PART 1 - DIVISION 28 – ELECTRONIC SAFETY AND SECURITY

PART 2 - SECTION 28 13 00

PART 3 - ACCESS CONTROL

PART 1 - GENERAL

1.01 SECTION INCLUDES

A. Head-end Hardware and Software

B. Software Only (owner-provided head-end CPU hardware)

C. Field Panels

D. Cards & Readers

E. Electric Locks

F. Request-to-Exit Devices

G. Wiring

1.02 PRODUCTS SUPPLIED BUT NOT INSTALLED UNDER THIS SECTION **[DELETE IF NOT APPLICABLE]**

1.03 PRODUCTS INSTALLED BUT NOT SUPPLIED UNDER THIS SECTION **[DELETE IF NOT APPLICABLE]**

1.04 RELATED SECTIONS **[CHOOSE AS RELATED TO YOUR PROJECT]**

A. 28 13 43 Identification Management Systems

B. 28 16 00 Intrusion Detection

C. 28 23 00 Video Surveillance

D. 28 31 00 Fire Detection and Alarm

E. 27 50 00 Intercommunications Systems

1.05 SUMMARY

A. Labor and Materials: Unless otherwise noted in the Drawings and Specifications, the Contractor shall provide and pay for all labor, materials, equipment, tools, utilities, construction equipment and machinery, transportation and other facilities and services necessary for the proper execution, operation and completion of the Work.

B. Specification Language: Specifications and notes are written in imperative and abbreviated form. Imperative language of the technical specifications is directed at the Contractor, unless specifically noted otherwise. Incomplete sentences shall be completed by inserting “shall”, “shall be”, “the Contractor shall”, and similar mandatory phrases by inference. The words “shall be” is supplied by inference where a colon (:) is used within product specifications.

C. Drawings and Specifications:

1. Contractor shall be provided three (3) sets of the Drawings and Specifications for his use. Additional sets, if requested by Contractor, shall be furnished to the Contractor for the actual cost of reproduction.
2. Contractor shall carefully study the Drawings and Specifications, and shall at once report any error, unforeseen circumstances, inconsistency or omission upon discovery.
3. The **[CLIENT]** Project Manager shall be the interpreter of the requirements of the Drawings and Specifications, subject to the final approval of **[CLIENT]**.

D. Intent and Correlation:

1. The intent of the Project Drawings and Specifications is to include all items necessary for the proper execution and completion of the Work.
2. The Project Drawings and Specifications are complementary, and what is required by any one shall be as binding as if required by both.

1.06 REFERENCES

A. Submit the project and customer information of customers for at least three other projects of similar size and complexity using similar technologies.

1. Shall include a minimum of the following:

a. Customer Name
b. Customer Point of Contact
c. Customer Point of Contact Phone Number and email address
d. Address of project
e. Title of Project
f. Type of project completed

1.07 DEFINITIONS

A. Industry standard words and phrases are used throughout the Drawings and Specifications, except:

1. Words which have well-known technical or trade meanings are used in accordance with such recognized meanings.
2. Whenever the following listed words and phrases are used, they shall be mutually understood to have the following respective meanings:

B. The words “as indicated.” means: as shown on the Drawings, and in accordance with the Specifications.

C. The words “as required.” means: as required to provide a complete and satisfactory Work in full conformance with the Drawings and Specifications.

D. The word “New” means: new Work to be provided by Contractor.

E. The word “Provide” means: furnish, install, connect, test and make ready for use.

F. The words “Relocate existing” means: remove existing item from present location. Reinstall, re-connect, and test existing item and make ready for use at new location as shown on the Drawings.

G. The words “Remove existing “ means: remove existing item and return item to **[CLIENT].**

H. The word “Replace” means: remove existing item and return item to **[CLIENT]**. Provide new item as indicated.

I. The word “Work”: The Work is the completed construction required by the Drawings and Specifications, and includes all labor necessary to produce such construction, and all materials and equipment incorporated or to be incorporated in such construction.

J. The word “Furnish” means: supply item as specified. Item to be installed by others.

1.08 CONTRACTOR DESIGN REQUIREMENTS

A. The Project Drawings represent the level of system design to be provided by **[CLIENT]**. Contractor shall provide all additional system design work required, including:

1. Conduit layout and sizing.
2. Wire and cable layout and sizing.
3. Point-to-point wiring and equipment hook-up information.
4. Equipment mounting details.
5. Design of equipment cabinets.
6. Other detailed design work required.

B. Contractor’s design shall conform to all applicable codes and ordinances. All electrical design, including the sizing and placement of conduit, raceways and conductors, shall be in accordance with NFPA 70: National Electrical Code, current version, unless local codes establish more stringent requirements.

C. Contractor’s design work is subject to review and approval by **[CLIENT]**’s Project Manager.

D. Contractor’s design shall also include:

1. The addition of all wire, cable, conduit, connectors and junction boxes required for system operation.
2. The installation of conduit between the control components and all equipment at each door, as necessary.
3. Completed “as-built” documentation of all security systems, including documentation of existing equipment, wiring, conduits, and raceways.
4. Other Work as defined within the Project Drawings and Specifications.

