Appendix C – Security Management System Technical Specifications

STATE OF SOUTH DAKOTA

SECURITY MANAGEMENT SYSTEM
TECHNICAL SPECIFICATIONS

1.01 INTENT

A. It is the intent of this document to define the functional requirements for an integrated security management system (SMS) for the State of South Dakota ("State").

B. The purpose of this document is to specify security management system requirements in a generic and non-manufacturer-specific manner. It is understood that terminology, system architecture, and application design vary greatly between system manufacturers. This document does not intend to exclude any security management system that may use a different terminology or system architecture, provided that all functional requirements of this specification can be met.

C. In this document, the term "system" shall mean the integrated security management system.

1.02 SYSTEM OVERVIEW

A. The system shall provide access control, alarm monitoring, photo identification badging, and security control functions for the State of South Dakota. For details regarding physical hardware, please see section 1.09 below.

B. The system shall consist of the following essential components:

1. Intelligent Controllers: Intelligent field panels (defined as "Intelligent Controllers" within this document) shall be used to support access control and alarm monitoring functions within various buildings throughout the State. Intelligent field panels shall serve as connection points for card readers, monitor point inputs, and system outputs.
2. SMS Host Computer: The SMS host computer shall be an industry-standard server-type computer running SMS application "server" software. The SMS host computer is to be centrally located within the State or hosted at a hosting site that meets State expectations for security and reliability. SMS host computer shall provide centralized security control, monitoring, and database management for Intelligent Controllers located at State buildings.

3. SMS Operator Workstations: SMS Operator Workstations shall be industry-standard computers running SMS application "client" software. Operator Workstations shall serve as the user interface to the system and shall be used for programming, administration, and monitoring functions. Operator Workstations shall be installed as needed at various locations throughout the State.

4. SMS Browser Interfaces: Basic SMS Operator Workstation functionality shall be provided via industry-standard browsers (e.g., Chrome, Microsoft Edge), operating on industry-standard computers and possibly iOS/Android mobile devices as well. Thick client-only applications will not be considered.

1.03 SYSTEM ARCHITECTURE

A. The system shall use a flexible, open architecture that facilitates the integration of a wide range of security systems.

B. System shall use "industry-standard" computer hardware, operating systems, surveillance systems, databases, etc. To the greatest extent possible, system software shall utilize industry standard application software for system functions such as databases, graphical user interfaces, and communications.

C. Operating system for the security management system shall be Microsoft Windows Server 2019 or later. All SMS client and server software (if applicable) shall have been written as native Windows applications. Unless hosted at a vendor location, systems that use an underlying operating system other than Windows (such as Linux or UNIX) shall not be considered.

D. System shall interface to external systems using a "software" level interface, where encrypted commands are exchanged between systems using a standard communications interface, such as an Ethernet connection. Systems that require a "hardwired" interface (where dry-contact outputs from one system must be wired to inputs of the other system or vice versa) shall not be used.

E. System shall support the sharing of data with external databases and other application software using industry-standard, encrypted protocols.

F. System shall provide an API, or the offeror shall demonstrate and attest to investment in the development of an API capable of integrating with State standard electronic credentialing and identification systems.

1.04 USER INTERFACE – GENERAL

A. System shall be designed to be practical and user-friendly (requiring fewer clicks, fast speed to transaction completion, etc.) for any non-technically proficient State employees assigned responsibility for managing the system. For this document, the term “System Operator” shall mean any State employee responsible for managing the security management system or any portion thereof.

B. System shall allow authorized System Operators to define and modify system operating parameters, such as cardholder records, doors, time codes, monitor points, alarm conditions, and the like. For this document, the term “configuration” shall mean the definition of system operating parameters by a System Operator.

C. Operation, monitoring, and configuration of the system shall be usable by industry-standard desktop or laptop computers and industry-standard browsers (e.g., Chrome, Microsoft Edge) running on such computers. The system shall provide “client” software that allows industry-standard computers to serve as “workstations” for the SMS directly and/or through a browser. The installation of special software (including browser “plug-ins”) on the remote computer shall not be required.

D. Operator Workstations shall be connected to the SMS host computer through the State’s existing Ethernet network. The State’s network allows for multi-can, encryption, routable, firewall (FW) ports. For this document, the term “Operator Workstation” shall mean an industry-standard computer running client software or a browser interface (using Microsoft Edge, Chrome) and serving as a workstation for the SMS.

E. The use of a desktop or laptop computer as an Operator Workstation shall not prevent other application software such as word processors, spreadsheets, and electronic mail programs from being used on the same computer.

F. The system shall be multi-user, multi-tasking, and allow the simultaneous use of multiple Operator Workstations in line with State standards. The system shall allow no fewer than thirty-two (32) Operator Workstations to be in use simultaneously. If licensing costs are associated with Operator Workstations, those costs must be included as part of the offeror’s response.

1.05 USER INTERFACE – GRAPHICAL FEATURES

A. The system application software shall provide the operating features indicated within this document. System software shall use menu-driven commands and provide interactive prompts. The system shall use English language program and error messages, providing clear and understandable sequences of events. The user interface and menu structures shall be consistent throughout the system.

B. System shall provide a Windows-style graphical user interface that makes extensive use of graphical elements such as toolbars, icons, and pull-down list boxes. System commands and functions shall be available using a “mouse” type pointing device. Text-based systems that require the entry of commands on a command line shall not be used.

C. Any part of the system that is not solely browser-based shall use the Microsoft Windows graphical user interface and have the “look and feel” of a standard Windows application program (such as Microsoft Office). System shall comply with established standards and conventions set forth for Windows applications.

D. All system functions shall be available via a graphical user interface. It shall not be necessary to “shell-out” of the graphical user interface to execute any system command.

1.06 USER INTERFACE – OPERATOR RESTRICTIONS

A. Access to the system shall require users to authenticate to the system. System password processes shall be capable of using the State’s Single Sign On (SSO) process. All users must login with an account managed by BIT, preferably utilizing OAuth2 or OpenID Connect.

B. System shall provide multiple System Operator permission levels, each allowing a different degree of System Operator privilege, as configured by the State. The system shall provide no less than fifty (50) System Operator levels. It shall be possible to assign various groupings of commands and system functions to each level. System Operators logging on to the system will only have access to the system commands and functions determined by their assigned levels.

