes, Doors, Time Intervals, Time Codes, Monitor Points, Door Groups, Secured Areas, and other configuration data. System shall provide ability for

P. operator to selectively print specific types and numerical ranges of data all based on an operator's assigned operator profile.

1.25 Archival Data Storage and Backup Tools

A. System shall provide capability to fully backup complete System and database files, including cardholder, hardware, alarms and events databases, to the local computer or external / network storage disk/device. System shall provide a menu-driven backup and restore graphical user interface, with operator prompts, enabling backups and restore functions to be made while the ACS application program is running (when using SQL database only). The ACS shall allow the scheduling of backups and archives using configurable days for the backup to

automatically occur. Archiving of data shall be configurable to allow operator to retain up to 36 months of data in the live database.

B. Backups shall be capable of being initiated from any operator workstation. Backup capability shall be available without requiring that the ACS application be closed and backups shall not interrupt System operation or require restarting of the ACS server.

C. System shall provide for archival transfer of event data from hard disk to CD. Archival transfer shall load event data to the local drive or external / network location and shall clear event data from the on-line/live System database after verifying good archive copy. System shall provide a menu-driven utility to allow archival transfer. The ACS shall allow for configurable days and times for the archive process to occur automatically.

D. The ACS shall permit archival storage and back-up to external storage devices via the Users network.

1.26 Archival Database Retrieval Feature

A. The ACS shall provide an integrated database retrieval process for archive purposes. The database retrieval process shall include search and retrieval capabilities, enabling selective reporting from a previously archived database.

B. In addition to basic search tools, the database retrieval System allows the use of Structured Query Language (SQL) to conduct more advanced searches. The SQL used shall be an industry-standard type that is in common use. SQL queries shall permit access to all data stored in System Journal and well as all data in System configuration database including Cardholder Records.

C. Database retrieval reports shall be capable of being printed to designated printers upon operator command. Retrieval of data shall not interrupt System operations.

D. The ACS shall allow database retrieval reports to be exported in industry standard data formats capable of being exported into external spreadsheets, databases, and report analysis tools.

E. The ACS shall provide a menu-driven utility that enables the retrieval of journal data from archival storage, for the purpose of generating reports. Retrieval, reporting, and viewing of data from archival storage shall not interrupt system operation or require that the current event data be cleared from hard disk.

1.27 Quick Look-Up Feature

A. The ACS shall provide a method to quickly display the cardholder record and photo image for any cardholder based on cardholder name. This feature shall be available to authorized operators at any operator workstation.

PART 3 EXECUTION

1.28 System Installation

A. The Access Control Solution (ACS) shall be installed in accordance with the recommended procedures defined in the relevant manufacturer's documentation for the system, individual device or component.

B. Intelligent controller and sub-controller panel installation:

1. Install each panel in equipment closet locations as indicated. Install each panel at a location and height to facilitate ease of service.
2. Identify the software and hardware address of each panel with a permanent marking label installed on the exterior of the cabinet.
3. Neatly dress and tie all wiring within panel. Do not obstruct access to terminal strips and configuration jumpers with wiring.
4. Provide terminating resistor on all unused input connections.
5. Label all inputs and outputs with a permanent marking label.
6. Ground all shielded cables in accordance with manufacturer's instructions. Trim and wrap all unused shield wires to prevent shorting or inadvertent grounding.

C. Data communications:

1. Provide interconnection of ACS server, operator workstations, and intelligent controllers using the TCP/IP Ethernet network. Coordinate connections and IP addressing with Owners designated telecommunications representative.

D. Power supply installation:

1. Install all System power supplies at intelligent controller panel backboard locations as indicated.
2. Unless otherwise noted, all System accessories, such as REX motion detectors, door alarm horns, sounders and the like shall be powered from 12 VDC auxiliary power supply located at equipment backboard.
3. Unless otherwise noted, power all electric lock hardware from 24 VDC lock power supply located at equipment backboard. Do not power lock hardware from other power supplies.
4. Connect power supply fault output to input point on intelligent controller. Provide pilot relay where needed to provide dry-contact output from power supply.

E. Card reader installation:

1. Where possible, all card readers mounted outdoors shall be installed out of direct exposure to sunlight, rain, and snow.

2. Unless otherwise noted, card readers are to be mounted at a height of 40” above the finished floor (measured from floor to centerline of card reader.) to be ADA compliant.
3. Securely mount all card readers using tamper-resistant fasteners.
4. Card readers shall completely cover any electrical back box or other electrical rough-in. Provide trim plates, adapters and back boxes at locations where required.
5. Card readers shall be installed so that they are “low-profile” and protrude from the wall only a minimum distance.
6. Completely seal all exterior openings of outdoor mounted card readers to make weather-tight.
7. Make card reader field adjustments in accordance with manufacturer's instructions.

F. Connection to electric lock hardware:

1. Provide wiring and final connection to electric strikes, electric locks, transfer hinges, electric exit devices, detention hardware, and other such devices.
2. Provide diode for transient suppression across coils of electric locks, electric strikes, and relay coils.
3. Verify operating voltage and current requirements of all lock hardware with hardware supplier. Coordinate cable requirements and connection points. Thoroughly test the operation of all electric lock hardware for proper operation.
4. Install pilot relay to control lock hardware where current requirements of the hardware exceed the relay contact rating of the intelligent controller or where electrical isolation is required.