1.09 SYSTEM USER REQUIREMENTS

A. System Overview:

1. The contractor shall provide and install a new integrated security system. The new system shall be able to provide Access Control, Identity Management, Alarm Management, Video Management, Visitor Management and other functionality in a single fully integrated Security Management System
2. The Security Management System shall have a simple, consistent and easy-to-use graphical user interface.
3. The manufacturer of the proposed system shall have produced access control products for at least 20 years and shall be ISO 9001 certified.
4. All SaaS products provided by the manufacturer must be hosted in a SOC 2 certified environment, no exceptions.
5. The manufacturer shall be ISO27001 certified.
6. The manufacturer shall be ISO 140001 certified indicating their commitment to conserve energy and reduce waste.
7. The Security Management System shall operate using a Microsoft SQL Server database and shall support Microsoft SQL Server 2016-64 bit, 2017-64 bit, 2019-64 bit, 2022-64 bit.
8. The Security Management System shall be developed using the Microsoft Visual Studio development environment
9. The System shall support virtualization certified to work on VMWare and Hyper-V
10. The System shall support both Microsoft Clustering and NEC Clustering software for resilience
11. The system shall carry FIPS-140-2 certification of appropriate parts of its communication encryption infrastructure, and the manufacturer shall provide the NIST certificate number confirming certification. Systems that do not carry FIPS-140-2 certification shall not be acceptable.
12. The manufacturer shall supply, immediately upon request, a VPAT statement showing support for Section 508.
13. The manufacturer of the proposed system shall require resellers to pass a formal training program prior to being certified as authorized to sell and install the system. Such certification shall require annual re-qualification. The system integrator proposing the system shall be in possession of such a certification.
14. The Security Management System client and server software shall be used in conjunction with intelligent controllers to provide a distributed access control and alarms monitoring system. In the event of a communications failure between the host server and the field controllers, the controllers shall continue to make local access control decisions and save all transactions in memory until communications are restored. At that time the controller shall upload all stored transactions to the server.

15. The Security Management System shall seamlessly integrate the functions of access control, alarms monitoring and response, video management, badge design/creation, identity management and visitor management. Licenses for all of these items (except for licenses for individual cameras) shall be included as part of the base price of the proposal, and not as extra-cost options.
16. All Security Management System user interface components shall run in an integrated application environment as part of a single application executable. Systems which provide their user interface through multiple separate applications programs shall not be acceptable, except as specifically indicated below.
17. Language packages in at least 3 languages shall be available at no extra charge.

B. Required Access Control Hardware Features

1. The Security Management System will provide the option of using either conventional modular door controllers which enable between 2 and 16 doors to be housed within one steel enclosure or alternatively using Edge Network Controllers supporting PoE+.
2. The Security Management System intelligent database controller shall support a minimum of 20,000 cardholders with expansion capabilities of up to 1,000,000 cardholders.
3. The Security Management System intelligent database controller shall support a minimum of 12,000 offline transactions. The option to provide for at least 65,000 transaction storage at the panel must be available.
4. The Security Management System hardware shall be comprised of modular components that connect over standard interfaces to one another. There shall be database storage and processing module (DBU), and once data has been downloaded to the DBU it shall locally make access control decisions. Access granted or denied decisions shall be made in under 0.5 seconds.
5. The DBU shall store firmware in non-volatile flash memory to allow for convenient updates through a firmware update application. The DBU shall store the cardholder and configuration database information in battery-backed memory so that loss of primary power will not cause the loss of the database.
6. The Security Management System hardware shall be capable of expansion via 4-, and 8-door controllers. Door controllers shall support one or more input/output module expansion cards that require no additional addressing and provide 8 monitored input points or 8 auxiliary output points.
7. The DBU shall support configurations that include: 16 card readers, 96 monitored input points, or 96 auxiliary output points.
8. There shall be an intelligent controller option to provide control of 8 readers/doors from a single circuit board (communications, memory, CPU, and reader/door functions integrated) with an available 8-reader/door add-on to provide a 16-door controller from two circuit boards. The 8-door controller shall provide an integrated on-board RS-232 interface, and shall have provisions for modular expandable memory.
9. System must support the installation of card readers at any distance up to 3000 feet from the reader interface board. Systems that do not support this requirement, or that require additional, separately mounted components to achieve the requirement shall not be acceptable. This requirement does not apply to biometric reader devices or Wiegand readers.
10. Each supplied card reader shall be continuously monitored for tamper (reader removed from backing plate or reader removed from wall). Tamper detection switch must be part

of the reader and fit entirely within the reader housing. Use of external tamper switches shall not be acceptable. This requirement does not apply to biometric reader devices.

11. When using the vendor's proprietary card readers, each supplied reader shall be actively and continuously monitored for communications loss by the Security Management System hardware. This monitoring shall consist of a two-way Poll-Response mechanism that insures the integrity of all signaling including LED and LCD (if equipped) data paths. Systems utilizing uni-directional "heartbeats" or not including active, continuous monitoring of reader communications shall not be acceptable. This requirement does not apply to biometric reader devices or Wiegand card readers.
12. When using the vendor's proprietary card readers, the Security Management System shall optionally annunciate door forced and held conditions using the reader's onboard sounder, Systems that do not offer this behavior, or that require additional wiring, use additional relay outputs, or require external sounders to accomplish it shall not be acceptable. This requirement does not apply to biometric reader devices or retained legacy readers.
13. The hardware shall be made with a lead-free manufacturing process to meet RoHS requirements.
14. Communication Schemes

    a. Network Communications

        i Field panels shall have the ability to communicate with its server or (for very large systems) its communications PC over the local or wide area network. This shall be achieved by the addition of a network interface option module (except in the case of controllers with a pre-installed network interface card [NIC]). The network interface shall support a minimum of "100 base TX" communications speed.
        ii The network interface shall support encryption utilizing AES 128 or AES 256 algorithms.
        iii Field panel models should be available to allow chains of connected panels to be created where the first panel is directly connected to the network and a minimum of 30 additional intelligent field panels daisy-chained together such that they communicate back to the single network interface.
        iv An optional modem and telephone line shall be configured to provide an alternative path for the reporting of alarms in the event of unavailability of the network. The fallback to dial-up alarms reporting shall be automatic in the event of detecting a network communications failure.