C. All system functions shall be available at any Operator Workstation provided that the System Operator has the correct permission level. The system shall not require that system functions be segregated by workstation, i.e., there should be no distinction between a “system administration” workstation, “alarm monitoring” workstation, or “badging” workstation.

1.07 USER INTERFACE – HELP UTILITY

A. System shall have integral online help utility. Help utility shall be available from any menu screen through a help icon and as a pull-down menu option. Help utility shall conform to Microsoft Windows conventions and operate similarly to the help utilities found in common Microsoft Windows applications.

B. Help utility shall be context-sensitive, providing appropriate information relevant to the particular task that the System Operator is attempting to perform. (For example, activating the help icon while in the cardholder record screen shall automatically bring up help topics related to entering/editing cardholder record data.)

C. Help utility shall provide complete information necessary for the management and operation of the system. Information contained within help utility shall minimize or eliminate the need for the System Operator to consult a printed instruction manual.

1.08 WEB BROWSER USER INTERFACE

A. As described earlier in section 1.04, in addition to the Operator Workstation, the system shall provide a web browser user interface that is accessible using standard web browser software.

B. Web browser user interface shall permit essential system functions (such as editing a cardholder record, modifying a time code, manually unlocking a door, etc.) to be performed by System Operators with a valid password.

C. Web browser user interface shall be accessible from any network-connected remote computer with a standard web browser. The installation of special software (including browser “plug-ins” or other software such as Java) on the remote computer shall not be required.

D. Additional consideration may be granted to systems able to effectively support basic interface-based functionality via browsers and potentially on apps running on mobile devices such as tablets and phones.

1.09 PHYSICAL ACCESS CONTROL FEATURES

A. System shall provide card access control of doors, gates, elevators, and other devices. Each card access-controlled point shall be provided with a card reader. The system shall provide an individual contact output for each card reader that shall be used to unlock doors and other devices. Output shall provide a normally-open and normally-closed contact. Output time shall be System Operator-definable and capable of being adjusted from 1 to 60 seconds for each output. The card reader and output combination shall be defined as a “Door.” The system shall provide the capacity for a minimum of 2,500 Doors. The offeror shall document in the response the maximum number of doors possible.

B. The system shall provide the capability for the System Operator to assign an alphanumeric name to each Door. The Door name shall be a minimum of twenty-four (24) alphanumeric characters. The Door name shall be used on system menus and reports for identification purposes.

C. Doors shall be capable of being grouped for the purpose of control. A “Door Group” shall be a System Operator specified group consisting of a combination of one or more Doors, as selected by the System Operator. The system shall provide the capacity for a minimum of two-thousand-forty-eight (2048) System Operator-definable Door Groups. A Door shall be capable of being assigned to multiple Door Groups.

D. To assist the offeror with its cost estimates, below is a list of approximate quantities of access control types across a variety of physical sites statewide to be monitored by the system. If the offeror(s) will require new hardware to be installed, consider these quantities in your estimates for purchase, delivery, installation, wiring, setup, training, staffing/labor, travel costs, etc.

Access Control Type	***Approximate Quantity***	***Notes***
Buildings	70	This number is increasing daily
Doors	683	This number is increasing daily
Gates	9	All gates are outdoors
Security Cameras	800	Not currently integrated with door security, but would like them to be
Monitored Fences	N/A	Not currently being utilized, but would like to have this capability
Access Cards	6,500 cards currently being utilized	To future proof, the system should be able to handle 15,000+
CardReaders	683	This number is increasing daily
Controllers	105	
Digital Keypads	62	
Intrusion Systems with Alarms	6	
Monitoring Points with Alarms	500	
Environmental Monitors (Temperature, Moisture Detection, etc.)	N/A	Not currently being utilized but would like to have this capability

E. Essential operation shall be as follows: Presentation of access card at card reader shall cause the card reader to read, identify and send the card information to the system processor (Intelligent Controller). Processor checks card information against System Operator-specified criteria. If card information meets the criteria, then the processor sends the signal to unlock the door and initiates a “Valid Access” condition. If card information does not meet System Operator-specified criteria, the system shall initiate an “Invalid Access Attempt” condition.

F. All communication related to the presentation and reading of a card shall use encryption such that it is highly secure and cannot be hacked by intercepting communications. This includes “through the air” via RF or other means of transmitting wirelessly, but also through the communication wires or fibers that relay the card information back to the system.

1.10 ANTI-PASSBACK FEATURE

A. At locations where card readers are used for both entrance and egress through a Door, the system shall allow each card reader to be System Operator-defined as either an “entry” reader or "exit” reader. The system shall require a cardholder using a card at an "entry" reader to subsequently use the card at an “exit” reader before the card can once again be used at an "entry” reader. This feature shall be known as the “Anti-passback" feature. Cardholders attempting to use cards out of sequence shall be denied access and shall cause a “Passback Violation” condition. If so configured, Passback Violations shall create an Alarm Condition, causing an immediate report to be sent to Operator Workstation; and causing other System Operator-specified system operations to occur.

B. System shall provide a passback “forgive” feature that can be activated by System Operator. The passback forgive feature will reset the passback status of any card to a neutral condition (neither “in” nor “out”), allowing the passback sequence to be restarted.

C. System shall allow the Anti-passback feature to be enabled and disabled upon System Operator command and automatically based on Time Code.

1.11 ELEVATOR CONTROL FEATURE (This is a nice-to-have feature)

A. The system shall provide an elevator access control feature that permits access control of individual elevator cars. To operate an elevator car, the cardholder will present his access card to a card reader inside the elevator. The system shall respond to a valid access card by activating outputs that temporarily enable the floor selection buttons for those floors to which the cardholder is authorized. The system shall support elevator access control for a minimum of 96 elevator cars, with up to 24 floors per elevator.

If the system provides this support via a separate module, that must be noted in the response. The information must include the module name, owner, cost, and a diagram showing its basic components.

B. The system shall allow, but shall not require, outputs from elevator car floor selection buttons to be connected as monitor point inputs to the system. When so connected, the system shall track which floor was selected when the card reader was used and automatically reset floor outputs for other floors once the initial floor has been selected.

C. Elevator control feature shall be fully functional even when Intelligent Controllers are “off-line” with the SMS host computer. The system shall not rely on the host SMS host computer to provide elevator control functions.