G. General device wiring:

1. Connect card readers, inputs, and outputs to intelligent controllers as indicated on the enclosure or otherwise indicated.
2. Card reader, door switch, request-to-exit, and lock output wiring shall be “home-run” and connected to a sub-controller as indicated on the enclosure or otherwise indicated.
3. Use standard and consistent wire conductor color-coding for device wiring. Use the same colors for each function throughout the project, for example: Red and Black colored wires always used for power, Green and Yellow colored wires always used for detection circuit, etc.
4. Install end-of-line resistors at detection device. End-of-line resistors shall be connected to flexible wire leads and be protected with heat-shrink tubing or equivalent. Direct crimp or wire nut connections to resistor are not permitted.

H. Interface to fire alarm system:

1. Fire alarm output module to be provided (under Division 16) at locations adjacent to security equipment backboards. Fire alarm output module will provide a single Form C dry-contact output rated at one ampere. Contractor to provide pilot relays as needed to provide additional contacts or greater current capacity.

I. Card reader control of elevators:

1. Coordinate installation of card access System for elevator with elevator installer.
2. Coordinate requirements for conductors in elevator traveling cables with elevator installer. Verify that conductor quantities and types are suitable for use with card reader.
3. Provide card readers to elevator installer for installation in elevator. Make final connections to card reader.
4. Provide relay interface circuit between Security Management System and elevators as indicated on drawings. Route cabling in the elevator machine room to locations designated by elevator installer.
5. With cooperation and assistance of elevator installer, fully test all elevator control functions. Provide assistance to elevator installer, as required to troubleshoot any elevator control related problems.

J. Special interface requirements:

1. "Fire Exit" Stair doors: These doors to have fail-safe electric lock hardware. Provide pilot relay at each 24 VDC lock power supply. Connect lock outputs at these doors in series with pilot relay contacts so that doors automatically unlock on fire alarm condition regardless of state of ACS output.
2. Card reader doors with automatic openers: Provide pilot relay connected to inside door opener actuator buttons. Activation of buttons shall cause activation of REX input as well as operation of automatic door opener.

1.29 Programming and Configuration

A. The system shall be configured in accordance with the manufacturer's recommended procedures as defined in the documentation for the system.

B. If bundled with a hardware, software may be configured prior to delivery and installation.

C. All device firmware shall be the most recent provided by the device manufacturer, or of a version specified by the ACS manufacturer.

D. All ACS software shall be delivered and installed with the manufacturers latest release version of the software.

E. The contractor shall provide initial programming and configuration of the software to make the ACS fully operational. Initial programming of the software shall include:

1. Installing and configuring ACS server and workstation software
2. Configuring interfaces to external systems
3. Creating and configuring:
    a. Operator accounts and permissions
    b. Graphical floor plans
    c. Alarm reporting and alarm routing
    d. Doors and device groups
    e. Individual input and outputs
    f. Input and output groups
    g. Clearance codes
    h. Schedules and operating modes

F. Input of all program data shall be performed by the Contractor. The Contractor shall consult with Owners Representative and Security Consultant to determine descriptor names and system operating parameters.

G. The Owner, with the cooperation and assistance of Contractor, will input the cardholder data for each access card.

H. Contractor shall maintain a complete, up-to-date backup of the ACS configuration and cardholder database. Backups shall be maintained throughout the programming period until final acceptance by Owner.

1.30 User Documentation

A. The manufacturer shall provide user documentation that explains how to install, configure, operate and maintain the software.

B. The Contractor shall maintain hard copy worksheets which fully document system programming and configuration:

1. Worksheets shall be kept up to date daily by Contractor until final acceptance by Owner.
2. Worksheets shall be subject to inspection and approval by Owner.
3. Contractor shall provide final copies to Owner prior to project close-out.

1.31 Training

A. The manufacturer shall offer professional training services to assist the organization in meeting their training requirements.

SECTION 28 23 00 VIDEO MANAGEMENT SYSTEM

PART 1 GENERAL

1.32 System Summary

The contractor shall install a scalable, standards-based Video Management Software (VMS) solution. The VMS shall include support for native (built-in) video analytics from the same manufacturer as well as dynamic events from ONVIF-compatible sources.

The VMS shall be installable on commercial-off-the-shelf (COTS) hardware that runs the Microsoft Windows® operating system. The solution must be scalable and have automatic failover capabilities for the video and database servers that do not require Microsoft Clustering technology.

The solution shall follow a flexible, per-camera licensing model in which additional cameras can be added to the system on a per-camera license basis, without the need to purchase a group of camera licenses or other type of license.

