R15011

JOLIET JUNIOR COLLEGE
1901

CARD READER ACCESS CONTROL SYSTEM
BUILDING AUTOMATION SYSTEM
Request for Qualifications

Proposal Request

Joliet Junior College, Illinois Community College District 525 (JJC) is soliciting proposals from vendors for a card reader access control system. **Proposals will be received until 2:00 PM CST on November 4, 2015** at Joliet Junior College Main Campus, 1215 Houbolt Road, Room A3102 Joliet, IL. The criteria for evaluating proposals will be based on the items set forth in this Request for Qualifications that meet the specifications and qualification questions (Attachment A). An award will be made to the most responsive and responsible proposal, which in the judgment of Joliet Junior College, best meets the current needs and long-term goals of Joliet Junior College. Joliet Junior College reserves the right to reject any and all Proposals and/or waive any informality in the solicitation process.

I. INTRODUCTION

Background

Joliet Junior College is a comprehensive community college. The college offers pre-baccalaureate programs for students planning to transfer to a four-year university, occupational education leading directly to employment, adult education and literacy programs, work force and workplace development services, and support services to help students succeed. The College has a combined total of 15,888 full time and part time students enrolled in Fall 2015 classes on its main campus located within the city of Joliet, and its five extension campuses located in Romeoville, Morris, Frankfort, Weitendorf, and City Center in downtown Joliet.

Vision Statement

Joliet Junior College will be first choice.

Mission Statement

Joliet Junior College is an innovative and accessible institution, dedicated to student learning, community prosperity, cultural enrichment, and inclusion. Joliet Junior College delivers quality lifelong learning opportunities empowering diverse students and the community through academic excellence, workforce training, and comprehensive support services.

II. PROJECT SUMMARY

Joliet Junior College is seeking a vendor to provide the college with a card reader access control system for the main campus and the five (5) extended campuses. Only manufacturers of card reader access control systems are to respond to this request. When JJC selects a manufacturer as a result of this submission, the various installations around the multiple campuses will be sent out for bid at a later date.

III. PRIMARY OBJECTIVES

The primary objective will be to provide the college with a modular secure access management system used to better control employee and visitor movements at various Joliet Junior College facilities.

IV. SCOPE OF SERVICES

Provide a written qualification proposal of your card reader access control system addressing the following:

Specifications (Attachment A)

V. REFERENCES

Provide a list of at least three (3) references whose systems are of similar complexity and have been installed and maintained by the security system integrator in the last five (5) years.

VI. SITE VISITS

There are no tours scheduled on campus.

VII. BLACK-OUT PERIOD

After JJC has the advertisement out for the RFQ, no firm shall contact any JJC officers or employees involved in the solicitation process, except for interpretation or clarification of request. Such firms making such request shall be made in writing as stated in the RFQ document and shall direct all correspondence to Janice Reedus, Director of Business and Auxiliary Services jreedus@jjc.edu or 815-280-6640. No firm shall visit or contact any JJC officer or employee until after the RFQ is awarded, except when a site inspection is required for the submission of a response.

During this black-out period, any such visitation, solicitation or sales call by any representative of a prospective vendor in violation of this provision shall cause the disqualification of such a firm's proposal.

VIII. EVALUATION CRITERIA

1. Ability to meet specifications
2. The firms overall experience, reputation, expertise, and stability
3. Experience with projects of similar size and complexity
4. Contractor/integrator qualifications
5. Feedback from references

IX. FINAL DOCUMENTATION

An original and seven (7) copies of the requested statement of qualifications, and a complete electronic copy (DVD or flash drive) of the statement must be provided in an envelope clearly marked: "Card Reader Access Control System" to the attention of:

Ms. Janice Reedus, Director Business & Auxiliary Services
Joliet Junior College
A3102
1215 Houbolt Road
Joliet, IL 60431-8938

X. SCHEDULE OF EVENTS

• Distribution of RFQ	October 15, 2015
• Deadline for Receipt of Written Questions Submit questions via email to: purchasing@jjc.edu	October 22, 2015 @Noon CST
• Issuance of Written Response to Questions	October 28, 2015 by the end of the business day
• RFQ Submission Deadline	November 4, 2015 @ 2:00 PM CST
• Evaluation of Responses	November 4 -20 , 2015
• Presentations by Short Listed Firms, if required	November 4 -20 , 2015
• Notification of Award	December 9, 2015

ATTACHMENT A

TABLE OF CONTENTS

CARD READER ACCESS CONTROL SYSTEM

PART I GENERAL

1.1 GENERAL DESCRIPTION

Only manufacturers of card reader access control systems are to respond to this request. Contractors/installers submitting on behalf of a manufacturer will not be accepted. When JJC selects a manufacturer as a result of this submission, the various installations around the multiple campuses will be sent out for bid at a later date.