1.12 DIGITAL KEYPAD FEATURE

A. The system shall permit the use of digital keypads as alternate or supplemental access control devices. Keypads shall provide no fewer than twelve numeric keys. Operation of a digital keypad shall require the entry of a valid Personal Identity Number (PIN). The PIN for each user shall be definable by System Operator. As per the table in 1.09.D, there are currently 62 digital keypads in use by the State. These keypads will need to be compatible with the upgraded system, which could include environmental controls/monitoring.

B. PIN Keypads shall be capable of being defined by the System Operator to operate in “PIN Only Mode.” When in PIN Only Mode, entry of a valid PIN permits access. Use of an access card is not required in PIN Only Mode.

C. PIN Keypads shall be capable of being defined by the System Operator to operate in “PIN Plus Card Mode.” When in PIN Plus Card Mode, both entry of a valid PIN, plus the use of a valid access card corresponding to PIN, shall permit access. Use of an access card alone or PIN alone shall not permit access when PIN Plus Card Mode is enabled.

D. System shall allow the switching between PIN Only Mode, PIN Plus Card Mode, and Card Only Mode upon manual command by System Operator and automatically based on Time Code as assigned by System Operator. When in Card Only Mode, the system will disable PIN Keypad, allowing the use of a valid access card alone.

1.13 DEFINITION OF ACCESS PRIVILEGES

A. The system shall use a flexible, modular method of defining which doors each cardholder can enter and when.

B. A “Time Interval” shall be defined as a continuous range of time that can be contained within a 24-hour day. (An example of a Time Interval would be: 00:00 – 22:00). Time Intervals shall be System Operator-definable. The system shall provide the capacity for a minimum of one-thousand-twenty-four (1024) System Operator-definable Time Intervals.

C. A “Holiday” shall be a System Operator-specified date that shall be treated by the system as a Holiday. On dates defined as a Holiday, the system shall use the time criteria that have been System Operator-specified for Holidays. The system shall provide the capacity for a minimum of sixty-four (64) System Operator-specified Holidays.

D. A “Time Code” shall be a System Operator-specified code comprising combinations of Time Intervals and Days of the Week. Time Code shall be used to specify times that the card may be used to gain access. Each Time Code shall allow not less than three individual Time Intervals for each day of the week and shall allow for not less than three individual Time Intervals for the day that is System Operator-specified as a Holiday. The system shall provide the capacity for a minimum of one-thousand-twenty-four (1024) System Operator-definable Time Codes.

E. A “Clearance Code” shall be a System Operator-specified group consisting of a combination of one, two, or three Door Groups; and one, two, or three Time Codes, as selected by System Operator. Clearance Codes shall be used to specify each card’s access privilege level. The system shall allow the assignment of up to ten (10) individual clearance codes to each card. The system shall provide the capacity for a minimum of two-thousand-forty-eight (2048) System Operator-definable Clearance Codes.

F. The system shall provide the capability for the System Operator to assign an alphanumeric name to each Clearance Code. Clearance Code name shall be a minimum of twenty-four (24) alphanumeric characters. The Clearance Code name shall be used on system menus and reports for identification purposes.

G. System shall allow the System Operator to establish an “Effective Date/Time” for each individual access card. The Effective Date/Time shall be the date and time that the access privileges associated with that card begin to take effect. Cardholders attempting to use an access card before the Effective Date/Time shall cause an Invalid Access Attempt condition to occur.

H. The system shall allow the System Operator to establish an “Expiration Date/Time” for each individual access card. The Expiration Date/Time shall be the date and time that the access privileges associated with that card shall be canceled. Cardholders attempting to use an access card after the Expiration Date/Time shall cause an Invalid Access Attempt condition to occur.

1.14 CARDHOLDER RECORDS

A. The system shall provide a unique “Cardholder Record” to store data for each cardholder in the system. The system shall provide capacity for a minimum of twenty-five thousand (25,000) Cardholder Records.

B. The system shall provide a data entry screen (form) to allow the creation and editing of Cardholder Records. The Cardholder Record shall contain the following fields as a minimum:

1. Cardholder Identification Number: 1 to 14-digit record number.
2. Cardholder Name: 1 to 48-character alpha-numeric name.
3. Access Card Number #1: 1 to 9-digit access card number encoded on the cardholder’s primary access card.
4. Access Card Number #2: 1 to 9-digit access card number encoded on the cardholder’s secondary access card.
5. Access Card Number #3: 1 to 9-digit access card number encoded on the cardholder’s tertiary access card.
6. PIN Number: 1 to 8-digit. (Personal identification number, if used.)
7. Effective Date/Time: Date/Time when access privileges are to begin.
8. Expiration Date/Time: Date/Time when access privileges are to expire.
9. Clearance Codes: Allows assignment of 1 to 10 named Clearance Codes.
10. Trace: On/Off flag (If flag enabled, causes special Trace report to be generated when a cardholder uses access card.)
11. Date/Time Last Changed: Identifies the date/time when this record was created or last modified. (Data for this field is automatically provided by the system and cannot be edited.)
12. Last Changed By: Identifies the System Operator who created or last modified this record. (Data for this field is automatically provided by the system and cannot be edited.)
13. Twenty-four (24) user-defined fields: (Custom alpha-numeric fields, consisting of up to 255 characters each, to be used as determined by the State.)

C. The system shall permit the State to custom-tailor the format and overall appearance of the Cardholder Record form.

D. The system shall use the Cardholder Identification Number as the primary key to uniquely identify the record in the database. The system shall permit the use of access card numbers as a key but shall not use access card numbers as the primary key.

E. The system shall allow no less than three different access card numbers to be assigned to each cardholder record. The system shall not require that a separate cardholder record be created for each access card number.

F. The system shall permit the creation of a Cardholder Record without requiring an access card number to be assigned. This feature shall allow a Cardholder Record to be created for “PIN Only” users who will be assigned a PIN only and not an access card.

G. The system shall provide an automatic “look-up” and selection function for Clearance Code fields in the Cardholder Record. The look-up function shall permit the System Operator to list and select, through a “pop-up” menu (or equivalent), any Clearance Code that has been defined in the system and to identify the Door Groups, Doors, and Time Codes associated with that Clearance Code. The look-up function shall not require that the System Operator exit from the Cardholder Record screen to perform this function.

