Aurora Software & Keyscan Controllers:

Architectural & Engineering Specifications

Access Control & Alarm/Event Monitoring System

Aurora (Ver. 1.0.23.0)

Foreword

The mission at dormakaba Canada Inc. EAD division has always been to engineer and manufacture the best access control systems while offering unsurpassed customer service and technical support within the security industry. We never wavered from that commitment during our more than 25 years of operation. Our Keyscan access control systems employ only proven technologies for reliable and effective system performance. Every access control panel is meticulously assembled and thoroughly tested before it's ever packed and shipped to a customer. And, we offer full on-going technical support to all our customers.

There are less expensive systems on the market, but not all systems are bundled with high quality control and important elements – elements not necessarily evident in the factual content of the architectural and engineering specifications.

After reviewing these A&E Specifications, if you have any questions, we invite you to contact us toll free at 1-888-539-7226 (Canada/USA) or 905-420-7522. We'll gladly answer your questions about our Keyscan access control systems and Aurora Software platform. This document is subject to change, contact dormakaba Canada Inc. Technical Sales to ensure you have the most up-to-date A&E Specifications available.

This document is furnished to assist in the preparation of a bid specification as it relates to a Keyscan access control system and Aurora Software. It includes all aspects of an installed system including optional software modules and related system capabilities. This document conforms to the guidelines established by The Construction Specifications Institute (United States) and Construction Specifications Canada – Master Format 2016 edition for Access Control. Please review the content of this document. It is incumbent on the bidder to make any necessary additions, modifications or deletions applicable to the proposed bid. Be sure to include all other required and relevant documentation.

While it may be necessary to modify this document, it is recommended that original text set out by dormakaba Canada Inc. not be modified; however, deletions may occur. Only the master copy of this document properly represents dormakaba Canada Inc. (where Keyscan access control systems and Aurora Software is manufactured).

Please delete the Cover page and the Forward page.

SECTION 28 10 00

ACCESS CONTROL SYSTEMS

PART 1 - GENERAL

1.1 SUMMARY

A. Section Includes:

1. The specifications to install and operate an integrated, computerized access control and alarm monitoring system.

2. (Placeholder for additional bidder specification statements, otherwise delete this line.)

B. Products Supplied But Not Installed Under This Section

1. (Placeholder for additional bidder specification statements, otherwise delete.)

C. Products Installed But Not Supplied Under This Section

1. (Placeholder for additional bidder specification statements, otherwise delete.)

D. Related Sections:

1. All Division 28 -13 Sections

E. Related Drawings

1. (Placeholder for additional bidder specification statements otherwise delete this line.)

1.2 PRICE AND PAYMENT PROCEDURES

A. Allowances

1. (Placeholder for additional bidder specification statements, otherwise delete this line.)

B. Unit Prices

1. (Placeholder for additional bidder specification statements, otherwise delete.)

C. Alternatives

1. The bidder shall not use alternatives or substitutes unless equal to or superior than the originally specified equipment and that the purchaser has expressly agreed to accept said substitutions.

2. (Placeholder for additional bidder specification statements, otherwise delete.)

D. Measurement and Payment

1. (Placeholder for additional bidder specification statements, otherwise delete.)

1.3 REFERENCES

A. The system shall comply with the standards, codes and regulations of the following regulatory bodies:

1. Underwriters Laboratories (UL) Std No. 294 Fifth Edition – Access Control System Units

2. Canadian Standards Association (CSA) Std C22.2 No. 205-12 – Signal Equipment

3. CE Standards

   a. EN 55022 RF Emissions

   b. EN 55024 RF Immunity

   c. EN 60950-1 Equipment Safety

4. FCC Subpart B – RF Emissions

5. Industry Canada ICES 003 Emissions

6. RoHS

7. (Placeholder for additional bidder specification statements otherwise delete this line.)

B. Definitions & Acronyms

1. Credential holder – an individual of record issued with a valid credential, such as a token or card, and authorized access at assigned system controlled entry portals.

2. System user – an individual of record with a valid user ID and password authorized with access control system administrative responsibilities

3. Credential – a card, token, PIN, biometric characteristic, or other device presented at a reader by a credential holder for gaining access at a system controlled entry portal

4. Portal - a point of access such as door, gate, elevator floor or other barrier controlled and monitored by an access control unit

5. ACU – access control unit

6. TCP/IP – transmission control protocol/Internet protocol

7. USB – universal serial bus

8. CCTV – closed circuit television

9. LAN/WAN – local area network/wide area network

10. NVR – network video recorder

11. SQL – structured query language

12. VMS – video management system

C. (Placeholder for additional statements otherwise delete line.)

1.4 ADMINISTRATIVE REQUIREMENTS

A. Coordination

1. (Placeholder for bidder specification statements otherwise delete line and article title above.)

B. Pre-installation Meetings

1. (Placeholder for bidder specification statements otherwise delete line and article title above.)

C. Scheduling

1. (Placeholder for bidder specification statements otherwise delete line and article title above.)

1.5 SUBMITTALS

A. General

1. (Placeholder for bidder specification statements otherwise delete line.)

B. Product Data

1. (Placeholder for bidder specification statements otherwise delete line.)

C. Drawings

1. (Placeholder for bidder specification statements otherwise delete line.)

D. (Placeholder for bidder specification statements otherwise delete line.)

1.6 CLOSEOUT SUBMITTALS

A. Maintenance Contracts

1. (Placeholder for bidder specification statements otherwise delete line and if applicable article title above.)

1.7 QUALITY ASSURANCE

A. Supplier/Installer Qualifications

1. The supplier/installer shall meet the following qualifications and experience:

a. (Placeholder for bidder specification statements otherwise delete line and if applicable article title above.)

b. (Placeholder for bidder specification statements otherwise delete line and if applicable article title above.)

B. Testing & Inspections

1. (Placeholder for bidder specification statements otherwise delete line and if applicable article title above.)

1.8 WARRANTY

A. Manufacturer Warranty

1. The Vendor shall warrant that all equipment furnished is new, undamaged, free of defects, and conforms to the specifications within this document.

2. (Placeholder for bidder specification statements otherwise delete line and if applicable article title above.)

B. Extended Correction Period

1. The Vendor’s obligation shall include removal, repair or replacement, transportation, re-installation, and testing without charge to the Purchaser, for all or any parts of the system found to be defective due to faulty materials or workmanship for a period of ____months after system installation.

2. (Placeholder for bidder specification statements otherwise delete line and if applicable article title above.)

3. (Placeholder for bidder specification statements otherwise delete line and if applicable article title above.)