The card reader access control system shall be a modular secure access management system used to better control employee and visitor movements at various establishments. The SMS shall be designed to maximize all tools offered by the Windows platform. All commands shall be accessible using only a mouse, and keyboard use shall be limited to documenting fields requiring numeric or alphanumeric data.

The operating program shall be multi-user and multi-tasking and capable of running on a non-proprietary CPU. The application software shall be based on a standard, high level programming language. The SMS shall be modular to facilitate its installation and the development of its capabilities while avoiding major modifications in its operation and in saving all defined system and historical data.

The server shall be a database server. All database management tools shall be included, such as back-up, indexing, and database cleaning tools. No third party database tools or licensing shall be required. The corporate gateway shall communicate system information between the server and controllers. The workstations shall be the main user interface to perform supervisory and programming functions. The owner will supply server(s) for the contractor to install. The contractor will be responsible for providing the owner with the requirements/specifications of the server(s) prior to owner purchase. The owner will then submit to the contractor for specific product detail and specifications for the servers they intend to purchase. Upon approval by contractor, the owner will furnish server(s).

The SMS shall enable the selection of at least two user languages. The basic dictionary shall include English, French, Spanish, Italian and German. However, the system shall include a vocabulary editor to be used in designing custom language dictionaries. The operator's profile shall permit the integration of one of the two basic languages.

The SMS shall include RS-232 / RS-485 communication link between the various system components as well as TCP/IP network interface capability. Field devices such as card readers, alarm inputs, control points, etc. shall be connected to fully distributed intelligent field panels capable of operating without host computer intervention.

The SMS shall be able to design customized ID cards directly from the access management software. No specific program or software other than the access management software and no additional licensing shall be required for this function. Any workstation shall be capable of being used as a badging station. Badging shall be fully integrated with the card database.

SMS shall be capable of controlling card reader access systems/subsystems at all 5 campuses. All hardware and software shall be included in the bid. Unit priced items shall be furnished installed as required. No additional hardware or software system components shall be required.

1.2 QUALITY ASSURANCE

1.2.A Manufacturer Qualifications

The manufacturers of all hardware and software components employed in the SMS shall be established vendors to the access control/security monitoring industry for no less than five (5) years and shall have successfully implemented at least 5 systems of similar size and complexity.

1.2.B Contractor / Integrator Qualifications

1. The security system integrator shall have been regularly engaged in the installation and maintenance of integrated access control systems and have a proven track record with similar systems of the same size, scope, and complexity.

2. The security system integrator shall supply information attesting to the fact that their firm is an authorized Dealer of the system.

3. The security system integrator shall supply information attesting to the fact that their installation and service technicians are competent factory trained and certified personnel capable of maintaining the system and providing reasonable service time.

4. The security system integrator shall provide a minimum of three (3) references whose systems are of similar complexity and have been installed and maintained by the security system integrator in the last five (5) years.

5. There shall be a local representative and factory authorized local service organization that shall carry a complete stock of parts and provide maintenance for these systems.

1.2.C Testing Agencies

1. The SMS shall be tested and listed by Underwriters Laboratories (UL) for UL 294 for Access Control System Units.

2. The SMS shall be tested and listed by Underwriters Laboratories (UL) for UL 1076 for Proprietary Alarm Units.

3. The SMS hardware shall comply with the following regulatory requirements:
    a. FCC Part 15 Class A
    b. FCC Part 15 Class B
    c. FCC Part 68 (TIA968)
    d. ICES-003
    e. CE
    f. ECCN for AES 128 bit encryption for IP communication
    g. Government standards NISPOM 5-313 Automated Access Control Systems, DICD Annex F 2.3 Accept/Reject Threshold Criteria, JAFAN Annex D 2.3 Accept/Reject Threshold Criteria

4. The SMS shall support Americans with Disabilities Act (ADA) compliance in door and access operation.

1.3 WARRANTY

The Security Management System (SMS) shall be provided with a 12 month product warranty from date of registration. Software version updates shall be available for no charge during this warranty.