1.33 Quality Assurance

A. The VMS manufacturer shall perform a vulnerability assessment of its software.

B. The VMS manufacturer shall perform penetration (PEN) testing of its software deployed in a standard configuration.

1.34 Definitions

The following acronyms and abbreviations are used in this document:

- ACS: Access Control System
- API: Application Programming Interface
- COTS: Commercial-of-the-shelf
- DHCP: Dynamic Host Configuration Protocol
- DNS: Domain Name System
- FPS: Frames per Second
- FTP: File Transfer Protocol
- H.264 (Video Compression Format)
- H.265 (Video Compression Format)
- IR light: Infrared light
- JPEG: Joint Photographic Experts Group (image format)
- LAN: Local Area Network
- LED: Light Emitting Diode
- MPEG: Moving Picture Experts Group
- NTP: Network Time Protocol
- ONVIF: Open Network Video Interface Forum
- PTZ: Pan/Tilt/Zoom

- QoS: Quality of Service
- SMTP: Simple Mail Transfer Protocol
- SMPTE: Society of Motion Picture and Television Engineers
- SNMP: Simple Network Management Protocol
- SSL: Secure Sockets Layer
- TCP: Transmission Control Protocol
- TLS: Transport Layer Security
- UPnP: Universal Plug and Play
- UPS: Uninterruptible Power Supply
- VMS: Video Management System/Software
- WDR: Wide dynamic range

PART 2 PRODUCTS

1.35 Video Management Software

A. The contractor shall supply an IP-based Video Management Software (VMS) solution.

B. The VMS shall include both video management and video analytic capabilities from the same manufacturer.

C. Video management, camera configuration, and video analytics shall be configured from the same user interface.

D. Video management and any alarms or operational data generated by video analytics shall be displayed within same operator interface.

E. The VMS shall be fully integrated with Perimeter Intrusion Detection Systems (PIDS) designed by Senstar Corporation and include the ability to display perimeter and VMS events within the same interface.

F. The VMS shall be fully integrated with Access Control Systems (ACS) designed by Senstar Corporation and include the ability for operators to send commands to, and receive status information from, doors and other managed hardware.

G. The VMS shall be open to integration with third-party access control hardware.

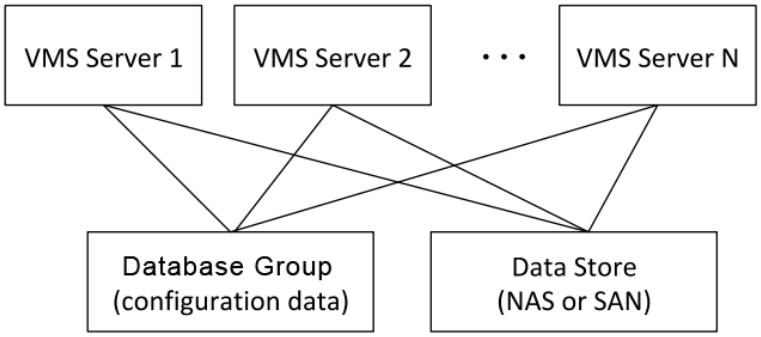
1.36 Manufacturers

A. The Senstar Symphony Video Management System from Senstar Corporation (www.senstar.com) meets the requirements stated in this document.

1.37 Architecture Requirements

A. All VMS software components shall be IP-based and comply with established networking standards.

B. The VMS shall support scalable, enterprise-level deployments that eliminates single points of hardware failure, as shown below.



C. The VMS shall include support for the following top-level components and user interfaces:

1. Server software
2. Web-based configuration interface
3. Microsoft Windows® operator client application
4. HTML5-compliant Web-based operator interface with no dependency on plugins
5. Native iOS and Android applications (smartphones and tablets)
6. Cloud-based IT management services
7. Server-based video analytics
8. Camera-based video analytics

D. The VMS shall use a 64-bit architecture for both the server software and Microsoft Windows® client.

E. Server requirements:

1. The maximum number of supported cameras and video streams per server shall not be artificially limited by software licensing. The actual camera limit shall be dictated by the performance of the server hardware.
2. The server software shall be capable of running on the following operating systems:
   a. Windows® 10 and 11
   b. Windows® Server 2012, 2012 R2, 2016 and 2019
3. The server software shall be capable of running on virtualization software, including VMWare and virtualization solutions from Microsoft.
4. The server software shall support the following high-availability databases for the storage of its configuration data:

a. PostgreSQL 12

b. Microsoft SQL Server

5. The server software must support the following storage configurations:

a. Direct attached storage (DAS)

b. Network attached storage (NAS)

c. Storage area networks (SAN)

d. Edge-based storage (such as network cameras)

e. Cloud storage capabilities (via third-party integration)

F. Data shall support UNC paths and scheduled backup of configuration and data separately.

G. The VMS shall support video analytics in the server running the video management system or embedded in an IP camera or encoder.

H. The VMS shall be extensible and customizable via new component development through a vendor-supplied Software Development Kit (SDK).

1.38 Video Standards

A. The VMS shall support the following video standards:

1. MJPEG

2. MPEG-4

3. H.264

4. H.265

5. Relevant ONVIF profile as defined by the ONVIF Organization

1.39 Video Management

A. The VMS shall include the following IP device capabilities:

1. Automatic discovery for cameras on the network

2. Camera templates to simplify Server set up and administration

3. Unicast and Multicast IP traffic

4. Camera resolution and frame rate shall be limited only by the hardware capacity and not the video management software.

5. Support for de-warping of 180 and 360-degree cameras

6. Analyze all video sources in real time at any bandwidth, frame rate and resolution supported by the camera or IP video encoder devices. Software shall automatically select the most appropriate stream for analysis out of all streams added for the camera.