1.15 AUTOMATIC ADJUSTMENT FOR TIME CHANGES

A. The system shall use a standard time source (such as NTP) to provide the ability to automatically adjust the system time to accommodate changes (e.g., the beginning and end of Daylight Savings Time) to ensure all devices, workstations, and servers stay in synch for logging purposes. The system shall allow the time changes to be set by System Operator in advance if needed.

1.16 PARTITIONED DATABASE FEATURE

A. The system shall provide the ability to establish multiple “logical views” of the access control system and cardholder database. Each “logical view” shall permit the viewing and modifying of only certain Cardholder Records, Clearance Codes, Doors, Door Groups, Monitor Points, and other such data. This capability shall allow the creation of logical access control “sub-systems.” The system shall allow the creation of not less than one-hundred-twenty-eight (128) logical sub-systems.

B. Each “sub-system” shall have full system capabilities, appear to the System Operator, and operate as if it were an independent access control system. (The typical sub-system used at the State would consist of a single building, but a sub-system may also consist of a single department in multiple buildings or a single department within a building that houses multiple departments.)

C. Creation of sub-systems shall be done through software partitioning of the database and shall not be dependent on the system hardware configuration.

D. The system shall allow the System Operators to be assigned privileges to view, create, or edit data in only specific “sub-systems”. For example, a System Operator who is only assigned privileges for sub-system “A” shall only be able to view and edit database records affecting sub-system “A.” This System Operator would be restricted from viewing and modifying other portions of the system database.

E. System Operator functions which may be restricted by sub-system shall include, but shall not be limited to, the following:

  1. Adding, deleting, and modifying Cardholder records
  2. Locking and Unlocking of Doors
  3. Arming and Disarming of Monitor Points
  4. Printing of activity reports
  5. Configuration of Clearance Codes, Time Codes, Door Groups, and other system parameters
  6. Establishment of automatic door lock and unlock times
  7. Monitoring of Alarm Conditions from specific Doors and Monitor Points

F. The system shall allow the assignment of any Door, Door Group, Monitor Point, Alarm Group, Auxiliary Output Contact, or other system elements to any sub-system.

G. It shall be possible to simultaneously assign any Door, Door Group, Monitor Point, Alarm Group, Auxiliary Output Contact, or other system elements to more than one sub-system.

H. The System Operator password shall determine access to each specific sub-system.

I. The use of logical sub-systems shall not prevent authorized System Operators from making system-wide changes or generating system-wide reports. (For example, it shall be possible for an authorized System Operator to add/delete a cardholder from all sub-systems with a single entry. The system shall not require a separate entry to add/delete a cardholder from each sub-system.)

1.17 INTERFACE TO EXTERNAL DATABASES

A. The system shall provide the ability to “import” information into the security management system host computer from existing personnel databases or other SMS system databases. The purpose of importing this information is to minimize the need for persons managing the access control system to manually enter data. Some of the desired capabilities include:

1. The ability to import information from the databases for the initial load of the cardholder database and for major loads of new information periodically.
2. The ability to update the cardholder database based on the import of an “exception file” reflecting change in employee status. Import of exception files shall allow the system to automatically add cardholder records, delete cardholder records, modify access privileges, and change other information contained in the cardholder database. The system shall allow the import of an exception file at any time.

1.18 DOOR CONTROL FEATURES

A. System shall be capable of unlocking and re-locking Doors and Door Groups upon command from Operator Workstation. The command shall be capable of being executed from a pull-down menu, an icon on the status screen, and an icon on Custom Map Display. The system shall automatically disable Door Forced conditions and Open-Too-Long conditions from doors that have been unlocked by the System Operator command.

B. System shall be capable of automatically unlocking and re-locking Doors and Door Groups based on Time Code, including the potential for a mass lock-down capability and/or panic-button related features. The system shall be capable of automatically disabling Door Forced conditions and Open-Too-Long conditions for Doors that Time Code has unlocked. The system shall also permit Doors that have been automatically unlocked to continue to be monitored for Open-Too-Long conditions if so, configured by System Operator.

C. System shall provide the capability to selectively disable Doors upon command from designated Operator Workstations. Disabled Doors shall deny access to all cardholders.

1.19 AUXILIARY CONTROL FEATURES

A. System shall have the capability to provide “Auxiliary Output Contacts” for auxiliary control purposes, such as the unlocking of non-card-reader-controlled doors, operation of audible alarm devices, and other such functions. Auxiliary Output Contacts shall be capable of being assigned to Door Groups and operated upon command from Operator Workstation and automatically by Time Code. The system shall provide the capacity for a minimum of ten thousand (10,000) Auxiliary Output Contacts.

B. The system shall provide the capability for the System Operator to assign an alphanumeric name to each Auxiliary Output Contact. Auxiliary Output Contact name shall be a minimum of twenty-four (24) alphanumeric characters. The Auxiliary Output Contact name shall be used on system menus and reports for identification purposes.

1.20 DOOR STATUS MONITORING

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

B. Where a card reader is provided only on the entry side of a door, the system shall allow the door Forced monitor to be disabled from the door’s exit side. Disabling of Door Forced monitor shall be accomplished through the use of a request-to-exit input, defined as a “REX.” REX input shall be a dry contact input to the system, allowing the connection of release buttons, motion detectors, and other devices. If the system is so configured, the operation of REX input shall disable the Door Forced monitor for a System Operator-specified period of time, allowing exit without causing a Door Forced condition. If the system is so configured, REX input shall also be capable of unlocking the door. One REX input shall be provided for each access-controlled Door.

C. System shall provide the capability to disable REX feature for each Door remotely. Each REX shall be capable of being disabled automatically by Time Code and upon command from Operator Workstation.

D. The system shall monitor the status of each access-controlled door to determine the length of time the door is left open. The time period shall be capable of being set for a System Operator-selected period of between 1 to at least 300 seconds. The time period shall be individually selectable for each Door.

E. System shall provide the capability to remotely disable the “Open-Too-Long” monitoring feature for each Door. The feature shall be capable of being disabled automatically by Time Code and upon command from Operator Workstation.

F. Door Forced conditions and Open-Too-Long conditions shall be immediately processed by the system in accordance with parameters established by the System Operator. If so configured, Door Forced conditions and Open-Too-Long conditions shall create an Alarm Condition, causing an immediate report to be sent to designated Operator Workstations and causing other System Operator-specified system operations to occur.