    b. Hardwired Communications

        i The field panels shall be located convenient to the access and monitor points that they control and shall be interconnected in a chain configuration to the server or a serial port of a convenient communications PC on the system.
        ii The system shall support a minimum of 31 intelligent field panels daisy-chained together such that they communicate back

to a single serial communications port at the server / communications PC.

c. Bi-Directional Communications

i A chain of field panels shall be wired in a loop configuration, by the addition of a cable from the last controller and connecting it into a second port on the PC. When this configuration is installed, should a break in the cable occur, the PC shall be able to communicate with the nodes after the break, via the secondary port. This requirement does not apply to retrofit controllers.

d. Dial-Up Communications

i Remote sites with field panels shall also have the ability to be centrally administered and monitored using low-cost dial-up connections via autodial/auto-answer modems with each site storing all access activity for up-loading during periodic calls to update the central history log. Should an alarm occur, the remote site shall immediately call and report the incident.

e. Secondary Dial-In Alarms

i Installations involving large quantities of remote dial-up sites shall have the ability to be configured with a secondary port, which is dedicated to receiving any alarms from the remote sites. This feature shall ensure that alarms can still be received even if the primary line is busy, for example, if card administration updates are occupying this telephone line.

15. Efficient Memory Management

a. Other than Edge Network controllers, DBU Controllers shall be capable of supporting cardholder populations of at least 200,000 cards when equipped with sufficient memory or be configured to a learning mode that allows the cards most frequently used to have their access rights stored locally in the panel's memory.
b. The system will include a "learn mode" function. When a card is presented which is not resident in the local panel, a verification request shall be made to the central database, if the card is valid the details shall be downloaded. If the card memory is full, the card with the oldest transaction date shall be deleted to make space for the card requested. This shall allow automatic management of cardholders, based upon frequent users having "instant" response and infrequent users learned when required.

16. Elevator Control

a. The system shall have the ability to provide elevator access control by (1) using a card reader to activate the elevator call button, (2) using a card reader in the cab to activate the correct floor selection button, or (3) a combination of both of these functions. The system shall have special field panels specifically designed to handle inputs and outputs used to interface with the elevator controls.

b. The panels specifically designed for elevator control shall support either a single elevator cab for up to 64 floors, or up to 4 elevator cabs for up to 16 floors each.
c. Each cardholder shall then have floor permissions assigned as part of the normal access rights. The system shall provide outputs to the elevator controls to verify which floors are authorized for each cardholder. The system shall be capable of tracking which floor was enabled/selected by that person.

17. Elevator Destination Dispatch

a. The system shall provide a two-way TCP/IP based software interface between the Security Management System and the Destination Dispatch elevator system.
b. The system must accommodate one or more computers driven kiosks as each elevator landing lobby connected to a computer-based elevator controller.
c. The system must display a free or secure status icon for each landing served.
d. The system must direct the passenger to the appropriate elevator car that was dispatched based on passenger's permission level.

18. Database Synchronization

a. To ensure synchronization of the distributed controllers' databases with a region's main database an internal checking process shall be provided within each controller. In the event of corruption of a controller's local database then it shall be able to detect this condition and automatically request the relevant data to be downloaded from its local server. This action shall not require Operator intervention.
b. The system shall continue to provide access control functionality during this re-synchronization process.

19. Door lock release relays shall be minimally rated for 3 A @ 30 VDC for non-retrofit controllers, 2A@30VDC for retrofit controllers.
20. Readers supporting various technologies shall provide data from card presentations or biometric authentications through a door control unit (DC) that includes the electrical interface to the reader as well as inputs for door sensors and form C relays for outputs.
21. The DC shall support Wiegand communications to the reader. In order to provide higher levels of security, the DC shall also support bi-directional, supervised communications to the reader. Door controllers that do not support encryption and supervision of reader communications are not considered equal.
22. The system shall support an option to store cardholder biometric hand geometry templates at the panel (as part of the cardholder record). Storage of the hand geometry template data at the reader shall be unacceptable. This requirement does not apply to edge network or retrofit controllers.
23. The Security Management System hardware (except retrofit controllers and connected legacy devices) shall support all of the following options for supervision of the monitored input points:

a. 2-state supervision – in which only secured and alarm state are indicated.
b. 3-state supervision – in which the input state can be secure, alarm or open circuit.
c. 4-state supervision – supports secure, alarm, short circuit and open circuit states.
d. 6-state supervision – supports secure, alarm, short or open circuit for the sensor in addition to tamper alarm and tamper short circuit states.

24. The system shall provide the option to install Edge Network Door Controllers which support either one or two doors using PoE+ (Power over Ethernet Plus).

    a. The intelligent PoE+ edge network controller shall provide access control processing, host functionality and 12VDC power for one or two doors (when connected to a PoE+ network port supplying maximum 802.3at power, including reader, lock, door status, request-to-exit device and auxiliary sounder).
    b. Each intelligent controller shall be powered using PoE, PoE+, or locally via a 12VDC supply. When powered using PoE, up to 700mA should be available for reader and electric lock power. When powered using PoE+, up to 1.5A should be available for reader and electric lock power.
    c. The network door controller shall provide full distributed processing of all access control functions. Each controller shall provide distributed intelligence and fast response to access requests including a minimum memory capacity of 90,000 cardholders and 18,000 offline event transactions.
    d. The controller shall support Flash Memory firmware infrastructure for ease of updating.
    e. The controller shall support Wiegand output card readers and MCLP protocol for reader communications.
    f. The controller shall provide four (4) auxiliary inputs for connection of dry-contact monitored devices. These inputs shall offer the option of 2, 4, or 6 state supervision.
    g. The controller shall provide two (2) auxiliary relay outputs for connection of external devices.
    h. The network door controller shall be capable of employing 256 bit Advanced Encryption Standard (AES) for all communications between the controller and host(s) system(s).
    i. The Edge Network Controller shall provide onboard connections to a client PC via the Local or Wide Area Network.
    j. The Edge Network Controller shall provide SNMP protocol monitoring.
    k. The Security Management System shall provide direct network discovery and programming for the Edge Network Controller for simplified installation.
    l. The controller shall be UL listed and conform to UL294 standards for access control systems.