PART II PRODUCTS

2.1 DESCRIPTION

The Security Management System (SMS) shall be an integrated system that utilizes a database for the storage and manipulation of related data. The SMS shall include applications software, corporate gateways for communication between the server and controllers, operator and administrator workstations with appropriate software, hard copy printers and secure backup media. The security field devices (readers, door position switches, REX, etc.) shall communicate with the field panels via a dedicated cable network. The field panels shall communicate to the server via a Fast Ethernet 10/100, TCP/IP network, RS 232/RS 485 connection, or dial-up modem.

The SMS shall allow for growth and scalability from a smaller system to a larger, high-end, or enterprise system. The SMS shall be modular in nature, allowing system capacities to be easily expanded without requiring major changes to system operation. All defined system data as well as historical information shall be maintained. Customizable user interfaces shall allow management of system information and activity for administrators and operators. The response time between the moment when a card is presented at the reader and when the door is unlocked shall not exceed one second. The SMS shall include a badging solution with a GUI for badge design. No extra licensing shall be required for the badging solution.

The SMS shall support up to:

20	Workstations
6	Concurrent Web Stations
2	Redundant servers
41	Corporate gateways
5,000	Door controllers per Corporate gateway
25,000	Card readers and/or keypads
Unlimited	Access cards

2.2 PERFORMANCE - MONITORING

2.2.A Monitoring Mode

1. The SMS shall enable every operator to customize his/her desktop configuration. It shall be possible to modify the desktop appearance and to create up to eight desktops and to associate up to ten different display screens to each. It shall be possible to modify the size and position of all screens. It shall be possible to determine if these screens shall be floating anywhere on the desktop or fixed on the desktop. If the workstation is equipped with a dual output video card and two or more monitors, it shall be possible to distribute the screen to multiple monitors. However, each screen shall be able to be viewed alone or together depending on operator needs. Once these parameters are saved, the configuration shall automatically take effect whenever the operator logs in.

   For all types of screens, it shall be possible to access the general properties of the screen by simply right clicking at the center of the screen. From there it shall allow for linkage between associated screens without having to exit the current screen or section. It shall be possible to right click events on the desktop for editing which shall bring the user directly to the card, door, or component window and back.

2. Message Screen

   All events that occur shall appear in real time. The text shall include at least the date, time, and a pertinent description of the event as well as its condition. The display of this screen shall be customizable and a different background and message color can be used for every type of event.

Every in-coming event shall be documented by one or more icons representing video images, photos, access card, server, gateway, controller, card reader, and relay or supervision point. It shall be possible to classify the events on the screen by sequence, date and time, type of event, or type of message. In addition, a text filter shall be available to facilitate searching. It shall be possible to access the last up to 100,000 transactions from this window without the need to request a special report.

3. Card Holder Photo Screen

When a card is presented to a card reader, the software shall automatically display the photograph of the cardholder in this window. From this screen it shall be possible to select the cardholder's name, card number, event text, and comments as well as specify a door or group of doors for which the operator would like to display a photo. The SMS shall support the display of up to 4 pictures simultaneously.

4. Filtered Message Screen

This screen shall be a copy of the text messages screen except it shall be possible to select a specific message filter. The SMS shall include a choice of pre-configured filters and the ability to create customized filters. For every new filter it shall be possible to associate a name to it, select the type of event, select door, select workstation, select gateway, select supervision input, and select output.

5. Alarm Screen

Alarms that require an acknowledgement by an operator shall be displayed on this screen in text form only. The text shall include at least the date, time and description of the alarm, and its condition. It shall be possible to classify events on the screen by sequence, date and time, type of event, or type of message. A text filter shall be available in order to facilitate the search.

If instructions about an alarm are envisaged, they shall automatically appear in a second window on the screen. If a graphic is associated with the alarm, it shall appear automatically on the screen defined to this effect. The icon associated to the control point shall be represented and show the actual state of the point.