1.21 ALARM MONITORING FEATURES

A. The system shall provide monitoring of contact inputs from door switches, motion detectors, and other sensors located at field locations. Each input shall be defined as an individual “Monitor Point.” The system shall provide a minimum capacity of ten thousand (10,000) Monitor Points.

B. Monitor Point inputs shall utilize a supervised circuit requiring an end-of-line resistor. Inputs shall accept both normally-open and normally-closed dry contact input signals. Inputs shall provide a minimum of three distinct states, including “normal” (input is in normal or inactive condition), “alarm” (input is in alarm or active condition), and “trouble” (input is in fault or tamper condition).

C. Each Monitor Point shall be identified on system displays by a unique Monitor Point number. In addition, the system shall provide the capability for the System Operator to assign an alphanumeric name to each Monitor Point. Monitor Point name shall be a minimum of twenty-four (24) alphanumeric characters. The Monitor Point name shall be used on system menus and reports for identification purposes.

D. The system software shall provide an “Auxiliary Door Monitoring” feature. The Auxiliary Door Monitoring feature shall permit a REX input point to be logically associated in software with a Monitor Point to create a “virtual” door. This feature shall allow non-card reader doors to be monitored for both “door-forced” conditions and “open-too-long” conditions without requiring a card reader input port be used.

E. Monitor Points shall be capable of being grouped for the purpose of control. An “Alarm Group” shall be a System Operator-specified group consisting of a combination of Monitor Points selected by the System Operator. The System shall provide the capacity for a minimum of two-thousand-forty-eight (2048) System Operator-definable Alarm Groups.

F. The system shall provide the capability for the System Operator to assign an alphanumeric name to each Alarm Group. The Alarm Group name shall be a minimum of twenty-four (24) alphanumeric characters. The Alarm Group name shall be used on system menus and reports for identification purposes.

G. The system shall provide the capability to Arm (enable) and Disarm (disable) Monitor Points by command from Operator Workstation. The command shall be capable of being executed from a pull-down menu, an icon on the status screen, and an icon on Custom Map Display. Enabling a Monitor Point shall allow Monitor Point to cause an Alarm Condition if a point is activated. Disabling a Monitor Point shall prevent Monitor Point from causing an Alarm Condition if a point is activated. Monitor Points shall be capable of being Armed and Disarmed individually and by Alarm Group.

H. The system shall have the capability to automatically Arm and Disarm Monitor Points and Alarm Groups by Time Code.

I. Monitor Points shall be capable of locking and unlocking access-controlled Doors and Door Groups upon Alarm Condition.

1.22 EXTERNAL CONTROL OF ALARM GROUPS

A. The system shall allow Alarm Groups to be Armed and Disarmed through the use of card readers designated as “Arming Readers.” Presenting a valid access card to Arming Reader shall toggle the Alarm Group from the Armed state to the Disarmed state and vice versa.

B. The system shall allow Alarm Groups to be Armed and Disarmed through the use of external hardwired controls (such as a key-operated shunt switch.) The system shall permit Monitor Points to be defined as “Shunt Points.” Shunt Points shall be capable of being assigned to control an Alarm Group. When a Shunt Point is active, the Alarm Group it controls shall be Disarmed. When a Shunt point is normal (inactive), the Alarm Group it controls shall be Armed.

C. The system shall allow Auxiliary Output Contacts to function as Alarm Group status outputs. Two types of outputs shall be capable of being defined:

1. Armed Status Output: Output contact operates when the Alarm Group is in Armed Condition. (Typically used for “armed-status” indicator lights.)
2. Secure Status Output: Output contact operates when all Monitor Points assigned to the Alarm Group are in normal condition. (Typically used for “ready-to-arm status” indicator lights.)

1.23 CUSTOM MAP DISPLAYS

A. In addition to other means, the System shall be capable of displaying the status of and controlling system elements through the use of Custom Map Displays.

B. A “Custom Map Display” shall be a multi-color graphic display generated on Operator Workstations. Custom Map Displays shall be System Operator-created graphic displays that show the floor plans of buildings and other facilities.

C. Custom Map Displays shall allow the display of symbols (icons) representing Doors, Monitor Points, Auxiliary Output Contacts, and other such system elements to be placed on the map adjacent to rooms, doors, and other building features. Upon change of status, symbols shall flash or change color to identify a change of state.

D. Custom Map Displays shall allow activation of operator commands such as locking and unlocking Doors, arming and disarming Monitor Points, and operating Auxiliary Output Contacts. Commands on Custom Map Displays shall be activated by clicking on an icon representing a system element and then choosing desired command (unlock, relock, etc.).

E. Custom Map Displays shall be capable of being created using complex graphics shapes, including lines, circles, multi-sided polygons, complex curves, filled objects, and the like. Custom Map Displays shall be capable of utilizing no fewer than sixteen distinct colors.

F. Custom Map Displays shall be capable of being drawn using either the Operator Workstation keyboard or with a “mouse” type pointing device. All software tools necessary for creating Custom Map Displays shall be included with the system.

G. Custom Map Displays shall be capable of being created through the import of Autocad .DWG,.DXF, or other industry-standard drawing files.

H. Systems that store maps as vector-based files and allow “dynamic resizing” of map displays are strongly preferred over systems that store maps as bitmap files. “Dynamic resizing” shall allow a map image to be created and stored as a vector-based file. Once created, the image may be “panned” and “zoomed” without losing detail, allowing a single image to be viewed on-screen at any scale. Systems which use bitmap files and require that multiple maps be created to achieve the “zooming” effect are acceptable but less desirable.

I. System shall permit linking of Custom Map Displays, allowing links to be inserted on maps, which, when activated, cause the display of a different map. The system shall permit not less than three levels of map linking.

J. System shall provide a minimum of two thousand (2000) unique Custom Map Displays.

1.24 ALARM DISPLAY FEATURES

A. The system shall immediately process the activation of the Monitor Point in accordance with parameters as established by the System Operator. If so configured, activating a Monitor Point shall create an “Alarm Condition,” causing an immediate report to be sent to designated Operator Workstations, and causing other System Operator-specified system operations to occur. The maximum time period from activating the Monitor Point until Alarm Condition is displayed on Operator Workstation shall not exceed five (5) seconds.