7. Support for different frame rates for viewing, recording or alarm/analytic video

8. Support for corridor display (9x16) to maximize view of narrow scenes
9. Be able to record MJPEG, MxPEG, MPEG-4, H.264, and H.265 video streams from the same camera, as supported by the camera
10. Software must have the ability to record a different number of days per camera and/or video stream.
11. Support for video, 2-way audio, I/O, PTZ, VMD as well as multiple streams from the following network device manufacturers, when supported by the manufacturer or standard:
    a. Acti
    b. Arecont
    c. Axis
    d. Basler
    e. Bosch
    f. Canon
    g. Certis
    h. Dahua
    i. Dallmeier
    j. Dynacolor
    k. Eclipse
    l. Eneo
    m. Flir
    n. Geovision
    o. Grundig
    p. Hanwha
    q. HIKVision
    r. IPVisions
    s. Messoa
    t. Mobotix
    u. Oncam
    v. Panasonic
    w. Pelco
    x. Samsung
    y. Scallop Imaging

z. Siqura

aa. Sony

bb. Stardot

cc. Toshiba

dd. Vivotek

12. The VMS manufacturer shall provide a list of supported video devices.
13. The VMS shall be able to receive dynamic events like temperature alerts from ONVIF-compatible cameras.

B. The VMS shall include the ability to create extensive rules around analytic activity that include the following:

1. Trigger action for another camera (such as send PTZ camera to a preset or display another camera.
2. Trigger action to other integrated systems such as access control or I/O devices.
3. Send text and email messages to system users.
4. Video analytic activity shall be able to trigger alarms within the VMS.
5. Video analytic activity shall be able to trigger video recording
6. Server-based video analytics shall have the ability to transfer the analytic license from one camera to another without purchasing another license.
7. Server-based video analytics shall be independent of camera manufacturer or model.
8. The VMS shall have the be ability to record metadata from video analytics at different time lengths than video data.
9. The Video analytics should run in real-time and should be optimized to allow for the concurrent analysis of up to 50 cameras on a 6-core processor at 4CIF resolution.
10. The following video analytics should be embedded in the VMS and available on a per camera basis:

a. Object detection

b. Object removed

c. Object left behind

d. Different analytic rules and masks loaded per location on PTZ cameras

e. Auto-PTZ tracking

f. Auto-PTZ control with a single camera (no human intervention)

g. Use a fixed camera to initiate an auto-PTZ control session

h. Automatically follow an object from a camera that is executing a guard tour
i. Overhead people counting
j. 45-degree people counting
k. Wrong-way detection
l. Anti-tailgating
m. Crowd detection
n. Camera obstruction
o. Camera outage
p. Ability to classify person, vehicle or unknown
q. Anomalous movement detection
r. Zone exclusions
s. Tripwire
t. Tracks that had to begin or end at a specific location
u. Alarm, search and display based on complex contour of an object (not just fixed shapes such as rectangles)
v. Color detection
w. License plate recognition
x. Loitering/dwell time
y. Sensor fusion

11. The VMS shall support ONVIF alerts generated by edge-based video analytics.
12. Video analytics supported by the VMS shall:
    a. Accurately detect and track objects while minimizes false alarms.
    b. Categorize vehicles and people.
    c. Integrate with the VMS rules engine.
    d. Support indoor people counting with the following features:
        1. Generate alarms based on counts from individual or aggregate camera counts
        2. Generate dynamic HTML pages for use as digital signage that display current occupancy counts and provide warnings if counts are nearing or passing configured thresholds.
    e. Tracks bi-directional flow of objects as they pass through a user definable line
    f. Camera should be installed above where objects pass through for best

g. Includes reporting that can be run on an hourly, daily, weekly or annual basis

h. License Plate Recognition (LPR) video analytics integrated with the VMS shall be able to:

   1. Provide the ability to capture license plate information from an analog or IP video camera (not require a special camera designed for LPR).
   2. Be suitable for vehicle access, traffic control and enforcement applications.
   3. Track vehicle license plate information within the VMS. License plates from different regions and countries shall be recognized and logged.
   4. Provide alarms through the VMS.
   5. Support up to 12 FPS for each processor core.
   6. Read plates after analyzing 3 quality video frames, unless traveling at speeds up to 30 km/h (18 mph), in which 10 FPS may be used.
   7. Require a minimum of pixel size no greater than 32 pixels high for Latin characters and 40 pixels high for non-Latin (Arabic, Chinese) characters.
   8. Function with a camera mounted 5–50 m (16–160 ft) from the spot where the license plate is to be read at a height of 3–9 m (10–30 ft) with an angle of less than 30 degrees.
   9. Function with a camera in line with the vehicle (directly in front or back) or at an angle of less than 15 degrees.
   10. Read dots and dashes
   11. Be configured from within a standard web browser

i. Facial recognition video analytics integrated with the VMS shall be able to:

   1. Be able to identify people from any analog or IP video camera
   2. Be able to identify faces within a scene approximately 20 ft wide
   3. Provide alarms through the VMS
   4. Support up to 5 FPS for each processor core
   5. Read faces after 3 video frames
   6. Read faces with a pixel size of 50 Pixels high (face size)
   7. Function with camera mounted in line with the face (directly in front) or at an angle of less than 15 degrees elevation
   8. Be configured from within a standard web browser
   9. Support anti-spoofing mechanisms such as liveness checking.

PART 3 EXECUTION

1.40 System Installation

A. The system shall be installed in accordance with the manufacturer's recommended procedures as defined in the manufacturer's documentation for the system.