The operator shall be able to access a log book in order to document the alarm that occurred. Once this information is recorded in the log it shall not be erasable or modifiable.

It shall be possible to associate video call-up with an alarm. When this occurs, the main screen shall become the video screen, not the alarm screen.

6. Video Screen (Video View)

When the SMS is integrated with digital video recorders, it shall be possible to view the video images of cameras associated with them. The SMS shall enable the creation of an unlimited number of video views, each one associated with up to 16 different cameras or graphics. It shall be possible for an operator to edit or modify an existing view or create a new one directly from this screen. For each video view it shall be possible to select sequential, mosaic pattern, or preset viewing modes.

It shall be possible for an operator to access all the commands of a motion PTZ camera to include rotate on its axis, adjust its focus, and have a larger view of the image. Accessibility to camera images and commands shall be limited by operator security level.

No additional licensing shall be required to perform this function.

2.2.B Graphics Screen

1. There are three options for graphics that appear as background on the screen. The first is a reproduction of the building(s) floor by floor. The graphic module shall be capable of importing files in BMP, EMF, WMF, JPEG, GIF, PCX, PNG, TIF, or PCD formats.

2. The second option is using web pages, or WebViews, as background on the screen. This can be used in the following manners:

    a. Accessing to DVR web servers
    b. Embedding default web pages into operator desktops
    c. Adding an IP camera onto a video view
    d. Embedding intranet pages or directories into the operator environment
    e. Adding PDF, Word documents, etc. to the desktop
    f. Accessing to network cameras from the Web Station
    g. HTML or PDF pop-up instruction on alarm
    h. Integrating report folders in the desktop for quick access

3. The third option is to assign a live video view as background on the screen if video integration is utilized.

4. For all three options, control points shall be represented by a descriptive icon. Control points include workstations, gateways, controllers, card readers, doors equipped with either card readers or supervision contacts, cameras, relays, and input monitoring points such as motion sensors. The icons shall be animated, meaning they shall represent the state of the point to which they are associated in real time. Every graphic shall support at least 100 control points.

    Right clicking on an icon shall directly access the manual commands of each control point. A door shall be capable of but not limited to temporarily unlocking, manually unlocking or locking, and enabling or disabling a reader. A supervision point shall be capable of being enabled or disabled. A control relay shall be capable of being activated, deactivated, or temporarily activated. Cameras shall be capable of viewing images or live video.

    No additional licensing shall be required to perform this function.

2.2.C Communication Methods

1. The SMS shall ensure the communication to remote sites over a LAN or WAN/Internet using a dedicated communication server device, IP Link, or a controller. This shall only be applicable with the use of Corporate Gateways. It shall ensure secure communications by the use of 128-bit AES Encryption. It shall reduce bandwidth consumption by managing the communication protocol of controllers at the remote site. Polling of controllers shall be done by the IP Link or the controller in the field and not over the network. The IP Link or controller shall provide support for up to 32 door controllers. The IP Link or controller shall be configured from the access software or from a web page which has the security feature of being disabled after successful use.

2. For sites that do not have network links, communication to remote sites shall be ensured by Dial-up modems. This shall only be applicable with the use of Corporate Gateways. The SMS shall support up to 32 such modems that can simultaneously communicate and transmit or receive data from remote sites. No modem shall be dedicated to specific sites; communication shall be established such that the first site calling shall have access to the first available modem, and so on.

3. Each Corporate Gateway should be able to control 32 local controller loops by using the RS-232/RS-485 protocols via serial or USB port. In addition, each Corporate Gateway should be able to control up to 512 Ethernet loops using TCP or UDP protocols, via the use of the IP Link or controller of 32 controllers each.

2.3 PERFORMANCE – PROGRAMMING & CONFIGURATION

2.3.A User Section

1. This section shall include all functions involved in the issuance of an access or ID card as well as database search and importation tools. During the addition or modification of a card, information about the card shall be sent to the door controllers affected by these new parameters as soon as the operator accepts the addition or modification. An additional command requiring a reloading of the cards database in the door controllers shall not be acceptable.