25. Wireless Locks

    a. The system shall provide for the connection of Assa Abloy “Aperio” locks via the connection of one or more Aperio Serial hubs. Systems only supporting Aperio Wiegand hubs shall not be acceptable.

        i Aperio hubs shall be connected to a database unit that holds a local copy of the access rights for 16 doors. The database unit must be capable of granting access and recording activity even when disconnected from the host. Systems not offering this capability shall not be acceptable
        ii The system shall support Aperio “office mode”. Systems not offering this capability shall not be acceptable.

    b. The system shall provide for the connection of Assa Abloy WiFi wireless locks through the addition of the relevant software license

c. The system shall provide for the connection of Allegion AD-400, and NDE style locks

d. The system shall provide for the connection of Salto family locks

26. Enclosures and Power Supplies

a. All electronic circuits supplied, with the exception of the Edge Network Controllers, retrofit controller, or those which are PoE powered or within a client or server or recorder PC, shall be mounted on standoffs inside the manufacturer-supplied enclosures. All such enclosures must include a key lock on a removable hinged door, and must include a tamper switch to detect when the door is opened. Systems without key locking of enclosure doors or without doors which are both hinged and removable shall not be acceptable.
b. All electronic circuits supplied for the access control system, except those which are PoE powered, are components of the retrofit controller, or are within a client or server or recorder PC, shall be powered by 18-20VAC through supplied 120VAC to 20VAC molded case, fully insulated isolating transformers. The transformer shall be mountable inside the supplied enclosure or separately. Systems which require 120VAC power to be brought directly to the enclosure shall not be acceptable.
c. All electronic circuits supplied for the access control system, can use either Life Safety Power, or Altronix pre-configured enclosure types.

C. High Availability and Disaster Recovery

1. The Security Management System shall support a variety of High Availability (HA) and Disaster Recovery (DR) solutions including:

a. Fault tolerant servers for 99.999% rated availability
b. Microsoft clustered server support for 99.99% rated availability
c. Remote redundancy through backup servers of general purpose nature or as in 1.09C.1.a and 1.09C.1.b synchronized through software monitoring the operation of the paired server.

2. To provide greater client software availability, software shall be installed so that in the event of a database server failure, client machines will quickly and without operator intervention, automatically connect to a standby server machine.
3. The Security Management System product shall be capable of supporting options for 99.99% and 99.999% availability.
4. The Security Management System product shall support a disaster recovery solution using off-site database replication.

D. Encryption

1. Encryption falls into two distinct areas, firstly between clients and their Server, secondly between client and local area network panels (LAN Nodes). LAN node links shall support AES 128 and AES 256 bit encryption between the supervising client PC and its LAN Chains.
2. For client to server connections, the Security Management System shall support a solution using industry standard network cards supporting IPSec and 3DES encryption.
3. Web-based (thin client) Security Management System clients shall support SSL encryption.

E. Required Standard Software Features - The following software features shall be part of the standard product offering without requiring additional purchase or licensing:

1. The installation of the server and client software shall utilize a “wizard” interface to guide users through the appropriate installation steps.
2. The server and client software shall utilize a software-based licensing scheme. Systems requiring hardware based keys or dongles shall not be acceptable.
3. The Security Management System shall utilize Microsoft .NET architecture.
4. The Security Management System shall start up as part of the Operating System. The Security Management System server shall communicate to all clients (operator workstations and field hardware) through Windows services. The Security Management System shall run as a service in the OS, and there shall be no requirement to run an application after the operating system is ready.
5. The Security Management System shall support a Graphical User Interface that minimizes training needs for even inexperienced users. The software shall include on line help displays to eliminate operator reference manuals.
6. The Security Management System software shall be run using standard x86-based hardware, and the operating system shall be Microsoft Windows as follows:

    a. The Security Management System server shall run on 64-bit Windows Server 2012 R2, 2016 or 2019 (Standard or Datacenter Edition).
    b. Security Management System server shall support operation in a VMware ESXi environment and a manufacturer-supplied manual describing virtualization support shall be provided.
    c. The Security Management System client software shall run on 64 bit Windows 8.1 Professional or Ultimate, Windows 10 Professional and Enterprise, Windows 11 Professional and Enterprise
7. The system shall allow other authorized applications to gain access to the system’s database should wider integration of the system at the site become a requirement.
8. It shall be possible to select any function, within a given Operators permission, independent of the currently displayed screen. Functions will be accessed via tool bar Icons, which will include Help prompts that will appear when the mouse pointer dwells on the selection button. It shall also be possible to link any standard Windows application to a custom toolbar icon.
9. The Security Management System shall support an unrestricted number of hours definitions. An hour definition is a description of the times during a 24-hour period during which a function will be active. The system shall support a minimum of 10 intervals per hour definition.
10. The system shall support an unrestricted number of time codes. A time code is defined as a set of hour definitions – one assigned to each day of the week (including Saturday and

Sunday) as appropriate and assigned to the various types of holidays (exceptions) defined in the system.