PART 2 - PRODUCTS

2.1 MANUFACTURERS

A. Specifications, functionality, system capabilities and products presented are based on Keyscan access control units, related communication devices, and Keyscan Aurora software.

B. (Placeholder for bidder specification statements otherwise delete line.)

2.2 SYSTEM OVERVIEW

A. The access control system shall be an inter-connected group of components consisting of but not limited to the following devices:

1. Access control units (ACUs)

2. Communication devices

3. Access control software

4. Readers

5. Credentials

6. Door locks

7. Lock power supplies

8. Personal computers/servers

B. The system shall be capable of the following functions:

1. Regulate and monitor access at system controlled doors.

2. Control access to elevator floors and monitor elevator floor button activity.

3. Interface with a telephone entry system – phone bill and no phone bill types.

4. Monitor and control access to parking lots/parking garages.

5. Monitor connected detectors (supervised and auxiliary inputs) with the ability to manually or automatically arm and disarm them.

6. Control event initiated devices connected to system outputs, such as alarm panels or supported network video recorders, with the ability to automatically or manually arm and disarm them.

7. Report an alarm/event condition.

8. Distribute an annunciated alarm/event condition via an e-mail notification off-site.

9. Establish a hierarchy of alarm/event types to prioritize handling alarm/event conditions.

10. Maintain a comprehensive database recording all site activity.

11. Integrate with a closed circuit television system (CCTV) and interface with select NVRs.

12. Provide a photo ID badge template design editor allowing for a fully integrated ID badging operation when interfaced with a Windows-compatible card printer.

13. Provide a fully integrated map editor to create active floor plans that include representative door, input, output, and CCTV camera icons etc., which system users may manually manipulate for enhanced security monitoring.

14. Provide a fully integrated visitor management component.

15. Interface with select intrusion alarm panels.

16. Offer remote system access via the Internet or a corporate intranet with an optional WEB server application.

17. Offer an optional integration license to interface with MS Windows Active Directory

C. Building Integration

1. Providing that the necessary communication infrastructure exists, the system shall be capable of integrating multiple buildings within one collective access control and monitoring entity whether the buildings, in relation to one another, are proximate or distant. The access control system's design shall further allow expansion or modification within existing buildings or allow integration of new buildings at any time.

D. Software as a Service

1. The system shall have an optional capability of being configured as a centrally managed access control service using a reverse network mode of communication. Also refer to sub-section 2.4H on page 33.

2. The system, when configured for reverse network communication, shall provide a central monitoring station with the ability to service remote locations via Internet connections. Further, when the access control system is configured to run as a service, the software, database and servers shall reside at the central monitoring station.

E. Communication Modes

1. The software application modules shall be designed to communicate to the access control units using one or a combination of the following connection modes:

a. Network (TCP/IP)

b. Reverse network

c. Serial (RS-232)

F. Multiple System Users

1. The system shall support multiple system user workstations with access to the system database. The number of concurrent system users shall only be limited by the software licensing agreement.

2. The software shall provide selectable controls to govern individual system user activity with log on accounts and passwords. System user activity shall be recorded to the database and accessible for audit and review.

2.3 SYSTEM FUNCTIONS

A. Access at System Controlled Portals

1. Access shall be governed by controlled entry portals using an assigned credential that a credential holder presents to a sensing device referred to as a reader.

2. At least one credential shall be supplied for each individual who requires access at system-controlled entry portals.

3. The system shall be capable of supporting the following reader formats:

   a. Proximity (125 kHz)

   b. iClass Contactless Smart Card (13.56 MHz)

   c. Mifare Contactless Smart Card (13.56 MHz)

   d. Mobile Credential (optional)

   e. Radio frequency transmission (433 MHz long range)

   f. Biometrics

   g. Personal Identification Number (PIN) only

4. Each credential shall be internally encoded with an individual number. The system shall provide the means to enter these numbers into a database for transmission to each ACU.

5. The reader shall be capable of scanning and transmitting the credential's internally encoded number to the ACU.

6. The ACU shall process the credential data and unlock the appropriate controlled entry portal only if the credential is determined to be valid at said entry portal.

7. Where heightened and more stringent security is required, the system shall avail one of the following additional facilities:

   a. A reader may be programmed for "dual custody" mode whereby two (2) authorized credential holders must each present their credential in succession before access is granted at the entry portal.

   b. A keypad/proximity reader combination may be used in tandem whereby a credential holder presents a valid card and/or enters a personal identification number (PIN) to gain access. Only one (1) reader port shall be used when both a reader and a keypad are in place. A system user may create PIN codes in the credential holder records.

8. An access request at a reader shall be based on the following conditions:

   a. Is the credential valid for this site?

b. Is the credential valid for this entry portal?

c. Is the credential valid for this day?

d. Is the credential valid for this time?

e. Is today a holiday? If yes, is the credential valid for this holiday?

9. Should any of the above conditions be false, access would be denied. An ‘Access Denied’ event is recorded in the database.

10. Doors shall be unlocked for valid credential holders requesting entry within one second following the reader scan regardless of all other system activity.

B. Door Identification and Control

1. The system shall provide the means to identify with a unique alphanumeric description each portal that is controlled by an ACU and provide the following controls or functions:

a. User-defined door relay unlock time of 2 to 99 seconds, adjustable in 1 second increments.

b. User-defined door held open time of 1 to 16,383 seconds, adjustable in 1 second increments.

c. The ACU shall automatically re-lock the controlled portal either when sensed as closed or the door relay unlock time has expired.

d. Provide a separate accessibility feature such that an access control output relay can be connected to a door operator with separate door timer settings. The accessibility feature is for individuals who may require an extended time period for accessing the portal.

e. Provide a pre-alert that advises when a door remains open at the half interval of the combined door unlock and door held open times.

f. Each ACU shall provide a dedicated request to exit input for each door (i.e. an exit button).

g. Control a door where a reader and keypad are used conjointly with the following access modes:

1) Card or Keypad – Either the credential or the PIN may be used for entry

2) Card Only – Only the credential may be used for entry

3) Card and Keypad – Both the credential and the PIN must be used for entry

h. The preceding access modes may be assigned schedules whereby the system automatically changes from one access mode to another access mode if alternate security protocols are required during certain periods.

i. Monitor the status of all doors controlled by ACUs with the status represented in one of the following conditions:

1) Locked

2) Unlocked

j. Provide a manual override to lock or unlock doors controlled by the access control units.

k. Provide a programmable facility to automatically unlock and relock specified doors during an assigned schedule allowing access without the use of a credential.

l. Provide a programmable safety mechanism called "first person in" which arrests the scheduled auto unlock start time until a valid credential holder presents his or her credential at an assigned reader so as to keep doors locked in the absence of authorized personnel on site.