2. The SMS shall enable the creation and definition of a user access card. There can be up to five cards per user and users can be managed by cardholder name or card number. When creating user cards, the operator shall be able to select a card format directly from a Card dialog and enter the card number as it is printed on the card.

3. The following user information shall be able to be saved in the user section:

    a. Card number
    b. First and last name
    c. Card type
    d. Additional information (10 fields)
    e. Start date
    f. Expiry date
    g. Personal ID number (PIN)
    h. State of the card
    i. Comments

    In addition, it shall be possible to associate a photograph, signature, and badge template to a card.

4. The SMS shall allow for the creation of an unlimited number of card templates to be used as ID cards. Template parameters include name, number of sides, and size. It shall be possible to directly print a template on an access card. The operator shall be able to design customized badging templates directly from the access management software. No specific badging program or software other than the latter and no additional licensing shall be required for this function. Any workstation shall be capable of creating ID cards based on operator security level. The following items shall be capable of being added to and modified on a badge template:

    a. All information fields associated to a cardholder
    b. Bar code
    c. Text zone
    d. Start date, expiry date, today's date
    e. Saved images and logos
    f. Borders
    g. Rectangles (including rounded rectangles, ellipse)
    h. Lines and arrows
    i. Photograph (can be cropped)
    j. A background

5. The SMS shall allow for the creation of a day pass to be issued to visitors for a single day. The SMS shall also have the ability to create temporary ID visitor cards.

6. The SMS shall offer the possibility of modifying the parameters of a group of cards simultaneously based on Card Type. The system shall enable the creation of an unlimited number of card types. The following fields shall be modifiable:

a. Card status (valid, invalid, lost, stolen)
b. Card monitored (yes, no)
c. Start date (schedule)
d. End date (schedule)
e. Delete after expiration (yes, no)
f. Wait on keypad (yes, no)
g. Access group (selection menu)
h. Template model (selection menu)

7. The operator shall be able to search for a card by last or first name, card creation date, card number, or any of the ten fields of user definable information. The system shall display the last card transactions, namely the latest sixteen denied access events, authorized events, database events, and/or time & attendance events.

8. The SMS shall enable the creation of an unlimited number of Import/Export models, give them a name, select required fields, select their layout, and determine the field delimiter. This shall allow for acceleration of the data entry process by importing databases from a spreadsheet.

9. The SMS shall allow for 250 access levels programmed per Corporate Gateway. Every card shall be assigned an access level which shall determine where and when the access card will be valid. When the system consists of several sites or gateways, it shall be possible to use batch programming of access levels.

2.3.B Definition Section

1. The SMS shall allow the creation of 100 schedules per Corporate Gateway and an unlimited number of system schedules. Each schedule can include up to 4 intervals. A schedule can be associated with a supervision point, a relay, an access level, a door, elevator floor, an operator, or an event. The SMS shall allow time zone management.

2. The SMS shall allow the creation of 366 holidays. It shall be possible to define a name, define a date, and determine the type. The SMS shall allow the operator to view all the holidays defined in holiday type and sites by viewing them all in a yearly calendar.

3. The SMS graphics shall enable operators to view the exact location of a component installed at the site, or the state of components and peripherals represented in the graphic such as doors, contacts, motion sensors, controllers, etc. The SMS shall allow for the creation of an unlimited number of graphics. The components on the graphics represented by icons as well as the graphics themselves shall have the ability to be modified. The SMS shall allow for printing of the graphics with their respective components on the graphical floor plan.

4. The SMS shall allow the management of 2,048 elevator cabs of 64 floors each for each gateway. It shall be possible to associate a schedule to the call button. Outside of the schedule, a valid card for a particular floor will have to be presented to the cab reader for it to be activated. The floor selection button group associated with the card's access level will become operational for a predefined duration and all other buttons shall become inactive. The SMS shall allow the creation of groups of floors and access levels.

5. The SMS shall provide the possibility of setting up guard tours with existing components of the system. Card readers, magnetic contacts and motion sensors can be used as control stations for the guard tour. Key switches can also be located at strategic points for the guard to activate.

6. The SMS shall provide the possibility to setup unlimited amount of tasks via the user friendly task builder. The operator shall be able to create emails templates that can incorporate variable to dynamically populate the emails. Using the command GUI menu, the operator can program commands for any component in the SMS. Commands such as but not limited to lock, unlock,

temporary unlock, toggle, back to schedule for the doors, relays, inputs and enable and disable readers. The operator can also program commands for specific card count. The commands should be able to accept specific components or variables that can filled dynamically.