1.41 System Configuration

A. The system shall be configured in accordance with the manufacturer's recommended procedures as defined in the documentation for the system.

B. If bundled with a hardware platform, the system may be configured prior to delivery and installation.

C. All device firmware shall be the most recent provided by the device manufacturer, or of a version specified by the VMS manufacturer.

1.42 User Documentation

A. The manufacturer shall provide user documentation that explains how to install, configure, operate, and maintain the software.

B. The installer shall provide the following deployment-specific documentation:

   a. Video surveillance schedule, including all camera names, definition, location, resolution, framerate, recording profile and associated alarms.

   b. Server and storage calculations completed with a video management system design tool. Calculations shall be based on the following:

      1. Type A cameras at 3840x2160 resolution, 15 FPS, and 14 days storage

      2. Type B cameras (two video streams):

         1. Stream one: 1920x1080 resolution, 8 FPS, and 30 days storage.

         2. Stream two: 640x360 resolution, 10 FPS (for video analytic processing and no recording)

   c. Schedule listing server, storage, power, and UPS requirements based on server and storage calculations described in section 3.3.B.b.

1.43 Training

A. The manufacturer shall provide training materials that provide instruction in the installation, configuration, and operation of the system.

B. The manufacturer shall offer professional training services to assist the organization in meeting their training requirements.

SECTION 28 51 00 INFORMATION MANAGEMENT AND PRESENTATION

PART 1 GENERAL

1.1 System Summary

The contractor shall install a Common Operating Platform (COP) for the monitoring and management of video, security, and access control devices via unified interface. The COP shall be installable on commercial-off-the-shelf (COTS) hardware that runs the Microsoft Windows® operating system. The solution must be scalable and have automatic failover capabilities for the servers that do not require Microsoft Clustering technology.

The solution shall follow a flexible, per-device licensing model in which additional devices can be added to the system on a per-device license basis, without the need to purchase a group of licenses or other type of license.

1.2 Quality Assurance

A. The COP manufacturer shall perform a vulnerability assessment of its software.

B. The COP manufacturer shall perform penetration (PEN) testing of its software deployed in a standard configuration.

1.3 Definitions

The following acronyms and abbreviations are used in this document:

A. COP: Common Operating Platform

B. SMS: Security Management System

C. VMS: Video Management System or Software

PART 2 PRODUCTS

1.4 Video Management Functionality

A. All viewing clients connected to the system must include support for:

1. Live view
2. PTZ control
3. Recorded video
4. Alarm report
5. I/O status

B. The COP shall include a Windows® client with the following features and capabilities:

1. All operator features available from a single software user interface and in no case requiring multiple software user interfaces.
2. Customizable user interface, including the location of the alarm log, server list, map, camera/device tree and system log. Authorized users shall be able to save multiple user customization layouts. Layout options include:
    a. Full screen
    b. Tiled matrix
    c. Floating Windows®
    d. Dockable Windows®
    e. Resizable Windows®
    f. Custom maps (.bmp, .png, .jpg or .dwg files)
    g. Display live and recorded video
    h. Play back at least four cameras from multiple servers on the same screen at different speeds.
    i. Digital zoom
    j. Digital tracking that follows a zoomed in view of the tracked object when a tracked object appears. If two or more objects are being tracked at the same time, the viewable area shall include the bounded region of all tracked objects.
    k. Manual recording of live video for a configured period of time
    l. Send device-applicable commands via right-click menu in camera/device tree.
3. Visual tracking links: transparent “hotspot” areas that enable operators to switch the current video panel to another linked camera or view by selecting it on the screen.
4. Camera navigation:
    a. Go to PTZ preset
    b. Go to specific camera
    c. Send to clipboard
    d. Send to printer
    e. Send to file
    f. Navigation from maps
    g. View live and archived video streams
    h. Matrix and carousel elements. Different cameras can be configured to be displayed for different amounts time.
5. Multiple monitor support

6. Support for 4K video displays
7. Camera layout options:
    a. Saved layouts appear in camera tree for easy navigation
    b. Customizable camera tree view spanning one or many physical servers
8. Video search options:
    a. Basic search
    b. Time and date
    c. Individual and consolidated graphical timelines
    d. Alarm
    e. Smart search (ability to select an area or object in a scene)
    f. Analytic search including:
        1. Direction
        2. Dwell time
        3. Area based activity
        4. Movement across one or more tripwires in certain directions
        5. Tracks the begin or end at a specific location
        6. Items left behind or removed
        7. License plates
        8. Searches can be scheduled to run automatically on a specific interval
        9. Deliver search results that:
            1. Include video data with video analytic decorations included (e.g., boxes or contours to identify triggers)
            2. Include a flexible number of seconds pre- and post-event search result
            3. Stitch all qualified video snippets from a camera into a continuous movie (e.g., 20 snippets are stitched together so that you can select play and watch all 20 snippets continuously without interruption)
            4. Provide .JPG images of each qualifying snippet
            5. Each video snippet should be numbered in visible search results
            6. The total number of video snippets results should be visible in the search results
9. PTZ support with point-and click controls:
    a. Zoom in/out to marked rectangle