2. Anti-Pass Back Mode

a. The system shall allow doors to be set on 'anti-pass back' mode preventing a credential from being passed back and used twice in succession for either entering or exiting providing the system has been configured for in/out monitoring. The system shall flag the status of the credential as in or out. After a card is presented at an IN reader and enters, the card must be presented at an OUT reader and exit before the system permits the card to enter again. In the absence of in/out monitoring the system shall provide a timed mode between successive credential presentations.

b. The system shall be configurable for global 'anti-pass back' or local 'anti-pass back':

1) Global shall enforce 'anti-pass back' at doors where the doors are connected at different access control units providing the applicable communication hardware and infrastructure exists.

2) Local shall enforce 'anti-pass back' at doors connected to the same access control unit.

c. The 'anti-pass back' function shall have a manual override to clear the in or out status.

d. The system shall have multiple modes of anti-pass back:

1) Hard Mode – designated credential holders are denied access on violating anti-pass back enforcement.

2) Soft Mode – designated credential holders are allowed access but an anti-pass back violation is reported.

3) Timed Mode – designated credential holders are denied access on violating anti-pass back. Enforcement is based on a time interval. Timed mode can be employed on a single reader.

4) Executive Access Mode – excludes designated credential holders from anti-pass back enforcement.

C. Elevator Floor Identification and Control

1. The system shall provide the means to identify with an alphanumeric description each floor that is controlled by an elevator control unit (ECU) and provide the following controls or functions:

a. User-defined floor button selection time in seconds that the valid elevator floor buttons remain active after a credential presentation.

b. User-defined telephone entry interface floor button selection time in seconds that the valid elevator floor buttons remain active after a visitor has been "buzzed in" via a telephone system.

c. The system shall provide a facility to schedule an auto-unlock period for specified elevator floors in which access does not require a presentation of a valid credential.

d. The system shall provide an override facility to manually secure or un-secure elevator floors/floor buttons.

D. Alarm/Event Monitoring Functions

1. The system shall provide forced entry detection at specified door locations. A forced entry alarm shall be generated immediately whenever the door is opened without authorization. Authorization shall be determined by a valid credential, request to exit transaction, or by user intervention from the system software.

2. The system shall provide door held open detection at ACU controlled doors. A door held open warning shall be generated immediately whenever the door is held open longer than its specified time limit.

3. The system shall feature the provision to monitor auxiliary and supervised input points. The system shall be capable of detecting state changes between four distinct conditions for each of these points:

a. Alarm

b. Secure

c. Trouble due to open circuit wiring

d. Trouble due to short circuit wiring

4. The system shall also have the provision for reader supervision when connected with a "heartbeat capable" reader to detect and report one of the following alarm/event conditions:

a. Reader communication failure

b. Reader tamper alarm

5. The system shall on detecting an input change of state generate a message stating the nature of the alarm/event, the location and the time. The system shall record the alarm/event such that it can be later retrieved for an audit report.

6. The system shall provide the means to trigger an alarm in the event tampering occurs at the ACU.

E. Control Of Event Initiated Devices

1. The system shall have the ability to control event initiated devices that respond to alarm events. Said devices may be armed or disarmed automatically by user-defined schedules or armed and disarmed manually by operator intervention.

F. Communication Failures

1. The system shall notify the Client workstation of any communication failures with the ACUs.

G. Mobile Credentials (Optional)

1. At least one mobile credential shall be supplied for each individual who requires access at system-controlled entry portals.

2. Each mobile credential shall be encoded with an individual number. The system shall provide the means to enter these numbers into a database for transmission to each ACU.

3. The reader shall be capable of scanning and transmitting the mobile credential's encoded number to the ACU.

4. The ACU shall process the mobile credential data and unlock the appropriate controlled entry portal only if the mobile credential is determined to be valid at said entry portal.

5. Doors shall be unlocked for valid mobile credential holders requesting entry within one second following the reader scan regardless of all other system activity.

2.4 SYSTEM SOFTWARE

A. The system software shall provide full integration of all system components for overall access control management.

B. System Software Requirements

NOTE: For systems greater than 25 doors, please review the Aurora System Architecture Document #KD50013.

1. The system shall be based on independent, intelligent devices that are interconnected and communicate to Windows® compatible servers or workstations with the following recommended specifications:

a. Client Work Station

1) Intel Core i7 – 4770 3.4 GHz with 4 cores

2) 16GB RAM 1600MHz DDR3 NON-ECC

3) 500GB 7.2K RPM SATA Hard Drive

4) Supported operating systems:

i) Windows Server 2022 Standard 64-bit

ii) Windows 11 Enterprise & Professional 64-bit

iii) Windows Server 2016 Standard 64-bit

iv) Windows 10 Professional 64-bit

v) Windows 8 Professional 64-bit

vi) Windows 7 SP1, 64bit Ultimate, Enterprise & Professional

vii) Windows Server 2012 64-bit Datacenter, Standard, Essentials & Foundation

viii) Windows Server 2008 R2 64-bit Datacenter, Enterprise, Standard & Foundation

5) AMD RADEON HD 8490 1GB Dual Monitor or AMD RADEON HD8570 1GB Dual Monitor (System compatible with 1024x768 or higher resolution—single or dual monitor)

6) USB 2.0 Ports

7) Ethernet Port - 1GB Network Card

8) Keyboard & Mouse

9) UPS Backup (recommended)

b. Aurora Communication Server

1) Intel Xeon E5 – 2403, 1.80GHz, 10MB Cache with 4 cores

2) 8GB RAM 1333MHz, RDIMM

3) 500GB 7.2K RPM SATA Hard Drive

4) Supported operating systems:

i) Windows Server 2016 Standard

ii) Windows Server 2012 64-bit, Datacenter, Standard, Essentials & Foundation

iii) Windows Server 2008 R2 64-bit, Datacenter, Enterprise, Standard & Foundation