B. System shall be capable of displaying Operator Instruction Displays. “Operator Instruction Displays” shall be System Operator-created text messages of not less than 160 characters. The system shall provide a minimum of two thousand (2000) unique Operator Instruction Displays.

C. Upon Alarm Condition, System Operator-designated Operator Workstations shall sound an audible warning, display an alarm message, and graphically identify the point that caused the condition.

D. If so configured by System Operator, Alarm Condition shall automatically display a System Operator-specified Custom Map Display on Operator Workstations. The symbol (icon) representing the Door, Monitor Point, or other device causing Alarm Condition shall change color or flash to identify the point of alarm origination.

E. If so configured by System Operator, Alarm Condition shall automatically display a System Operator-specified Custom Operator Instruction Display.

F. The system shall provide real-time tracking of the actual status of each Armed Monitor Point, indicating when Monitor Point is activated, and when Monitor Point is cleared, and record all such information in System Journal.

G. Alarm Conditions shall be capable of being configured to require System Operator acknowledgment. In addition, the system shall allow Alarm Conditions to be configured as “log-only” events.

H. The system shall provide a visual indication of all unacknowledged Alarm Conditions at System Operator-designated Operator Workstations.

I. System shall provide the capability for System Operator to designate, for each Alarm Condition, Operator Workstations as either “Primary” or “Secondary”, as configured by System Operator. The system shall provide the capability to direct Alarm Conditions only to Primary Operator Workstations. In the event that an Alarm Condition is unacknowledged at Primary Operator Workstations for longer than a System Operator-specified period (from 1 to 300 seconds), Alarm Condition shall automatically report to Secondary Operator Workstations.

J. System shall allow all Alarm Conditions intended for Primary Operator Workstation to be immediately redirected to Secondary Operator Workstation during System Operator-specified time periods, as determined by Time Code.

1.25 ACTIVATION OF OUTPUT CONTACTS UPON ALARMS

A. All Alarm Conditions, including Door Forced conditions and Open-Too-Long conditions, shall be capable of activating one or more Auxiliary Contact Outputs to enable the operation of audible sounders, door alarm horns, and other such devices.

B. System shall permit the “global” relationship of Alarm Conditions to Auxiliary Output Contacts, where conditions occurring at one Intelligent Controller shall be capable of causing outputs to occur at any Intelligent Controller in the system.

C. The system shall allow System Operator to define how each output will operate during each Alarm Condition. As a minimum, the system shall permit the following operating conditions:

1. Output tracks Alarm Condition: Output activates when Alarm Condition is active and deactivates when Alarm Condition clears.
2. Output tracks acknowledgment: Output activates when Alarm Condition is active and deactivates when Alarm Condition is acknowledged by System Operator, even if Alarm Condition has not yet cleared.
3. Timed output: Output activates when Alarm Condition is active and deactivates when Alarm Condition has cleared or after a preset time period, whichever occurs first. Time shall be definable by System Operator for a period of between 1 and 300 seconds.

1.26 EMAIL MESSAGING UPON ALARM CONDITION

A. System shall provide the ability to automatically send email and text messages to designated recipients upon Alarm Conditions. The system shall utilize standard MAPI email and authenticated SMTP protocols to permit transmission to any valid Internet email address or phone number.

B. Email and text message to be sent shall be System-Operator definable for each Alarm Condition and shall consist of up to 256 text characters per message. Texting and email must use industry standard interfaces to permit the use of a 3rd party to process the texts or email.

C. Email messages and text shall be capable of being sent to email Address Groups and text groups based on Time Code. Address Groups and text groups shall be capable of containing not less than five separate email or text addresses. Each Alarm Condition shall permit a minimum of three Time Code/Address/Text Group combinations.

1.27 SOUND EFFECTS UPON ALARM CONDITION

A. System shall provide the ability to automatically play audio messages on designated Operator Workstations upon Alarm Condition. The system shall allow the attachment of separate audio files to each Alarm Condition. Audio files shall be standard .WAV format audio files.

1.28 TRACE FEATURE

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

1.29 SYSTEM REPORTING AND LOGGING FEATURES:

A. The system shall provide an electronic log of events, recorded on a real-time basis as they occur. Events shall be recorded with date and time. The automatic log of events shall be defined as the “System Journal.” The system shall also support the routing of all or a subset of log events via an industry standard interface to the State’s utilized SIEM platform.

B. When Intelligent Controllers are in an “online” (in communication with the SMS host computer) status condition, System Journal events shall be immediately sent to the SMS host computer and stored on a hard disk. In order to preserve journal information in the event of a system failure, journal entries shall be written to disk immediately, without the “buffering” of more than one entry at a time.

C. When Intelligent Controllers are in an “off-line” (not in communication to SMS host computer) status, Intelligent Controllers shall store (“buffer”) System Journal events in memory. Each Intelligent Controller shall be capable of storing a minimum of five thousand (5000) Journal Events in memory.

D. In addition to being stored, System Journal events shall also have the capability to be immediately displayed at designated Operator Workstations and designated printers, providing real-time reporting of all system events.

E. The system shall support standard network printing facilities to allow the use of any printer connected to the State network. The use of specific printers for specific types of reports shall not be required.

F. The system shall allow System Journal events to be selectively reported to Operator Workstations and Printers, providing the ability to direct certain System Operator-specified types of events to certain Operator Workstations and printers on a real-time basis. At a minimum, the system shall allow the selective reporting of the following events: Alarm Condition, Monitor Point activity, Forced Door, Open-Too-Long, Invalid Access Attempt, Passback Violation, Trace, Hardware Failure, Communication Failure, Tamper, and Power Fail.

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

H. All card access activity shall be logged into System Journal. For Valid Access, Invalid Access Attempt, and Trace conditions, the System Journal shall be capable of logging the following information as a minimum: Door name and number; card number; and cardholder name (If truncated, it shall be 12 characters minimum). For Invalid Access Attempts, System Journal shall also log the reason for rejection. for Trace, System Journal shall also log Trace.

I. System Journal shall log all Monitor Point and Alarm Condition activity.

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

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

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

M. All System Operator configuration activity, such as modification to Clearance Codes, Time Codes, Monitor Points, Cardholder Records, and other system data, shall be recorded to System Journal. At a minimum, the log of configuration sessions shall identify the data type that was modified and identify the System Operator who modified it.