7. The SMS shall provide the possibility to setup unlimited batch card operations via the user friendly task builder. The mass card modifications shall take effect in real time. Each mass card modifications task shall allow for mass cards to be changed based on their card type. The mass card modification task shall be able to change:

    a. Card State
    b. Supervisor level
    c. Card count value
    d. Card Tracing
    e. Start Date
    f. End Date
    g. With deletion on expiration
    h. Waiting for keypad
    i. Card access group
    j. Replacing access levels
    k. Updating access levels
    l. Adding new access levels
    m. Updating and adding new access levels
    n. Card Badge layout

8. The SMS shall provide the possibility to assign the tasks previously created to be triggered on specific components and specific events.

2.3.C Devices Section

1. The physical components of the SMS including workstations, corporate gateways, gateway, site, controllers, doors, relays, and monitored inputs shall be individually configured and defined. Individual sites shall also be defined. The software shall allow the use of a controller setup feature in order to minimize the time needed for controller definition.

2.3.D Alarm Interface

1. The SMS shall allow interface with any external alarm system thereby arming or disarming the system by presenting a valid card to an entry / exit door. It also shall be possible to associate a keypad with a reader forcing the cardholder to enter a number in the keypad after presenting a card. This integration shall only be possible with the use of a corporate gateway. It shall be possible at a minimum to:

    a. Set a monitored input as an arming button
    b. Associate a usage schedule with an arming button
    c. Set the exit and entry delay
    d. Determine whether the system must wait for a valid access to arm
    e. Determine whether the door must relock on arming request
    f. Associate a monitored input with an alarm panel condition
    g. Lock a door unlocked by a schedule when armed

2.3 E Intrusion Integration

1. The SMS shall allow for:
    a. Single / multiple partition arming and disarming via reader
    b. Single / multiple partition arming and disarming via operator commands
    c. Receive events from intrusion panel

d. Receive partition names, user codes and zone names programming.
e. Update user codes
f. Assign user codes to cardholders

2.3.F System Section

1. The SMS shall define the profile of a system operator based on name, password, language, privileges, login schedule, security level, workspaces, and password expiry date. The SMS shall provide the possibility to force the operators to assign a mandatory card type to the users. The operator shall be able to provide a default card type for every card.

2. The SMS shall determine access rights granted to an operator based on security levels. The SMS shall have the ability to create an unlimited number of security levels that can be assigned to one or more operators. It shall be possible to determine from which system components the operator shall be authorized to receive events and take action. It shall be possible to specify for each programming window if the operator can (any combination):

    a. View the component in read only
    b. Add new components
    c. Modify existing components (cannot add new)
    d. Delete components
    e. Save as
    f. Print components
    g. View links

3. The SMS shall allow System Administrators to grant or deny operators access to system physical components such as gateways, sites, relays, etc. using Workspaces. This allows greater ease for larger sites to locate and assign components that pertain to specific gateways and sites. System administrators shall be able to tailor specific system applications and workstations Workspaces, therefore restricting access to information to all levels of operators. Operators shall be able to use temporary workspaces to narrow their fields of view when accomplishing specific tasks, and then easily revert back to their main workspace.

4. The SMS shall allow for the creation of unlimited instructions. These instructions shall be attributed to one or more events that will be used in documenting the event and guide the operator on duty in performing tasks. It shall be possible to edit the instructions in two different languages.

5. The SMS shall make it possible to customize system events. All events shall be pre-defined to display on all system workstations. For each event it shall be possible to:

    a. Determine a display schedule
    b. Determine a color
    c. Assign a printer
    d. Associate one or more workstations
    e. Associate an instruction
    f. Associate a schedule for an acknowledgement request
    g. Determine the priority level

2.3.G Report Section

1. The SMS shall include templates for various types of reports to include the following:

    a. Card use reports
    b. Manual operations reports
    c. Alarm reports

d. Historical reports
e. Time & Attendance reports
f. Detailed reports
g. Summary reports
h. Statistical reports
i. Roll Call Reports

2. The SMS shall allow for the creation of custom reports based on any event or component in the system. The SMS shall support an unlimited amount of customized reports.