5) Integrated HD Graphics Card

6) USB 2.0 Ports

7) Ethernet Port – Dual Port 1GB Network Card

8) Keyboard & Mouse

9) UPS Backup (recommended)

c. Aurora Database Server

1) Intel Xeon E5 – 2420, 1.90GHz, 15MB Cache with 6 cores

2) 16GB RAM 1333MHz, RDIMM

3) 2 x 1TB 7.2K RPM SATA Hard Drive RAID 1 Configuration

4) Dual, Hot-Plug, Redundant Power Supply

5) Supported operating systems:

    i) Windows Server 2016 Standard

    ii) Windows Server 2012 64-bit, Datacenter, Standard, Essentials & Foundation

    iii) Windows Server 2012 R2 64-bit Standard

    iv) Windows Server 2008 R2 64-bit, Datacenter, Enterprise, Standard & Foundation

6) Integrated HD Graphics Card

7) USB 2.0 Ports

8) Ethernet Port – Dual Port 1GB Network Card

9) Keyboard & Mouse

10) UPS Backup (recommended)

d. Aurora Web Server

1) Intel Xeon E5 – 2403, 1.80GHz, 10MB Cache with 4 cores

2) 16GB RAM 1333MHz

3) 500GB 7.2K RPM SATA Hard Drive

4) Supported operating systems:

    i) Windows Server 2016 Standard

    ii) Windows Server 2012 64-bit

    iii) Windows Server 2008 R2 64-bit

iv) Windows 10 Professional

v) Windows 8 Professional

vi) Windows 8 SP1 Professional, Enterprise and Ultimate

5) Integrated HD Graphics Card

6) USB 2.0 Ports

7) Ethernet Port – Dual Port 1GB Network Card

8) Keyboard & Mouse

9) UPS Backup (recommended)

C. Software Architecture

1. The system software shall be designed for installation on multiple servers/workstations operating on a LAN/WAN (TCP/IP) from any communication node on the network.

2. The system software shall be modular in design and consist of the following standard components:

a. client software application (system user input/monitoring/reporting)

b. communication service application

c. database engine – Microsoft SQL Server 2012

d. optional WEB server for remote Internet/intranet access

3. The system shall support upgrading to full SQL.

D. Client Software Application

1. The system shall support multiple concurrent client system users commensurate with the license agreement.

2. The system interface shall be based on Windows® conventions and standards. The screens shall have selectable graphic icons for direct menu access to all system functions.

3. The system shall provide the following user-selectable interface languages:

a. English

b. Spanish

c. French

d. Portuguese

4. The system shall allow the user to select a language from any screen.

5. The system shall retain the user's language preference for all subsequent logins until the user elects to change his or her language preference.

6. Entering data, managing system functions, auditing system activity and monitoring alarms and events shall be performed from the client software workstation.

7. The system shall further provide the system user with the facility to define, view, and print summaries based on system-wide activity recorded in the database.

8. The system software shall have the capability to program and monitor remote site systems simultaneously.

9. The system software shall provide the means of streaming site activity data in a comma delimited file format or network message to 3rd party applications.

10. Hardware Setup & Status

a. For system user convenience, the system software shall have a consolidated hardware setup interface for inputting all hardware-related settings. All related control unit communication settings, door settings, auxiliary inputs, outputs and control board protocols shall be accessible by the selection of tabs from a single interface screen.

1) The system software's hardware setup interface shall also have the provision for establishing global inputs and outputs such that inputs can be programmed to fire outputs across multiple control units. The global I/O function must meet the necessary communication and hardware specifications and may require optional equipment depending on the structure of the global I/O network.

b. The system software shall have the means to assign an output to trip if an ACU experiences an AC power failure. A user-selectable time delay may be programmed before the output is tripped.

c. Where keypads are installed, the system shall have the means of assigning an output for a keypad "duress" code. A distressed credential holder would press the designated duress key then enter the PIN code. The system would trip the output for an expedient response to the situation.

d. The system software shall allow instituting certain control unit settings from the software for added convenience.

e. The system shall provide a status interface for reviewing control board information and settings and initiating manual functions.

f. The status interface shall also have a disaster recovery utility in which a system user may retrieve data directly from each control unit to restore system operation in the event the database server fails and a backup copy of the database does not exist for restoring the system.

11. Credential Holders

a. The system software shall be designed such that a credential holder may be assigned multiple credentials in multiple formats.

b. The system shall allow a credential holder to be assigned to ten different access groups for maximum access flexibility.

c. The system software shall be designed such that a credential holder's record and assigned credentials may be enrolled at all sites without the need of copying a record from one site to another site. Further, the record and the credential shall each have a selectable Active/Inactive status. Where multiple sites exist and depending on access protocols, the record may be set as active so it is valid at selected sites but the credential made inactive so it does not have access permissions at selected sites.

d. The Active/Inactive status shall also serve as an alternative to permanently deleting a record or credential. While the Inactive status is in effect, the record or the credential are maintained in the database but are invalid and denied entry to all previously authorized access portals. The Inactive status shall remain in effect until manually reset on Active status.

e. The credential holder record screens shall be in a consolidated format. A credential holder's group access for all sites can be viewed or edited from the same screen; a credential holder's enrollment for all sites may be viewed or edited from the same screen for system user convenience.

f. The system software shall offer system-defined fields and user-definable fields to identify each credential holder. The system shall further provide two categories of user-defined fields which are either common for all sites or optional for specific sites.

g. The system shall provide the ability to import digital photographs or capture a photo from a supported optional USB camera and insert the image on each credential holder record.

h. The system shall provide an image editor with a suite of tools for image cropping and touch-ups when importing the image into a record or editing at a later time.

i. The system shall store cardholder images in the database and said images shall be preserved/updated to the database during backup operations.

j. The system shall provide a utility function in which the software can reduce the file size of large images conserving database space.

k. The system shall allow assigning credentials with a temporary status based on a defined date/time and/or a usage limitation. At the conclusion of the date/time or when the usage reaches zero, the system shall render the credential inactive and deny further entry.

l. A system user shall be able to view from individual credential holder records the most recent transactions that have transpired during the previous 45 days for auditing, investigating activity, or locating the individual’s whereabouts.

m. In the event a credential is lost or stolen or upon employment termination, the system shall allow a credential to be cancelled and rendered invalid.

n. In order to locate and review credential holder records, the system shall provide search capabilities to find one or multiple records.

o. The system shall also offer a time saving mechanism to import a CSV file of credential holder records from other external databases substantially reducing data entry.

p. The system shall also offer a facility in which credential holder records may be exported as a CSV file and used to populate external databases.

q. The system shall provide a facility to view an access level summary in determining which system regulated doors and elevator floors the credential holder may or may not access.

r. The system shall offer a function within the credential holder screen in which a system user shall have the convenience of enrolling an unregistered credential presented at a reader. This is beneficial in cases where the credential’s imprinted number has worn off from extensive use and the credential cannot be re-assigned until the number is known.

s. The system shall offer a bulk update function for simultaneously revising multiple credential holder records which require a shared common change saving a system user from having to open and manually alter each individual record.

t. The system shall provide a resource for bulk entry of sequentially numbered credentials and which, if desired, may be assigned temporary options.

u. The system shall have the ability to interface with single-sided or double-sided card printers for printing photo ID badges created in the card template editor.