N. System shall be capable of selectively displaying all system configuration data on the Operator Workstation screen, allowing the viewing of Cardholder Records, Clearance Codes, Doors, Time Intervals, Time Codes, Monitor Points, Door Groups, Alarm Groups, and other configuration data. The system shall provide the ability for the System Operator to selectively view specific types and numerical ranges of data.

O. System shall be capable of printing all system configuration data to a printer, allowing print-out of Cardholder Records, Clearance Codes, Doors, Time Intervals, Time Codes, Monitor Points, Door Groups, Alarm Groups, and other configuration data. The system shall provide the ability for the System Operator to selectively print specific types and numerical ranges of data.

P. System shall be capable of logging all updates, changes, and deletions of data related to access cards and card holders to include at least the operator who made the change, the date and time of the change, and the workstation from which the change was made.

1.30 ARCHIVAL STORAGE AND BACKUP FEATURES

A. The system shall provide the capability to backup and copy all system and database files, including cardholder database, to any industry standard output devices including NFS or SMB version 2 or 3, Azure Blob. The system shall provide a menu-driven backup and restore capability, with operator prompts, enabling backups and restores to be made from the security management system application program. Backup capability shall be available from the regular system menu, and making backups shall not interrupt system operation or require restarting of the SMS host computer. Additionally backups should be able to be scheduled to occur at regular intervals at the discretion of the end user.

B. System shall be capable of storing a minimum of five million System Journal events. The system shall provide for the archival transfer of event data between storage locations and devices. The archival transfer shall load event data to selected devices and clear event data from the online System Journal file after verifying good archive copy. The system shall provide a menu-driven utility to allow an archival transfer.

C. The System shall support the use of an industry-standard external file backup and recovery system for all data, tables, and files.

D. The system must be able to support database-level backup and point-in-time restore capabilities.

1.31 DATABASE RETRIEVAL FEATURE

A. System shall provide an integrated database retrieval system for the System Journal. Database retrieval system shall provide search and retrieval capabilities to allow selective reporting of past System Journal events from storage.

B. System shall provide basic search tools to allow selective retrieval of events according to criteria established by the System Operator. At a minimum, search tools shall allow selective recall of events by type, time frame, location, cardholder name, and card number. Basic search tools shall be usable by non-technical people who have received minimal training. Basic searches shall not require knowledge of any programming or query language.

C. In addition to basic search tools, the database retrieval system shall allow Structured Query Language (SQL) to conduct more advanced searches. The SQL used shall be an industry-standard type that is in common use, with Microsoft SQL preferred.

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

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

1.32 PHOTO IDENTIFICATION BADGE SYSTEM

A. The system shall provide photo identification badge capabilities allowing the design, production, and management of photo identification badges for State employees and vendors. The photo identification badge system within this specification shall be defined as the “badging system.”

B. Badging system shall be integrated with the SMS. Badging systems, which are software modules seamlessly integrated within the SMS software application program, are preferred over badging systems that must be used as a separate program. Badging system software must operate on the SMS host computer and use SMS Operator Terminals for badge production and verification. Badging systems requiring separate computers for badging system servers, or badge production and verification workstations are not acceptable.

C. Badging system shall store photo images and other badge information within the same database as Cardholder Record.

D. Badging system shall provide full-featured badge design and production capabilities. The badging system shall permit the State to create an unlimited number of badge designs and store them as reusable badge templates. Systems requiring that the manufacturer create or modify badge templates are unacceptable.

E. As a minimum, the badging system editor shall:

1. Permit badge layouts to be designed with either vertical or horizontal badge orientation.
2. Permit insertion, sizing, and placement of photo images on badge layout.
3. Permit insertion, sizing, and placement of text boxes within badge layout. Two types of text boxes shall be available: field text boxes that insert variable text from a selected field within the Cardholder Record and label text boxes that produce fixed text.
4. Permit the use of any standard Windows TrueType font in point sizes between 4 and 48 points. The text shall be capable of being formatted as normal, bold, italic, and bold italic.
5. Permit the use of both uppercase and lowercase text characters within a text box.
6. Permit both vertical and horizontal text on a badge, irrespective of badge orientation.

7. Provide text justification within text boxes. Types of justification shall include proper justification, left justification, and centered.
8. Permit text boxes to be defined for “scale-to-fit” formatting, where text size is automatically adjusted to accommodate available space within the text box.
9. Permit use of standard Windows colors for text, text box background, badge background, photo background, signature, signature background, and borders.
10. Permit the import, sizing, and placement of graphic images (such as logos) on the badges. Shall accept images in standard graphics formats such as .JPG, .BMP, .GIF, etc.
11. Provide tools for alignment and positioning of elements on badge layout. Tools shall include adjustable grids with an “align to grid” feature.

F. Badging system shall permit the use of signatures on badges. The badging system shall permit the capture of signatures using any electronic signature pad which utilizes standard Windows device drivers.

G. Badging system shall permit the use of any badge printer that utilizes standard Windows printer drivers. If supported by the printer, the badging system shall permit full-color, double-sided printing and laminating. The badging system shall permit edge-to-edge printing on the card if supported by the printer.

H. Badging system shall permit the capture of color photographic images from any of the following sources:

1. Direct video source, such as a live video camera, connected to a video capture board installed in a workstation.
2. Scanned image from any standard TWAIN-compliant scanner supported by Windows.
3. Image file in standard .JPG format from a digital camera or another source.

I. Badging system shall provide the ability to process color photographic images after they have been captured or imported into the system. As a minimum, image processing capabilities shall include the ability to adjust intensity/brightness, contrast, hue, and saturation.

J. Badging system shall provide a “print-preview” feature which allows badges to be viewed in a “what-you-see-is-what-you-get” (WYSIWYG) mode before being printed.

1.33 QUICK LOOK-UP FEATURE

A. The system shall provide a method to quickly display the cardholder record and photo image for any cardholder based on the cardholder's name. This feature shall be available to authorized operators at any Operator Workstation.

1.34 AUTOMATIC DISPLAY OF PHOTO IMAGE

A. The system shall allow the automatic display of the cardholder’s photo image on designated Operator Workstations when valid accesses or invalid access attempts are made at designated card readers.