11. The system shall support a minimum of 9 holiday types. A holiday type shall be assignable to an unrestricted number of dates on the calendar.
12. Operator Permissions

    a. System operators shall be associated with a log in Name and Password. A system option will determine whether strong operator passwords will be used. The minimum definition of a strong password shall be a password that contains at least one upper case character, one lower case character, one numeral and one punctuation mark, with a minimum password length of six characters. Additionally, the password cannot contain any full word of the operator's username.
    b. The option to use a Secure Biometric or Smart card for system logon shall be provided. When used, this option will force the operator to present their Name, Password and Biometric or Smart card.
    c. The operator's account shall be role-based. The role is a permission profile. This will determine the functions that shall be available to that operator when logged on to the system. The system shall support an option to hide Personal Identification Numbers of cardholders when an operator is viewing a record.
    d. The system shall show each operator only features and options for which he or she is authorized. Features and options for which the operator does not have permission must be hidden. Systems that display functionality that is unavailable due to inadequate permissions shall not be acceptable, even if such functionality is disabled or "grayed out".
    e. Card record data entry shall be divided into operator permission areas, allowing separate permission categories to be assigned for the viewing of personal data, ID badge printing and access right management.
    f. The Security Management System shall support an unrestricted number of operator accounts and operator roles.
    g. For all operators, a means of re-arranging their Icon tool bar shall be provided to allow the most frequently used Icons to be repositioned by the operator.
    h. The system shall store operator preferences based on logon information. This feature shall allow an operator to work with their preferred configuration independent of which workstation they occupy.
    i. The system shall support an option to reset all window layouts to a pre-defined "Home Screen".

13. Video Badging

    a. The system shall incorporate video imaging as a fully integrated function within the SME to customize access control cards by printing an identity badge directly onto the card. The badge design and image capture capabilities shall combine with the latest technology card printers to allow the production of an ID badge pass for each card holder at the time of registration.
    b. For each cardholder both a facial image and a signature shall be able to be captured, or imported, and stored within the database as part of the card record. These images shall be captured from a supported USB webcam or standard CCTV camera connected to the computer, or imported if available as a bit map or JPEG file. The system shall use data compression techniques to ensure efficient use of the available

hard disk space to maximize the number of images that can be stored on the hard disk.

c. System shall provide the ability to crop the image (live capture or imported from JPG, BMP, or WMF) to the desired area maintaining the proper aspect ratio.

d. Additionally, a signature may be imported from a signature capture terminal connected to the system via an RS-232 com port or USB port of the client PC local to where the card is being issued.

14. Badge Design and Printing

a. A comprehensive integrated badge design facility shall be provided as a standard integrated feature of the single Security Management System software application, with no separate licenses or license fees required to activate the feature. The badge designer must allow an unrestricted number of custom badge layouts to be defined and then saved with a suitable description as a reference. This shall make full use of the card record details such as name, card number, inactive date as well as allowing personal data to be included in the badge design. Company logos shall be imported as bitmaps (BMP) or JPEG images to provide a personalized corporate appearance to the card.

b. All elements incorporated into the design shall be able to be rotated.

c. Badge design within the Security Management System shall contain either single-sided or double-sided designs. Each side of the card may also be designated as being blank, or magnetic stripe side, or smart chip side, to ensure the designer is aware of the available space where printing may be incorporated for each card combination. The badge designer function shall be capable of supporting portrait, landscape, standard and custom-sized card designs.

d. When creating a new card record a badge preview screen shall also be included that displays the specific card's details on the selected badge design to allow confirmation prior to requesting the badge to be printed.

e. Each new cardholder record shall have the option to be flagged for future printing. Cards flagged in this manner shall be easily recalled at a later stage and processed for output to the printer in a single action. Selecting multiple cards for bulk printing shall also allow each card to be printed either with its specific badge design, as defined within each card's record, or alternatively printed with a selected common badge design. Encoding of magnetic stripe cards shall also be included as part of the bulk printing process.

f. The Security Management System shall support any manufacturer's ID badge printer with a Microsoft Windows (depending on the workstation configuration) compatible printer driver.

g. The Security Management System shall incorporate the option to encode a magstripe or smart card during the print cycle. Applications that require on-site encoding can combine both actions in a single process. Encoding may only be supported on a limited set of printer models defined by the Security Management System manufacturer.

h. Each badge design shall include a default printer and validity period.

i. Badge Designs shall include the ability to add access rights to the badge design, so a cardholder issued with a specific badge design will automatically receive badge permissions related to that badge design.

j. The badge designer shall support the ability for objects (images, or other fields to be printed to the card) to be enabled or disabled by the presence of a specific label in the

cardholder record. For instance, a logo indicating a certain training would be printed only if the personal data field identified indicated such a certification for that cardholder. Solutions requiring a separate badge design for any change in badge graphical content shall not be acceptable.

15. Identity Verification

a. Identity verification shall include the ability to monitor up to 9 lanes, and each lane shall comprise a single-entry point.
b. There shall be up to three live video camera views available per lane on the same window to verify that each card offered is in fact being used by the person to whom it was issued. (for monitoring vehicles approaching and arriving at the entry point of each lane for example).
c. A method of granting access to the individual at each entry point with a single mouse click shall be provided.
d. Each lane shall automatically display the stored image for a card when used at a reader.
e. The operator shall be provided with a means to quickly search cardholder records by name to manually compare and verify basic card information.
f. Each lane shall provide configurable cardholder information to be displayed when a card is presented at the entry point reader (for example card expiry date and personal data)
g. This screen shall also be frozen and printed to provide a hard copy evidence of any abuse observed by the operator. For high security entry points, the system shall be configured to not grant access until the operator has verified the stored and live images are the same person, with the door release being controlled by the system operator.
h. This screen shall provide manual operation of pre-defined commands as a means of rapid response to events for each lane.
i. Intercom station call and answer functionality shall be provided for each lane.