12. Schedules

a. The system shall provide 256 schedules (512 unique time blocks) for regulating door access, elevator access, inputs, and outputs.

b. Schedules shall be configurable on the basis of a seven (7) day week.

c. The schedule interface screen shall offer a system user multiple schedule creation methods: a “click and drag” method or a dialog box method. The schedule interface screen shall also offer the system user with “right click” copy and paste options for efficient schedule creation.

d. The system shall offer three (3) holiday schedules which can be used as overrides for regular schedules. Holiday schedules may be used for statutory holidays, special occasions, plant shutdowns etc., where on a specific date a system user may program the software to pre-empt regular schedules with a holiday schedule.

e. The system shall support assigning the three (3) holiday schedules to a maximum of sixty-four (64) holiday dates. When a holiday date is in effect, the assigned holiday schedule overrides the regular schedule on that date. The system shall further provide a facility to specify recurring holidays eliminating the need of resetting those holidays each year.

f. If holidays have been specified, the system shall be capable of listing all holiday dates and types.

g. Intended for multiple site configurations, the system shall provide a “master holiday” screen that provides the means to create a list of holidays common to all sites assisting system users in determining and assigning holiday schedules with consistency and uniformity.

h. The system shall automatically invoke a holiday schedule when the system clock matches any date defined as a holiday. A holiday schedule shall override all other schedules. Access shall be predicated on the times and authorizations of the holiday schedule for the stated holiday date. At the start of the next non-holiday calendar date the system shall invoke the regular schedule settings and access conditions.

13. Groups and Access Levels

a. The system shall allow creating up to 511 groups of which each credential holder may be assigned to 10 door groups and 10 elevator groups.

b. The system shall display the names and, if applicable, images of persons in a selected group for the benefit of the system user when reviewing group assignments.

c. The system shall provide a door access interface screen and an elevator access interface screen for separate group access and schedule assignments so as to provide greater flexibility by treating door access and elevator access as two distinct entities.

d. The system shall provide the option of selecting between two modes of viewing access levels: a basic view interface screen or an advanced view interface screen, so as to provide convenient system user viewing preferences.

e. The system shall provide the following three access levels for door groups and elevator groups:

1) 24 hour access

2) No access

3) Access based on a user-defined schedule

14. System Users

a. The system shall enforce log in protocols so only authorized individuals assigned a system user account with a unique user name and password may access the client software. Non-authorized individuals shall be denied software access.

b. The system shall provide an optional login authentication function in which the software shall recognize the Windows user account for login authentication. The optional login authentication function shall be compatible with a domain or local network setup. The system user, with the optional login authentication function, shall have direct system access and shall not be required to complete the system software's user name and password fields to log in.

c. The system shall have classes of user types to assist in structuring login accounts with respect to individual oversite and responsibilities.

d. The system shall allow each system user individualized permissions for adding, editing, deleting and viewing database information, as well as interrogating and issuing commands to the access control units.

e. The system shall provide a complex password mode whereby all system users must log in with a defined password format. The complex password mode elevates log-in security protocols for better protection against unauthorized access.

f. The system shall support an unlimited number of system user accounts. Passwords shall not be displayed or printed by the system at any time during usage. It shall be possible to change passwords at any time.

g. The system shall provide the means of tracking system user activity with the capability of generating a detailed summary.

15. Card Template Editor for Photo ID Badges

a. The system shall have an integrated card template editor utility to create photo ID badge templates.

b. The card template editor shall provide a suite of tools to draw, arrange and place objects, import images, edit text, insert photos, add barcodes, and insert database fields for creating ID badge templates.

c. The card template editor shall have a card type function in which the software shall only make available the relevant database fields specific to the card type selected. This shall help simplify the design task and offer the advantage of creating templates for printing visitor-specific badges with visit details or non-visitor badges based on site assignments.

d. The photo ID badge editor shall offer the system user a selection of industry-standard card sizes for accurate template dimensions.

e. The card template editor shall offer a library of industry-standard barcode types with a set of formatting options.

16. Active Map Template Editor

a. The system shall have an integrated active map template editor application for creating floor plans.

b. The map editor shall provide a suite of tools to draw objects, import images, edit text, as well as strategically place icons that represent doors, inputs, outputs, and CCTV cameras which are interactive when the map is displayed in the Client software.

c. The map editor shall allow importing, in a compatible image file format, drawings of floor plans.

d. Map Interaction

1) The active mapping component shall have full access to and complete interaction with the system database.

2) The system shall provide the means of manually opening a map from a menu icon for determining device locations or on-going monitoring.

3) Maps shall be updated as events occur.

4) The active mapping component shall be capable of automatically indicating, with an on-screen icon, when a credential is presented at a door.

5) The active mapping component shall have the ability to program a floor map to open automatically when an assigned device/transaction occurs. A door or device that has gone into alarm shall be indicated on the map to determine the source of the alarm.

6) The active mapping component shall be interactive and provide manual overrides for doors and inputs from an open floor map.

17. Event/Alarm Setup and Instructions

a. The system shall provide an alarm/event setup interface for defining alarms or critical events, listing persons to contact and conveying instructions about how the alarm or event should be handled.

b. The alarm/event setup interface shall allow defining alarm/events either individually or in groups where devices share a common transaction type to streamline the overall number of defined alarm events.

c. The alarm/event setup interface shall further allow setting various actions to be initiated when an event occurs:

1) a command line action which shells out to a third party application

2) an e-mail action which sends an event message to a specified recipient

3) a map action which opens a specified user-created floor map

4) a video action which opens the video management system interface

d. The alarm/event setup interface shall also have mechanisms to filter alarm/events with customized display characteristics, assign escalation actions when no one has responded to an alarm/event and a logging filter that suppresses alarm/event annunciation during specified periods.

18. Visitor Management

a. The system shall have an integrated visitor management component capable of scheduling and tracking visitor appointments. Visitors and appointments shall be recorded and retrievable from the system database for centralized visitor management.

b. The visitor management component shall have the facility of creating and retaining individual visitor files.

c. The visitor management component shall have the ability to scan a business card or ID card, such as a driver’s license, to populate personal information fields on the visitor record providing an optional compatible scanner is interfaced with the system software. An image of the card shall be retained in the database.

d. The visitor management component shall be capable of scheduling visitor appointments, citing dates and times, contacts, and visit status. The component shall further record all visits to the database for a historical archive.

e. The visitor management component shall have facilities to interact with the access control system whereby visitors may be issued credentials for independent entry at designated reader controlled doors or elevator floors.

f. The visitor management component shall have the ability of e-mailing an internal contact advising the visitor has arrived.

g. The visitor management component shall be capable of printing visitor badges when interfaced with a Windows® compatible card printer.

h. The visitor management component shall provide a visit status in which a system user may review a log of visits with selectable filtering switches.