1.35 INTELLIGENT CONTROLLER

A. Intelligent Controller shall be a field panel that provides local processing and control of all access control, alarm monitoring, and auxiliary control functions. Intelligent Controllers shall typically be located within equipment closets throughout the State.

B. Intelligent Controller shall provide full-featured card access control processing without requiring communication with the SMS host computer. All data necessary for card processing shall be stored within the memory of the Intelligent Controller. Communication with the SMS host computer shall not be required to process card access requests under normal conditions.

C. Intelligent Controller operating system, firmware, application program, and database shall be stored in solid-state memory media that is encrypted. The intelligent Controller shall not use any type of disk drive (hard drive) to support normal operations.

D. The application software used by the Intelligent Controller (often known as “firmware”) shall be field-upgradeable to permit system enhancements to be made as they become available from the manufacturer. Intelligent Controllers that utilize “Flash ROM,” which permits upgrades to be made automatically by download from the SMS host computer, are preferred over Intelligent Controllers that require manual field visits.

E. Intelligent Controllers shall be equipped with an integrated real-time clock. Intelligent Controllers shall be capable of processing timed-control functions (such as automatic unlock) without requiring communication with the SMS host computer.

F. Intelligent Controllers shall be capable of processing local alarm input/output events (such as the operation of a local audible alarm horn when Monitor Point is activated) without requiring communication with the SMS host computer.

G. The system shall be capable of communicating between Intelligent Controllers and the SMS host computer using the following methods:

1. Over the State’s existing Ethernet IPv4 network, with optional support for IPv6 or dual stack IPv4/IPv6. A native implementation of Ethernet, where the Intelligent Controller is directly connected to the Ethernet, is preferred. The use of external terminal servers to interconnect Intelligent Controllers with the SMS host computer is less desirable but also acceptable.
2. Through the dial-up, switched telephone network. Dial-up operation shall support the use of Intelligent Controllers at remote State buildings where network service is unavailable.

H. Each Intelligent Controller shall provide the capacity to control a minimum of eight (8) Doors. Each Door shall be configured with one card reader input, one SPDT (Form C) lock output, one door switch input for Open-Too-Long and Door-Forced-Open monitoring, and one Request-To-Exit input.

I. Intelligent Controller shall provide a memory capacity for no less than ten thousand (10,000) access cards.

J. In the event that card data is not contained within the Intelligent Controller's local memory, Intelligent Controller shall immediately transmit card data to the SMS host computer for processing and validation at the SMS host computer level. Intelligent Controller shall permit access of cards not in local memory upon validation of access request by the SMS host computer.

K. Intelligent Controller shall rapidly process all access control transactions. The time between the presentation of a valid card at the card reader until the time that door unlocks shall not exceed 1 second under worst-case conditions.

L. Intelligent Controller shall provide auxiliary monitor point inputs and auxiliary relay contact outputs. Inputs and outputs shall be provided directly by the Intelligent Controller or through the use of accessory modules. In addition to those inputs and outputs directly associated with access-controlled doors, each Intelligent Controller shall provide no less than thirty-two (32) auxiliary monitor point inputs and no less than twenty-four (24) auxiliary relay contact outputs.

M. Intelligent Controller shall utilize a standard Wiegand and OSDP protocol to interface Intelligent Controller to card readers, permitting multiple types of card readers and other input devices. Intelligent Controllers that rely exclusively on a "proprietary" card reader protocol that requires the use of any specific manufacturer's card reader or input device shall not be used.

N. Intelligent Controllers that accept Wiegand and OSDP inputs directly are preferred over Intelligent Controllers that require the use of an adapter to convert the Wiegand and OSDP input to the manufacturer’s proprietary format.

O. Intelligent Controller shall support the use of Wiegand formats of varying bit lengths from 26-bit to 55-bit. The Intelligent Controller shall permit the intermixing of Wiegand formats with a single Intelligent Controller. The Intelligent Controller shall also allow each card reader to accept multiple Wiegand formats.

P. Intelligent Controllers that utilize a “bus” architecture for connecting field devices (card readers, inputs, and outputs) are preferred over Intelligent Controllers, which require that field devices be connected exclusively to the Intelligent Controller itself. A bus architecture shall be defined as an architecture that permits card readers, inputs, and outputs to be connected through accessory modules to a single data circuit (“bus”) that is distributed through the building.

Q. Intelligent Controller shall be provided with a power supply with a standby battery. The battery shall be sized to provide a minimum of eight hours of full standby operation in the event of primary power failure. The Intelligent Controller shall report a loss of primary AC power to the SMS host computer within 10 minutes of power failure. The power supply shall be Underwriters Laboratories (UL) listed. The power supply may be integral to Intelligent Controller or furnished within a separate enclosure.

The Intelligent Controller shall monitor battery power levels and outages, and while standby batteries must be in a lockable frame, they must also be relatively easy to replace by State personnel as needed.

R. When Intelligent Controllers communicate with the system SMS host computer, all operator programming for Intelligent Controllers shall be immediately downloaded from the SMS host computer, and all events shall be immediately communicated (uploaded) to the SMS host computer.

S. In the event of a communications failure to the SMS host computer, Intelligent Controller shall store access control and alarm monitoring transactions in a memory buffer. The minimum size of the memory buffer shall be five thousand (5000) transactions. When communication is restored, Intelligent Controller shall automatically upload the stored transactions to the SMS host computer.

T. Intelligent Controller shall be designed in a manner that makes efficient use of space. Intelligent Controllers that are compact and provide a maximum number of inputs and outputs within the smallest amount of wall space are preferred.

U. In addition to the standard Intelligent Controller described herein, the system shall provide a "Compact Intelligent Controller.” The Compact Intelligent Controller shall have all the capabilities of a standard Intelligent Controller but will have reduced capacities. The Compact Intelligent Controller will be used at locations where less system capacity and/or a more economical controller is needed. The minimum capacities of the Compact Intelligent Controller shall be two (2) Doors, each configured with one card reader input, one SPDT (Form C) lock output, one door switch input for Open-Too-Long and Door-Forced-Open monitoring, and one Request-To-Exit input; four (4) auxiliary monitor point inputs, four (4) auxiliary relay contact outputs; and memory capacity for not less than five thousand (5,000) access cards.