16. Report Generation

a. Extensive history reporting shall be a standard integrated feature; and shall include the ability to review all system alarms, access control activity, and operator actions. These reports shall be made available for review via the operator's display screen, or to a printer, or to another disk media. Extensive sort parameters shall include by any of the "Personal Details" fields or Titles, for example by "Department", and only Names commencing with "SM*".
b. The system shall support generation of reports detailing the system operation. The following reports shall be available in the software:

i Cards on site
ii Hours on site
iii Cardholders with access to each door
iv Access rights of each cardholder
v System Configuration
vi Scheduled and Conditional Commands defined
vii System operator transaction history

c. It shall be possible to replay video clips associated with events by directly interacting with the report as published to the computer screen.
d. The system shall demonstrate the ability to export data, for example reports, to other standard office word processing packages such as Microsoft Word®.
e. The system shall provide system management reporting, including detailed listings for all the operator actions and the current cardholder database for output to the display screen, printer or disk media.
f. The system shall have the ability to save frequently used report configurations and associate them with a "Title". Such predefined reports shall be available from a list to simplify the report selection. It shall be possible to request these reports to run immediately or schedule them to occur at a specified date and time.
g. Scheduled reports shall additionally have the option to be automatically repeated by specifying the number of days and reporting period to be included, for example a weekly report of Alarms to run at 10:30 am each Monday and including the previous 7 days of Alarms.
h. The system shall allow custom reporting options by providing an interface to a commercially available 'off the shelf' reporting product, The interface shall present all database fields in a structured format, which does not require detailed knowledge of the database design and table relationships. SQL Views complete with a Data Dictionary of these views must be provided for custom reporting.
i. History Reporting

    i Extensive reporting shall be included to provide the ability to review all system alarms, access control activity and operator actions. These reports shall be available for review on the operator's display, to a printer, or to a file.
    ii Extensive sort parameters shall include any of the personal details fields of information such as by department, job title, vehicle registration, contractor company name or any other reference appropriate for each site.
    iii Frequently run report configurations shall be saved allowing them to be selected and run on demand, or scheduled to run automatically as required. When scheduled to run automatically this shall have the ability to be repeated.
    iv Total Hours Spent On-Site: This report shall provide a detailed audit of the arrival and departure times for cardholders and calculates the total time spent on site for the chosen reporting period. This report shall be filtered by any of the personal data fields of information associated with each cardholder.
    v Cards On-Site Reporting: This report shall provide a list of cardholders currently on the site. This may be for all persons within the site or just who, for a particular department or a particular contractor company, is currently present. The report may also be run to cover just a part of the site, for example, cardholders in a particular building or room.
    vi Report Auditing/Archiving: The Security Management System shall have the option to automatically and without user intervention keep a separate archival copy of each generated report, whether the report is sent to screen, printer, or file. The archival copy must be generated at the time of each request and

stored unmodified thenceforth. Systems that attempt to reconstruct the archival copy only when it is requested are not acceptable.

17. Client PCs

a. The system shall support an unrestricted number of client PCs to suit growing enterprise requirements. The system shall provide the means for multiple operators to simultaneously administer the system from convenient locations connected via a local area network (LAN) or across a wide area network (WAN).
b. Systems that operate on the SQL Express database server that restrict the number of clients shall be upgradeable to a fully unrestricted version of the software.
c. Clients shall not use mapped drives for server connections.
d. Clients shall not use UDP messaging.
e. System shall support a minimum of two pc monitors per client. The system shall additionally store the last position and size of all open dialog boxes and screens upon exiting the application on a per operator basis. The next time the operator logs into the application, the screen positions shall be restored. Such operation shall be independent of which workstation the operator uses.
f. The capability shall be provided to "lock" the window arrangement for each operator individually, such that each time they log on they have a fixed arrangement of windows that they do not have the ability to alter. Systems that cannot prevent an operator from closing or rearranging windows will not be considered. Systems that allow windows to be locked by workstation but not by user will also not be considered.

18. Addition of Cardholders to the System Database

a. The system shall provide a means of assigning access control rights to each cardholder. Access control rights determine which access points are accessible to the cardholder based on date and time of day. The system shall support an unrestricted number of access rights.
b. In addition to traditional functionality for managing access rights, the manufacturer must offer an option for PIAM capability via a product developed by the Manufacturer to support:
    i Onboarding from an Authoritative Data Source with capability to configure of Rules to provide Least Privilege Access.
    ii Request/Approval capability where employees and contractors can request access and have it approved by an Access Control Representative
    iii Auditing Campaigns of area permissions
    iv Offboarding and Use-it-or-Lose-it rules.
    v Integration to SwiftConnect for integration to Third Party Access Control Systems.

c. The software shall also provide the ability to assign an advanced set of Access rights to a cardholder on a temporary basis. The change may be initiated at any time by an authorized operator, or automatically between specified dates. This shall provide the facility of automatically adding to a card's rights between a specified date range,

after which the card will revert to its normal Doors and Times. Advanced access rights shall be able to be configured for multiple date ranges.

d. Each cardholder shall either be associated with standard door timings for door release, door open and door pre-held, or be given extended timings for persons with disabilities or – for example - someone who has to push a cart.

e. Cardholders who have not used a card reader for some time shall be readily listed to allow their card's status to be reviewed. An additional feature shall allow cardholders to be automatically set inactive and therefore access would be denied should the card have not been presented at any reader on the system for a defined number of days.

f. Cardholders shall be assigned an expiration date, and more specifically an expiry time, after which a card shall automatically become inactive and therefore be rejected at all readers on the system. To further simplify card administration, the system shall have the ability to be configured to automatically purge expired cardholder records after a configurable number of days from the date of expiration.

g. Cardholders who have mislaid or forgotten their issued card(s) shall be provided with a means of temporary card assignment. All cards issued for the cardholder shall automatically be inactivated whilst the temporary card is active.

h. The system shall allow for the definition of Access control rights to be associated with a badge design. Each user that selects that badge design shall be provided with the associated access control rights that can further be customized for the specific cardholder.