3. All reports shall be able to be displayed on screen, printed, or sent by e-mail on a daily, weekly, or monthly basis. All event reports can be automated to be generated and sent at a specific time for a specific time period.

4. The SMS shall support at a minimum the following report formats: Paradox, Dbase IV, CSV, XLS, PDF, RTF, and TXT.

5. The SMS shall be able to generate an access report in CSV with all the card information associated to that access event.

6. The system shall support for the creation of custom Time and Attendance reports. Each time and attendance report shall support up to 32 rules for masking the entry and exit times of each card. Also each report shall support a “First entry and last exit” feature.

7. The SMS shall allow the creation of custom Roll Call reports, which can without operator intervention be emailed to multiple people and/or printed on multiple printers. The Roll Call report shall be a system wide feature.

2.3.H Options Section

1. The SMS shall allow operators to access basic server and display functions and allow the operator to determine default settings for the server hard drive. The operator shall also be able to determine the time to perform a server backup, programmable on monthly, weekly, or daily basis. It shall be possible to schedule and plan mass automatic updates.

2.3.I System Status Section

1. The SMS shall allow operators to view the state of various access system components in text or numerical form. A specific controller’s state shall also be able to be viewed in graphic form via the picture of the controller with the status of each terminal. Workstation and database status shall also be able to be displayed.

2.3.J Various Tools

1. The SMS shall employ an Express Setup to configure system components such as sites and controllers, as well as peripherals associated to these components such as ports and inputs. This utility will reduce the programming time to a minimum.

2. The SMS shall employ a database utility to allow the re-indexation and verification of archived files and verify the integrity of indexes, links, and database arborescence.

3. The SMS shall include a vocabulary editor to be used in designing custom language dictionaries

4. The SMS should function with active directory for login and card holder setup

2.6 REDUNDANCY & MIRRORING

2.6.A Redundant Server

1. The SMS shall be able to support an optional redundant server whose main function shall be to monitor the primary server and ensure automatic (Hot Standby) take over if necessary. The redundant server shall have all the same characteristics and functions as the primary server.

2. The transition between these servers shall be completely transparent. When the primary server is operational once more, it shall be capable of synchronizing its database automatically with the redundant server and then resume absolute control of the access management system. No human intervention shall be required in this operation.

3. The operator shall be able to perform any and all operations during a fail-over synchronization between the primary server and redundant server.

4. The system shall support the use of multiple simultaneous redundant servers. The need to install third party licensing shall not be acceptable.

2.7 OPERATION

The SMS shall perform the following tasks:

1. Allow card access management for one or more buildings.

2. Control access to various doors equipped with a card reader. Allow the ability to set card use count options to limit the number of times a card can be used.

3. Allow automatic transfer of cards to an unknown area by a push of a button for emergency exit purposes.

4. Monitor all defined alarm points as well as all doors controlled by card readers based on programmed schedules.

5. Send transactions for which printing is required to one or more printers, based on a set schedule.

6. Access the system using the main and secondary menus (to which access is limited by a password) to make additions and required changes to various data files so that they can be updated by the user without the manufacturer's assistance.

7. Enable the entry of access code data for every card or group of cards.

8. Seamlessly connect to onsite alarm systems.

9. Associate to each event a recording schedule for each destination (hard drive, monitor).

10. Automatically display all alarms on screen in text with optional graphic or picture and trigger a sound requiring an acknowledgement on the keyboard to stop the alarm.

11. Each event should print on a log printer. For security reasons, each event shall be incremented with a print number. Numbering shall start from 0 every day.

12. Generate reports and view them on the screen, output them to a printer, or send them to an email address.

13. Supervise based on programmed schedules of specific points such as door contacts, volumetric detectors, mechanical points, high and low temperature sensors, or any other equipment necessary for good building management.

14. Save the database manually or automatically backup following a schedule.

15. Uninterrupted backups. The operator shall be able to perform any task during a SMS backup.

16. The operator shall be able to perform any and all operations during a fail-over synchronization between the primary server and redundant server.