b. Zoom using mouse

10. Camera tour support for PTZ devices:
    a. Unlimited camera presets per tour
    b. Go-to preset on event
    c. Automatic pause and resume option
    d. Set multiple patrolling schedules per camera per day
    e. Unlimited number of camera tours
11. Graphical timeline search:
    a. Move to next/previous alarm
    b. Move to next/previous motion
    c. Move to next/previous 10 seconds
    d. Move to next/previous second
12. Video export functions:
    a. Multiple cameras in the same export package, with the ability to enable simultaneous playback.
    b. Support MPEG and MPEG-4 formats
    c. Password protect exported video using 256-bit Salsa20 encryption
    d. Option to apply privacy masks prior to export if not already configured.
    e. Cloud export: If system includes Maintenance and Support licensing:
        1. Directly export video from Symphony to the cloud
        2. Generate URL links to simplify sharing via email and other services
        3. Export occurs in background and does not block access to other Symphony client functionality

C. The COP shall include a web-based operator interface with the following features and capabilities:
    1. Support for the following HTML5-compliant web browsers (no required browser plugin):
        a. Windows® Edge
        b. Google Chrome
        c. Apple Safari
        d. Firefox
    2. Remote view of live or recorded video for up to 16 concurrent cameras
    3. Ability to run reports such as heat map or people counting

4. Camera navigation with site map
5. Graphical timeline
6. Messages
7. Reports
8. Secure user authentication

D. The COP shall support a thin client video appliance that has the following features and capabilities:
   1. Display live video from the VMS
   2. Support video playback and export from the VMS
   3. Decode and display video on HD monitors using ONVIF or RTSP
   4. Display live video from any ONVIF-compliant IP camera
   5. Display live video from any RTSP-compliant IP camera
   6. Support H.265, H.264, MPEG-4, MxPEG, MJPEG and JPEG compression standards

E. The COP shall support a mobile client that has the following features and capabilities:
   1. Included with the system at no additional cost
   2. Offers native Android and iOS versions
   3. Displays live and recorded video from the VMS server
   4. Streams JPEGs and H.264 at user-configurable frame/refresh rates
   5. Can transmit video to the VMS for recording by the VMS
   6. Provides a grid view of images from cameras, with the image refresh rate defined by user preference
   7. Provides a searchable list of cameras
   8. Alarm management capabilities shall include:
      a. Alarm log for alarm review
      b. Alarm event thumbnail view
      c. Historical playback of alarm event
      d. Alarms can be acknowledged (status and comments) from mobile clients
      e. Push notification of alarms (for iOS clients)
      f. User profile defining which alarms are displayed in mobile client on a per user basis
   9. Ability to enable or disable digital I/O actions
   10. Enable or disable server rules

11. Includes complete online help in supported languages
12. Provides secure SSL authentication and communication connectivity
13. Provides all functionality in both portrait and landscape rotations

1.5 Security Management Functionality

A. The COP shall include a Windows® client with the following features and capabilities:

1. Site map:
    a. Support the following formats for use as graphical site maps: BMP, GIF, JPEG and DWG (AutoCAD).
    b. Use icons to visually represent the status I/O, access control and camera devices
    c. Use icons or lines to represent the status of Senstar perimeter intrusion detection sensors, including zone alarms, supervision alarms, or diagnostic and status data.
    d. Visually display the location of an intrusion event based on the distance data provided by a Senstar ranging sensor.
    e. Device-applicable commands via right-click menu
    f. Ability to create multiple maps
    g. Ability use hyperlinks to quickly switch between maps
    h. Enable or disable inputs or outputs directly from map
    i. Assign alarms to a map
2. Graphical timeline search:
    a. Move to next/previous alarm
    b. Move to next/previous motion
    c. Move to next/previous 10 seconds
    d. Move to next/previous second
3. Events:
    a. Manually trigger events and outputs
    b. Allow continuous audible alarms until acknowledgement
    c. Audible alerts by motion or event
    d. Link alarm events to a graphic map or camera
    e. Visually indicate alarms on linked video stream panel
    f. Device event watch window
4. Printing capabilities via the Windows® printer subsystem:

a. Images
b. Audit logs

5. Public and private bookmarks of events
6. Reporting:
    a. Object counts across a line
    b. Heat map (created by meta-data) with object paths, counts and dwell time
    c. Object count change over time as a graph
    d. Object count tables
    e. Alarm summary reports
    f. Device event reports
    g. Reports can be scheduled to run at certain intervals and deliver results to an email list
    h. Reports shall be exportable to PDF, HTML or Text
    i. Report fundamental data should be exportable to Microsoft Excel
7. Alarm handling:
    a. Centrally manage alarms from multiple sensors, including video analytics, access control, alarm I/O, and Senstar sensors:
    b. Display multiple video streams and maps associated with an alarm
    c. Alarm management:
        1. Two-stage alarm management: acknowledge and clear
        2. Mask and temporarily mask zones/nodes
        3. Alarm aggregation
        4. Re-alarm
        5. Assigned configurable categories to alarms
        6. Share alarms with other users
        7. Filter and sort alarms by time, site, category and severity
        8. Provide real-time feedback to multiple monitor agents connected to the system when alarms have been viewed by other monitoring agents
        9. Associate icons to different alarm types.
        10. Enter additional description about alarms
        11. Upload document to include as alarm details
    d. Alarms can be transmitted using the following methods:

1. FTP
2. Email
3. TCP/IP
4. OPC
5. SNMP

8. Rules engine:
    a. Shall be capable of starting, stopping or triggering actions based on activity such as motion, analytics, access control or intrusion activity.
    b. Actions for events within the rules shall include:
        1. Send a message via alarm, email, etc.
        2. Initiate camera recording
        3. Display multiple cameras and graphical maps in dedicated alarm console
        4. Display alarm-specific instructions to the user
        5. Send a PTZ camera to a preset
        6. Trigger an I/O device
        7. Start a script
        8. Display a specific map
    c. Rules can be enabled or disabled through the client interface.
    d. Rules can be turned on or off from a schedule.
    e. User can quickly search for specific rules or events.
    f. Queuing of actions with time-based triggering
9. Sensor fusion engine:
    a. Shall be capable of synthesizing low-level data from supported Senstar perimeter intrusion detection sensors with data from people and vehicle tracking video analytics.
    b. Shall generate a single alarm to indicate a real security event is occurring.
    c. Shall minimize nuisance alarms generated by non-threat activity such as high winds, rain, or snow.

1.6 Security and Privacy Requirements

A. Client authentication:
    1. Native authentication support
    2. Single sign-on support

B. Data transmission between all core system components and clients shall be fully encrypted via TLS 1.2.

C. User access:

1. Active Directory support for Windows® client and configuration pages.
2. User security privileges shall be managed directly for a user or through the creation of security groups. Users may be members of more than one security group.
3. Global user groups shall be capable of being fully supported through a cloud-based enterprise management tool.
4. The COP shall support two-person requirements for specific functions, such as video recording or video export.
5. The COP shall include controls that limit or block access to video footage based on the time of recording.

D. User Permissions:

1. User privileges shall be customizable through user groups.
2. The COP shall support different Security Profiles (complete set of all users and associated permissions) that allow administrators to set permissions for a profile under a normal activity. The administrators shall be able to quickly change permissions in case of emergency by selecting new profile groups.
3. Administrators shall have the ability to view active user sessions and to log off users.
4. The COP shall support supervisor logons that require two users to login together for security requirements.
5. User actions shall be stored by time, location, and/or camera.
6. Access to logging and alerts shall be controlled by user group.
7. The COP shall have the ability to limit the number of concurrent logons.
8. The COP shall control user access on a per-camera basis.

E. Audit logging of user actions or server errors shall be stored in plain text or a non-proprietary database.

F. The COP shall allow privacy masks to be defined per camera on a per user basis. When privacy masks are applied, users with limited permission can view the video but the motion areas are scrambled to protect privacy. Users with the appropriate permission shall view the video with the privacy mask removed.

1.7 Licensing Requirements

A. The COP shall follow a flexible, per-device (camera, sensor, or access control device) licensing model in which additional devices can be added to the system on a per-devices license basis, without the need to purchase a group of device licenses or other type of license.

B. All device licenses shall be bound to the server, not the MAC addresses of the camera or device. Replacing a camera or device shall not require that a new license to be purchased.

C. Each IP-connected device (camera or other device with an IP address) shall require one license, including multi-sensor cameras and IP encoders.

D. I/O devices shall require only one device license per device IP address. Individual I/O ports shall not require additional licenses.

E. The licensing model employed by the COP shall be as follows:

1. The COP shall provide licensing options that supports different deployment requirements while maintaining a consistent look and feel.

2. The COP shall use the following licensing categories:

a. Standard: Provides basic features for small and mid-sized facilities, including:

1. View live video

2. Record video

3. Interface to I/O devices via dry contacts

4. Microsoft Active Directory support

5. Access control

6. Perimeter intrusion detection sensor management

b. Enterprise: Includes the same features as Standard and includes the following additional features:

1. Built-in server farm capability for automatic failover, redundancy and load-balancing

2. Video wall capabilities

3. GIS and DWG map support

4. Multi-server integration

5. API/SDK for integration with third-party systems

3. The number of servers, storage devices and clients shall be unlimited, in that the license does not dictate, control, or change depending on their number.

4. Viewing systems do not require license and shall be available on an unlimited basis for each license category.

5. There shall be no cost for mobile devices to connect to the system for viewing.

6. Licenses shall be upgradable to a higher license category (e.g. from Standard to Enterprise).

7. The camera license shall provide the ability to add analytic capability to a specific camera without requiring all other license to be upgraded.

8. The analytic camera license can be moved from one camera to another without an additional license cost.

1.8 Network Requirements

A. The COP shall be accessible through firewalls with multiple servers on a single IP address masqueraded behind the gateway.