i. The system shall allow access control rights to be defined for a cardholder on a per reader basis. A timecode will be associated with each reader as it is assigned to the cardholder's access control rights.

j. The system shall allow access control rights to be defined for a cardholder on a per reader group basis. Reader groups are groups of readers. A timecode will be associated with each reader group as it is assigned to the cardholder's access control rights.

k. The system shall allow access control rights to be defined for a cardholder on an access code basis. An access code is a group of access control rights combining different readers and different reader groups, each at different timecodes. This is to be particularly suitable for role based access right assignment.

l. The system shall have a note field associated with each cardholder record. The note field shall be free form text and shall support a minimum of 256 characters. The note field shall further support the ability to attach multiple files (of any type or size) to each cardholder record.

m. When viewing a cardholder record the last twenty-five (25) valid door access transactions shall be displayed to help locate a cardholder.

n. A driver's license scanner shall be supported to simplify data entry of cardholder information. The scanner support shall include, at a minimum, the ability to automatically read, through optical character recognition, the most common fields from valid driver's licenses issued by all 50 states in the USA and from international drivers licenses, and populate these fields into the appropriate user-defined personal data fields in the cardholder record.

o. The system shall support a field for assigning an approving official to the cardholder record that defines the individual who authorized the assignment of a credential. Approving officials shall have an associated validity period and image of their signature. As an option, the assignment of an approving official shall be mandatory.

p. The Security Management System shall allow the user to enroll biometric data as part of the cardholder enrollment process. The number of verifications to determine applicability of the enrolled biometric data shall be configurable.
q. The Security Management System shall optionally be connected to other suitable biometric systems and the cardholder name and card number shall be passed to that other biometric system by a standard mechanism which has been configured by the biometric system manufacturer.

19. Cardholder Details

a. Cardholder information shall include first and last name, card number, PIN code and valid period to provide automatic expiration. PIN numbers shall be configurable from 4 to 8 digits in length.
b. Each cardholder record shall also incorporate at least 50 user-defined personal data fields, independent of user-defined fields for visitor management.
c. Data entry shall be simplified by remembering previous entries of personal data and allowing selection from a pick list to minimize repetitive typing when creating each cardholder's record. The cardholder database and the history log shall also be sorted by any of the additional fields of information making them a powerful tool for filtering data.
d. Personal data fields shall support free entry text, picking an entry from a previously configured list, or picking an entry from an updatable list. Each of these entries shall further be categorized as a date, a time, general input, card inactive date or customized input. Each category shall support the masking of input data to assure data integrity. For instance, a date mask might look like "mm/dd/yyyy" to indicate that the date input should be a two-digit month followed by a two-digit day followed by a four-digit year all separated by the slash character. The mask shall be required for customized input.
e. Personal data fields shall have the option of being configured as mandatory.
f. Personal data fields set as dates shall be definable so as to make badges expire when the date is reached, where the dates are dates at which specified training or other compliance expires

20. Locator

a. This feature shall provide a quick method of locating cardholders by displaying the last 25 valid history events along with the time, date and access point used. This information shall be available for an individual or group of persons by name, card number or by personal data.

21. Card Watch Feature

a. Any cardholder shall be easily tracked as they move around a large site by selecting card watch. As the person uses their access control card, the system shall have the ability to automatically notify the operator of the person's presence at each location.

22. Key Card Mode

a. Key card mode authority shall be assigned to special cardholders, such as site key holders, and can be enabled on a per reader basis. This shall allow a person when vacating an area or building to change the reader's mode of operation from normal access control to Key Card Out operation.
b. When in this condition only persons with key card privileges shall gain access through the door, all non-key card users are rejected regardless of their card's current access rights.
c. This special feature shall be activated/deactivated by the key cardholder, using a card swipe followed by a special code entered via the reader's keypad.

23. Serial Device Interface

a. The software shall allow the definition of ASCII commands to be sent out over a computer serial port (physical or virtual) or through the RS-232 interface of the DBU. These serial commands shall be available through the user interface as well as in the conditional logic described herein.

24. Automatic Holiday Override

a. The software shall be programmed by the operator to recognize special or holiday dates, which in turn can be linked to operational changes in how the site is to be managed on these specific days. This feature shall notify a system operator of individual holiday dates up to seven days prior provides a useful check on the date's current validity. Multiple types of holiday dates shall also be provided so that partial days or early closing requirements on specific dates can be accommodated.
b. Cardholder definitions shall be provided with the ability to add vacations in a quick and convenient manner. Dates and time periods shall be defined during which access is denied to all access points and an alarm generated if access is attempted.
c. The Security Management System shall provide a calendar function to enable scheduling of events up to three (3) years into the future.
d. The Security Management System shall provide the ability to schedule one-time events for up to three (3) years into the future.

25. Multi-Company System Partitioning

a. The access point readers, monitor points, and auxiliary outputs shall be managed on a multi-company partition basis by simply defining which devices are to be included in a partition.
b. The Security Management System shall be supplied with the ability to manage up to 64 partitions, and shall have an option to manage up to 999 partitions.
c. Multiple private or public entities shall be able to share the system with database segregation for card records and ownership of readers, monitor point inputs and switching outputs dependent upon the operators assigned permissions. Each company partition shall allow for autonomous system administration, allowing partitioned card administration, reports, and alarms.
d. Operator permissions shall be created and assigned globally or by the owning company. When created and assigned globally an Operator's password shall be associated with one or more companies.

e. Alarm reporting shall be routed to a client PC located at the company owning the monitor point or reader and can be automatically redirected to a different PC at pre-programmed times and selective days of the week.
f. Common areas, such as the main entrance, shall have the ability to be shared so that all companies may access these doors, even when different card customer/site codes have been configured.