17. Save events on a hard drive according to required criteria.

18. Perform the following operations from all workstations:

    a. Lock or unlock one door or a group of doors.
    b. Perform a global lockdown of facilities.
    c. Activate or deactivate a relay or a group of relays.
    d. Activate or deactivate a point or a group of points.
    e. Program or modify one card or a group of cards.
    f. Validate or invalidate one card or a group of cards.
    g. Change time and date.
    h. Demand the system state in text or graphic mode.
    i. Query, create and/or modify data on: Access levels, Schedules and holidays, Access card, Instructions, Reports and log, Doors, Supervision points and relays, Operator levels, and Graphics.
    j. Ability to use an easy to use system tree view to select the components.

2.8 EQUIPMENT

2.8.A Existing Equipment

The SMS system shall operate with existing Wire, Card readers, request to exit, Door contacts and door hardware.

2.8.B Server and Redundant Server Requirements

The SMS is desired to run on its own appliance with built in redundancy. If a different Server is needed. Sever and software will be supplied by the contractor approval of Owner.

2.8.C Corporate Gateway Requirements

The SMS corporate gateway requirements shall be provided by the contractor. The owner will supply the contractor with detailed product selection for approval by contractor. Upon approval, the owner will supply any corporate gateways.

2.8.D Workstation Requirements

The SMS should operate as a Web client and function with Window 8.1 and higher.

2.8.E Remote I/O

The SMS shall support the remote I/O unit to control:

1. The SMS controller is required to fit in the existing space of the current controllers in the owner's facility. Either in the existing box or footprint.

2. Mercury control boards or equal.

3. A one door controller with four monitored points, door strike power, and four auxiliary outputs. It shall accept Wiegand, proximity, bar code, magnetic, and integrated keypad reader types. It supports RS-485 communication.

4. A multi-door, ethernet-ready four or eight door controller with sixteen monitored points, on-board door strike power, sixteen reader outputs, four relay outputs, and auxiliary power output. It shall accept Wiegand, proximity, ABA clock and data, bar code, magnetic, integrated keypad, and smart card reader types. It supports RS-232, RS-485 and 128-bit AES Encrypted Ethernet 10/100Base-T communication. It supports expansion modules to provide 256 inputs and 256 outputs. It shall support 136 double end of line inputs.

2.8.F Card and Reader Support

1. The SMS shall function with the owner's existing cards.

2. The SMS shall support configuration of unlimited card formats.

3. The SMS shall support up to 2 card formats per controller (3 with DUAL ioProx driver).

4. The SMS shall support readers that provide Wiegand signaling and magnetic ABA signaling to include:

    a. Wiegand swipe readers
    b. Proximity readers
    c. Biometric readers
    d. Smart card readers
    e. Wireless readers
    f. Magnetic readers

PART III EXECUTION

3.1 TESTING

1. The software shall be entered into the SMS computer systems and debugged. The Contractor shall be responsible for documenting and entering the initial database into the system. The Contractor shall provide the necessary blank forms with instructions to fill-in all the required data information that will make up the database. The database shall then be reviewed by the Contractor and entered into the system. Prior to full operation, a complete demonstration of the computer real-time functions shall be performed. A printed validation log shall be provided as proof of operation for each software application package. In addition, a point utilization report shall be furnished listing each point, the associated programs utilizing that point as an input or output and the programs which that point initiates.

2. Upon satisfactory on-line operation of the system software, the entire installation including all subsystems shall be inspected. The Contractor shall perform all tests, furnish all test equipment and consumable supplies necessary and perform any work as required to establish performance levels for the system in accordance with the specifications. Each device shall be tested as a working component of the completed system. All system controls shall be inspected for proper operation and response.

3. Tests shall demonstrate the response time and display format of each different type of input sensor and output control device. Response time shall be measured with the system functioning at full capacity. Computer operation shall be tested with the complete data file.

4. The Contractor shall maintain a complete log of all inspections and tests. Upon final completion of system tests, a copy of the log records shall be submitted as part of the as-built documentation.

3.2 TRAINING AND KNOWLEDGE TRANSFER

The Contractor shall provide a competent trainer who has extensive experience on the installed systems and in delivering training to provide the instruction. As an alternate, the Contractor may propose the use of factory training personnel and coordinate the number of personnel to be trained.