B. The COP shall support customizable listening ports for client connectivity.

1.9 Hardware Requirements

A. The COP shall be installable on commercial off-the-shelf hardware such as BCD, Dell, HP, EMC, IBM or equivalent.

B. The COP manufacturer shall offer pre-built systems, in which the COP is pre-installed and configured.

C. The COP manufacturer shall offer a mobile client that runs on iOS and Android devices.

D. The hardware used to run the COP components shall be:

1. Manufactured in accordance with ISO 14001
2. Compliant with EU directives 2011/65/EU (RoHS) and 2012/19/EU (WEEE)
3. Compliant with EU regulation 1907/2006 (REACH)

E. The hardware devices used to run the COP components shall carry the following EMC approvals:

1. EN55022 Class B, EN55024, EN61000-6-1, EN61000-6-2
2. FCC Part 15 - Subpart B Class B
3. VCCI Class B
4. C-tick AS/NZS CISPR22 Class B
5. ICES-003 Class B
6. KCC KN22 Class B, KN24

F. The hardware devices used to run the COP components shall meet the following product safety standards:

1. IEC/EN/UL 60950-1
2. IEC/EN/UL 60950-22

G. The hardware devices used to run the COP components shall meet the following requirements:

1. IEC/EN 60529 IP66/67
2. NEMA 250 Type 4X
3. IEC/EN 62262 IK10+ (50 J)

4. ISO 20653 IP6K9K
5. IEC 60068-2-1
6. IEC 60068-2-2
7. IEC 60068-2-6
8. IEC 60068-2-14
9. IEC 60068-2-27
10. IEC 60068-2-60
11. IEC 60068-2-78

H. The hardware devices used to run the COP components shall meet the following railway environment requirements:

1. EN 50121-4
2. IEC 62236-4

1.10 System Management Administration

A. The COP shall include a web-based administration interface with the following features and capabilities:

1. Support for the following HTML5-compliant web browsers (no required browser plugin):
    a. Windows® Edge
    b. Google Chrome
    c. Apple Safari
    d. Firefox
2. Access to all administrative settings
3. Camera set up including recording and scheduling
4. Ability to create and administer camera templates
5. Analytic setup (if done through the server)
6. Alarm setup and rules programming
7. Server-based groups and views
8. Secure user authentication

B. All administrative changes shall be accessible via a standard web browser and not require version compatibility or additional software

C. The COP shall have the ability to be centrally managed across multiple sites, including performance monitoring, policy settings, software upgrades and cloud-based backups:

1. Servers shall be capable of being backed up and held to standard policies from the cloud without requiring someone to be on-site.
2. Client software must be able to be pushed by the server so that manual updates are not required.
3. Device Packs updates must be deployable from the server and pushed automatically to the clients. Client device packs are needed to support multicast video.
4. Software updates shall be capable of being automatically managed by the Server without requiring manual user intervention.

D. The COP shall include the following administration capabilities:
1. Server farm configuration (master/redundant/failover/overload protection)
2. Storage
3. System updates
4. Database backup and restore

E. Users shall have the ability to send text messages through the Software which could inform users of upcoming maintenance or act as a collaboration platform where operators can communicate real-time.

1.11 Cloud-Based Management and Administration

A. The COP shall include the ability to managed from a cloud-based Enterprise Management solution.

B. The Enterprise Management solution shall be hosted by the COP manufacturer and available on a subscription basis.

C. The Enterprise Management solution shall offer the following functionality:
1. The monitoring and management of servers, cameras and their associated settings. The solution shall display:
a. Status reporting for offline devices including servers, farms, storage, Thin Clients and cameras
b. Key performance characteristics including CPU and memory usage
2. Database backups and policy setting management
3. User management
4. A management dashboard interface providing access to system status and settings, including COP servers, farms, cameras and thin clients
5. All managed servers shall connect to the Enterprise Management system via SSL encryption with minimal bandwidth and firewall configuration
6. System capabilities:

a. Software updates and Thin Clients can be scheduled to run automatically without requiring someone to be on site

b. Supports database backups for connected servers

c. Servers and associated devices are not required to be on the same network to support Enterprise Manager capabilities

d. Supports camera templates for updating and maintaining stream parameters within a camera group

e. Capable of performing batch level firmware upgrades and password changes to multiple camera manufacturers without requiring someone on site.

f. Support direct export of video from Symphony and the generation of URL links for file sharing

g. Enterprise Manager shall support multiple server groups and settings to maintain policies within each user group.

7. User access:

a. Access to Enterprise Manager is available through a standard browser (not requiring additional software).

b. Shall require User Name and Password for login

c. Users can be defined and managed centrally allowing for creation, modification and removal of users.

d. Provides the ability to create user groups to change or view settings in Video Management system, analytics and cameras

e. Enables administrators to change login settings on remote servers

1.12 System Integration

A. The COP shall support the integration with third-party systems via a vendor-supplied Software Development Kit (SDK).

B. The COP shall support Senstar Network Manager software, including the ability to trigger device output points.

C. The COP shall support Symphony Access Control software, including the ability to:

1. Trigger device output points

2. Display an image of the card holder when triggered by an access control event

D. The system shall enable a deployment to be pre-configured off-site, so that the COP software can become fully functional after installation with minimal on-site configuration.

PART 3 EXECUTION

1.13 System Installation

A. The system shall be installed in accordance with the manufacturer's recommended procedures as defined in the manufacturer's documentation for the system.

1.14 System Configuration

A. The system shall be configured in accordance with the manufacturer's recommended procedures as defined in the documentation for the system.

B. If bundled with a hardware platform, the system may be configured prior to delivery and installation.

C. All device firmware shall be the most recent provided by the device manufacturer, or of a version specified by the COP manufacturer.

1.15 User Documentation

A. The manufacturer shall provide user documentation that explains how to install, configure, operate, and maintain the software.

1.16 Training

A. The manufacturer shall provide training materials that provide instruction in the installation, configuration, and operation of the system.

B. The manufacturer shall offer professional training services to assist the organization in meeting their training requirements.