19. Manual Overrides

a. The system shall furnish a system user with manual door controls from a client workstation as detailed below:

1) Unlock a door and leave it unlocked

2) Unlock a door momentarily, such that it automatically re-locks after the normal door relay unlock interval

3) Lock a door

4) Unlock or lock all doors controlled by a selected ACU

5) Schedule a timed unlock period for a specified door

b. The system shall provide a system user with the ability to manually override elevator floor control by toggling individual or all floors to secured or unsecured. The system shall allow the system user to restore the elevator floors to their scheduled setting.

c. The system shall provide a system user with the means to manually arm or disarm auxiliary and supervised inputs and outputs. The system shall allow restoring the inputs or outputs to their scheduled setting.

d. The system shall provide a system user with the ability of viewing the status of schedules and manually toggle schedules on or off.

20. Present3 Controls

a. The system shall provide a “Present3” function which allows a designated credential holder to independently invoke a change of state for specified doors and devices when a credential is presented at a specified reader.

b. The system's Present3 function shall be able to lock or unlock doors on an unscheduled basis, arm or disarm points connected to devices such as motion sensors, lock out other credential holders to prevent false alarms, implement a supervisory override to restrict access, or control lights, HVAC systems etc.

c. The system's Present3 function shall be capable of either toggling a door's lock/unlock state or toggling a schedule's off/on state and shall offer the following modes of operation:

1) Door Toggle

2) Schedule Toggle with Card Lockout

3) Schedule Toggle without Card Lockout

4) Schedule Toggle with Card Lockout and Exit Delay

5) Schedule Toggle with Card Lockout, Entry and Exit Delay

21. Site Management Reports

a. The system shall furnish the system user with the capability of transposing site information and activity recorded by the database into one of the following report types:

1) Transaction Report – summarizes user-filtered access control system activity and events

2) System Log Report – summarizes system user activity

3) Cumulative Hours Report – lists when credential holders entered and exited access portals and summarizes the total IN time providing a controlled enter/exit environment exists with in and out readers

4) Door Access Granted Summary Report – summarizes access granted transactions that occurred at each door during a framed time period

5) Active/Expired Credential Report - summarizes credentials assigned with a temporary date range that will become active or will expire during the requested report period

6) Unused Since Credential Report – summarizes inactive credential holders within a given period of time

7) People In/Out Report – allows viewing the current status of all or selected credential holders at the specified site

8) Deleted People Reports - provides a summary of persons whose records were deleted in the access control software

9) Group Status Report – summarizes active and inactive groups

10) Visit Report – summarizes various aspects of visitor activity

11) Site Setup Report – user-input summary of access control system information and settings

12) Person Reader Access Report – summarizes individual credential holder's access levels at each door

13) Reader Access Report – summarizes group access levels at door control unit readers

14) People Information Report – produces a summary for all or selected person records

15) Visitor Information Report – provides a list of all persons designated as visitors with selectable report details

16) Holiday Reports – summarizes holiday dates and associated system details

17) Door In/Out Summary Report – lists the number of access granted transactions at specified in/out readers

18) Door Access Summary Report – lists the number of access granted and access denied transactions at specified doors

19) Total People by Hour Report – tabulates, by the hour, access granted transactions at selected readers

20) Alarm Watch Report – reports the in/out status of credentials

21) Group Access Report – summarizes all predetermined group access levels within a specified site

22) Schedule Assignment Report – summarizes schedule types and assignments within a given site

23) E-Plex Door Access Report – summarizes group access levels at wireless locks and the schedules for each specified E-Plex door

b. The system shall furnish the system user with the ability to filter reports based on specifying relevant field criteria.

c. In the case of Transaction Reports, the system shall be capable of allowing a system user to automatically schedule the system software to self-generate a formatted report. The system shall further provide a mechanism to automatically send the report as a PDF attachment to a specified e-mail address.

d. To facilitate report distribution for non-system users, the system software shall provide the means of saving reports as Acrobat® PDF files and other recognized third party file formats.

e. The system shall provide the system user with a report viewer to examine the results of the specified report request.

22. Printing Reports

a. The system shall provide the system user with the ability to print a report from the report viewer interface screen.

b. The system shall allow the system user to direct a print request to the printer interfaced with the Windows® operating system. The report shall be fully formatted complete with report name, headings, page numbers, time, date, and site name.

c. The system shall be capable, where the appropriate computer configuration allows, of selecting network printers.

23. Online Transactions

a. The system shall provide the capability for a system user to view site transactions as each event occurs for enhanced facility observation and security. The system user shall have the option of viewing multiple online transaction windows simultaneously.

b. The system shall allow a system user to view online transactions for remote sites in different time zones in real time.

c. The system shall provide the capability to show on-file images for credential holder related transactions in the online transaction screen.

d. The system shall also provide a dedicated credential transaction monitoring screen in which the screen only displays the image and transaction details of credential holders when presenting a credential at a reader for door or elevator floor access.

24. Software Connections

a. The software shall provide the means to list all servers, system users, and associated access control applications currently operating on the system.

25. Alarm Annunciation And Processing

a. System occurrences deemed as violations shall be articulated as alarms/events at the client module workstation.

b. The system software shall allow assigning user-defined names for any door or input point which serves to distinguish its location for the benefit of the system user.

c. The system shall further provide the following alarm/event notification/processing:

1) Display the alarm/event in a transaction response screen so as to apprise a system user of a potential security breach or problem.

2) If programmed, play an audible warning sound.

3) The system shall provide a designated screen with user-defined alarm/event information and instructions accessible to system users monitoring/operating the software. The information shown shall include:

i) Access control unit reporting the alarm/event

ii) Device name where the alarm/event occurred

iii) Alarm/event type

iv) Date and time of the alarm/event

v) Status of the alarm/event

vi) Alarm/event response instructions and comments

4) The system user shall have the means of acknowledging that either an alarm/event has been investigated and completed or placed on hold for further investigation.

5) The system user shall be provided with a facility to add and save comments on the disposition of an alarm/event.

6) If the system is integrated with an optional CCTV component, the transaction response interface shall provide the system user with the means of viewing images captured by the associated cameras during the alarm/event.

7) As an additional visual aid, the transaction response interface shall provide a system user with the option of opening a floor map to pin-point the location of the door or device that tripped the alarm/event.

8) The system user shall be able to view or examine information for all alarms/events currently waiting for processing one at a time without acknowledging and/or clearing them.

9) The system database shall log each occurrence of an alarm/event.

10) The system user shall be furnished with the means to view new or pending alarm/events or search for alarm/events by device type, by a specific ACU, by transaction type, by site name, or by a date range.

11) The system shall incorporate the ability to e-mail an alarm/event or critical message to a device capable of receiving e-mails.

26. System Health

a. The system software shall have a system health function apprising the user of the current state of the access control system.

b. The system health function shall be represented by colour coded icons indicating various degrees or levels of warnings or alarms.

c. In the event that a health related issue arises, the system health icon shall be clickable opening a drop down box that informs the user of the current health issue. The message in the drop down box shall have a click-through to the relevant screen to address the issue.

27. Building Emergencies/Evacuations/Lockdowns

a. Providing a valid in/out reader configuration exists, the system shall have the capability of automatically issuing an e-mail with a PDF People In/Out Status Report attachment listing who is in and out of the building during emergencies or evacuations.

b. The system shall have a lockdown function designed to lock doors or elevator floors in response to a building emergency.

1) The system shall be designed so a lockdown may be triggered with one of the following methods depending on the control unit series and communication hardware:

i) Client workstation

ii) Global message

iii) Triggering device such as a key switch or push button connected to an assigned auxiliary input

2) The system shall provide a reader lockdown mode whereby the reader's LED flashes rapidly indicating a lockdown is in effect.

28. Database Management and Maintenance

a. The system shall advise system users when the database has reached 90% of its maximum allowable size.

b. The system shall have the provision to automatically upload to the ACUs added, edited, or deleted database information without system user intervention.

c. The system shall provide the capability to perform database uploads to the ACUs on demand.

d. The system shall provide the facility for a system user to back up the database manually at any time or automatically at regularly scheduled intervals which ensures all site information is protected in a saved file. During the backup of the database file, the system shall continue to function with on-going data collection.

e. The system shall provide the option to purge from the database older user-selected transactions. The system shall further provide the option of viewing in CSV format the daily transaction count back to the last date of transactions in the database.

f. Database files may be backed up at another server location or onto another medium such as an external USB drive.

g. The contents of the database shall be available to system users for retrieving site information in user-defined reports.

29. CCTV and Video Management System

a. The system shall provide an optional CCTV license to integrate a closed circuit camera system within the access control system. The camera system shall not be proprietary to the access control system.

b. The system shall interface with compatible NVR models from select manufacturers.

c. The CCTV license shall provide the system user with the ability to access and open the NVR interface for live monitoring and setting camera commands.

d. The system user shall have the ability to retrieve historical video from past alarm events.

30. Software Development Kit (SDK)

a. The system shall interface with an optional software development kit allowing a third party application to manipulate underlying access control software program functions.

31. Intrusion Panel Integration

a. The system shall offer an optional intrusion panel software license that integrates with compatible burglar alarm panels. The system software shall act as a virtual intrusion panel keypad.

b. With the optional intrusion panel software module, the system shall be capable of monitoring the status of zones, areas and partitions.

c. The module shall be capable of allowing a system user to manually arm or disarm individual partitions or configure target readers for remote arming and disarming of partitions.

d. The system shall also provide a mechanism to insert icons representing alarm partitions on an "active map" for real-time monitoring with manual arming and disarming overrides.

32. Active Directory

a. The system shall offer an optional license that integrates with MS Windows Active Directory and shall be capable of the following functions:

1) The system`s people records shall be automatically updated from changes made in MS Active Directory.

2) The system shall be able to use Windows domain or local password login authentication.

33. Output Module

a. The system shall provide a function that outputs software transaction data in either a comma delimited file format (CSV) or UDP message that can be used by other 3rd party applications.

b. UDP Output

1) The system shall be configurable for universal datagram protocol output which identifies and collects the same data as the Output Module. The UDP output shall be capable of being directed to a single or multiple servers.

34. Help

a. The system shall offer a built-in help facility that provides system users with assistance on setting up and operating the access control software. The help shall be accessible by pressing the F1 key from any interface screen.

E. Optional Remote Internet/Intranet WEB Server Application

1. The system shall provide an optional Internet/Intranet WEB server application that allows remote connectivity for managing select access control system functions.

2. The optional Internet/Intranet application shall have user ID and password authentication for secure log on.

3. The optional Internet/Intranet application shall offer two view formats: standard view for devices with larger screens and mobile view for devices with smaller screens.

4. The optional Internet/Intranet application shall offer three interface language options: English, Spanish and French; after login, the optional Internet/Intranet application shall default to the user’s preferred language setting in the system client software.

5. The optional Internet/Intranet WEB server application shall include the following functions:

   a. Add, edit, or delete people records

   b. Show or modify door group and elevator group access levels

   c. Create, edit, or delete schedules

   d. View the current status or manually lock/unlock/pulse system-controlled doors

   e. View the current status or manually secure/de-secure system-controlled elevator floors

   f. View online system activity

   g. Format and produce transaction reports

   h. Schedule and update visit appointments

   i. Enable lockdown function

6. The optional Internet/Intranet WEB Server application shall be programmed with an automatic logout function. After a lapsed time of mouse or keystroke inactivity, the application automatically logs the user out to protect the site from potential unauthorized access.

7. The optional Internet/Intranet WEB Server application shall have a self-contained help module for system-user assistance.

F. Microsoft SQL Server 2012 Database

1. The system shall provide a dedicated internal Microsoft SQL Server 2012 database which shall retain all input data, performed tasks, and site activity including alarms.

2. The system database storage capacity shall be limited only by the hard disk capacity of the server or the limitation of the Microsoft SQL Server 2012 database. Microsoft SQL Server 2012 database supports 10 gigabytes of data storage. Able to upgrade to full SQL, contact Keyscan for purchasing details.

3. The system database information shall be distributed among the ACUs as well as stored on the server.

G. System Communication Service

1. The system shall use a communication service to direct communication between the system database and the access control units. The communication service shall have the following attributes for robust and flexible system communication:

   a. The communication service shall be configured as a Windows™ service and run automatically with nominal system user intervention.

   b. The communication service shall be designed to regulate data flow sending system user updates/commands to and receiving transactions from all access control units at all sites.

H. Optional Reverse Network Communication

1. The system shall provide an optional communication application referred to as “reverse network communication” whereby the ACU initiates communication with the communication application installed on a server located at a host site or centrally managed facility.

2. Reverse network communication shall be compatible to operate over a network (TCP/IP), corporate intranet, or the Internet.

3. Reverse network communication shall use specialized communication hardware that employs AES Rijndael 256-bit encryption technology for secure data transmission over the Internet.

4. Reverse network communication shall employ Dynamic Host Communication Protocol (DHCP) at the access control unit to communicate with system servers eliminating associated static IP address costs and IT management and oversight.

2.5 CONTROL UNIT TECHNICAL SPECIFICATIONS

A. Control Unit Configuration

1. The system shall be comprised of access control unit(s) to regulate and monitor door access and monitor inputs and/or elevator control units to regulate and monitor elevator floor access.

2. The access control units shall have dual on-board processors for robust performance such that during uploading and downloading of data the system operates at peak efficiencies.

3. The standard access control units shall be capable of storing up to 45,000 credential holder records.

    a. The system shall be capable of integrating an optional M-series control unit with expanded memory which can store up to 90,000 credential holder records.

4. All ACUs shall have fully distributed and fully intelligent data processing and shall be capable of rendering all decisions independently. Further, if the system goes off-line, the ACUs will continue to function at 100% operability without resorting to a de-graded mode of operation.

5. Access control units shall be capable of retaining the last six thousand (6,000) events in memory such that, in the event of disrupted communication, those transactions captured during an off-line period shall be transmitted to the database server when communication is restored.

6. Database information required for full functioning of each reader shall be distributed to reside in the non-volatile memory of the ACU.

7. The control unit shall store proprietary software and program logic in read only memory (PROM).

8. The access control units shall be capable of accepting other Wiegand protocols.

9. The access control unit shall match the credential number against the internal number with no cross-referencing.

10. The control boards shall have a protective metal cover to safeguard the circuit board's vital components and ensure extended board longevity.

11. The control board shall have system and communication LEDs. The LEDs shall be readily identified and visible providing technicians with a valuable diagnostics resource when installing and servicing the controller.

12. The door control boards and the elevator control boards shall be available in the following configurations.

    a. Door control boards – 1, 2, 4, & 8 portal configurations

        1) The door control board with the single (1) portal configuration shall be a stand-alone unit and have the following additional features:

i) Have a built-in on-board Ethernet module (IEEE 802.3af) configurable for encrypted and non-encrypted communication.

ii) Capable of operating with Power over Ethernet (PoE) via the on-board Ethernet module (680 mA @ 12 VDC) or from an independent 12 VDC power supply.

iii) Support Dynamic Host Configuration Protocol (DHCP)

b. Wireless lock interface control unit – 8 door, stand-alone unit. The wireless lock interface control unit shall provide integration with select manufacturer`s wireless locks

c. Elevator control boards – 1 & 2 cab configurations

13. Operating Voltages

a. The transformers shall be Class II - 16VAC 40VA or 16.5VAC 37VA.

b. The internal power supply shall be 13.5 VDC @ 1.2 amps.

c. The backup battery shall be 12VDC 7 amp/hr.

14. Operating Environment

a. The control units shall operate within the following environmental conditions:

1) Fahrenheit: 41° to 120°

2) Celsius: 5° to 49°

b. Humidity: 0% to 90% R.H., non-condensing

15. Relay Outputs

a. The relay outputs shall be Form C contacts rated at 24VAC – 10 Amps, 30VDC – 5 Amps maximum.

16. Control Unit Enclosure – for 2, 4 and 8 door control units and elevator control units

a. The control unit enclosure shall be a single locking box CEMA/NEMA Type 1.

b. The dimensions of the enclosure shall be as follows:

1) Imperial – Height 20 in. x Width 16 in. x Depth 5 1/2 in.

2) Metric – Height 50.8 cm x Width 40.64 cm x Depth 13.97 cm

c. The control unit enclosure shall be equipped with a tamper switch such that it may be connected to an auxiliary input for alarm monitoring in the event the unit is opened without authorization.

17. Control Unit Enclosure – for 1 door and 8 wireless lock interface control units

a. The dimensions of the unit shall be as follows:

1) Imperial – Height 7.625 in. x Width 6.875 in. x Height 1.75 in.

2) Metric – Height 19.37 cm x Width 17.46 cm x Height 4.45 cm

B. Readers

1. (Placeholder for bidder specification statements otherwise delete line and if applicable article title above.)

2. (Placeholder for bidder specification statements otherwise delete line)

C. Credentials

1. (Placeholder for bidder specification statements otherwise delete line and if applicable article title above.)

2. (Placeholder for bidder specification statements otherwise delete line.)

PART 3 - EXECUTION

3.1 INSTALLERS

A. (Placeholder for bidder specification statements otherwise delete line and if applicable article title above.)

3.2 INSTALLATION

A. Installation shall comply with all other relevant sections.

B. The system shall be installed in accordance with manufacturer specifications and installation guidelines.

C. (Placeholder for bidder specification statements otherwise delete line and if applicable article title above.)

3.3 TESTING AND CERTIFICATION

A. The access control system and its subsidiary components/integrated systems shall be tested in accordance with the following parameters:

1. (Placeholder for bidder specification statements otherwise delete line and if applicable article title above.)

2. (Placeholder for bidder specification statements otherwise delete line and if applicable article title above.)

3.4 ACCEPTANCE TESTING

A. (Placeholder for bidder specification statements otherwise delete line and if applicable article title above.)

3.5 TRAINING

A. The Vendor shall provide at least ____days of formal, hands-on training of the installed system. The cost of this training shall be included in the tender price.

B. (Placeholder for bidder specification statements otherwise delete line and if applicable article title above.)

3.6 MAINTENANCE AND REPAIR AGREEMENTS

A. The Vendor shall have an ongoing agreement with the Purchaser for the maintenance and repair of the system equipment. The tender price shall include the cost of maintenance for a period of ____months after system installation. Requirements for maintenance schedules, documentation, and tasks are listed in an attached addendum.

B. The Vendor agrees to arrange all software licenses as stipulated by the supplier. The Vendor also agrees to purchase appropriate software maintenance agreements for full support and maintenance of all system software as available from the supplier. The price of all software licenses and maintenance agreements shall be included in the tender.

C. Where the Vendor plans to sub-contract any portion of the maintenance contract, he shall indicate the items affected and the names of the sub-contractors.

D. Placeholder for bidder specification statements otherwise delete line and if applicable article title above.)

END OF SECTION