26. Alarm Management

a. Alarm and activity management must be handled in the same executable program as other access control functions such as cardholder management, badging, and hardware configuration. Systems utilizing a separate application for alarm handling shall not be acceptable.
b. Alarms must be displayed in a separate window from non-alarm system activity. Systems which display both alarms and non-alarm activity in a single window shall not be acceptable. It must be possible to display either the alarm window, the activity window, or both at any time.
c. The Alarm window shall provide a method to filter alarms for all available alarm field parameters. Configured filters shall be saved per user with the option of sharing to all users. Filtered records shall be displayed in a separate view within the alarm window.
d. The system must provide separate permissions for alarms and activity, and allow users to be individually granted rights to view and or process either, neither, or both. Systems which cannot separately grant privileges for alarms and for non-alarm activity shall not be acceptable.
e. Alarm handling shall be efficiently managed with up to 999 priority levels and user definable instruction messages to ensure the operator monitoring the site takes appropriate responses.
f. To provide additional information when reviewing alarm signals, the operator shall either enter custom comments or simply select from a predefined pick list to provide a time-stamped record of all the actions taken throughout the incident.
g. Predefined manual commands shall be uniquely assigned for each alarm, and readily activated by the operator via a command button provided on the alarm acknowledgement screen. Additionally automatic trigger commands shall be configured to automatically operate in response to any given alarm condition.
h. The Security Management System shall be optionally configured to require operator comments when acknowledging alarms.
i. The Security Management System shall support the ability to selectively choose alarms to acknowledge and/or clear.
j. Each alarm shall be configurable to have a specified user defined color and sound, using standard sounds provided with the system or custom generated multimedia wave files.
k. Each alarm shall be capable of linking video from specified integrated video management systems (if applicable) for incident playback.
l. The Alarm Monitor screen shall provide an indication that cardholder information is available for a specific alarm. A “Card” button shall be available that when pressed will display the cardholder badge image.
m. Alarm monitor screen shall support the display of alarm statistics, shall provide up to ten alarm filters to be displayed in different tabs on the alarm screen, and shall provide the ability to sort based on each different column.

n. It shall be possible to add additional relevant fields of information to the alarm monitor screen
o. Each alarm shall be time-stamped in the local time zone (not the server time zone), and the system shall support the additional display of labels associated with different geographical time zones such as PST, EST, GMT, etc. The labels for time zones shall be customizable.
p. The system shall permit the routing and display of real time activity at any standard client PC. Activity shall be shown in a dedicated activity window that is updated automatically when new transactions occur. This option shall not be limited to routing transactions to one location and shall support the simultaneous routing and display of real time activity at multiple locations.
q. The activity display refresh near real-time and shall allow filtering, color coding, addition of cardholder photos to relevant events, freezing of the display and review of historic activity for any previous date where the activity is still in the database.
r. Alarms shall be capable of being routed to specific client machines by time of day or day of week.
s. Unacknowledged alarms shall be capable of being routed to alternate client PC(s) or to be sent by email based on age and priority of alarm.
t. E-mail alarm messages shall be controlled by time of day and day of the week. For example, e-mail to the Facility Security Supervisor would only be generated when alarms occur during after-hours times.
u. Each alarm definition shall allow a destination e-mail address to be defined. The e-mail address may be an address group as defined in the e-mail MAPI application.
v. The display of reader door alarms shall be automatically enabled or disabled by the use of timed commands, either by reader or by a group of readers.
w. The system shall support a generic ASCII input capability that allows the system administrator to define specific ASCII input strings as alarms to be displayed in the alarm monitoring window as well as on the graphical map interface if so configured.
x. An optional advanced alarm workflow capability will be available providing alternative routings through the alarm processing based on the answers to questions provided by operators. The workflow capability will be configured through an integrated dataflow diagram style drag and drop configuration screen

27. Task Management

a. A method to allow any ad-hoc or regular tasks to be completed by operators shall be provided.
b. Tasks shall define actions to be completed by specific users, or any user with a specified user role.
c. Each task shall be assigned a due date and time, and if the task is not marked as completed before the due time is reached its status shall automatically change to ‘overdue’.
d. The tasks selection window shall show all completed and incomplete tasks, each task displaying subject, due date and time, the user name or role that the task is assigned to and current status.
e. The tasks window shall provide filters for viewing task records and the ability to add new tasks, or open existing tasks (to mark them as complete or add comments for example).
f. Tasks shall allow alarm generation when they become overdue or on the immediate creation of a new task.

g. It shall be possible to add details to each task (for example, how to complete the task) and comments to facilitate management.
h. Tasks shall be configurable for re-occurrence (for example every Tuesday or every day). Once the task is completed a new instance of the task shall be created.
i. A means to attach files to tasks shall be provided.
j. Overdue tasks appearing in the alarm window shall be cleared by opening the alarm and selecting 'complete'. If the task is configured as 're-occurring' a new task shall be generated depending upon the settings in the tasks recurrence window tab.
k. Completed tasks shall be deleted automatically after the period specified by the 'Purge daily logs after' value configured for the Security Management System.
l. The number of unacknowledged task alarms shall be displayed in the Security Management System status bar along the bottom edge of the main window -a blue background shall distinguish them from system alarms.
m. The task Manager shall be a standard feature of the Security Management System with no separate licenses or license fees required to activate the feature.

28. Graphical Site Maps

a. To further enhance the presentation to the operator, the system shall have the ability to import and use graphical maps. Graphics shall be linked together using a tiered tree structure. To speed the location of an incident, each map level shall contain a clearly visible indicator as to which sub map the operator should select next to find the device that is in alarm.
b. Graphics shall also have the ability to be configured to appear automatically on presentation of a new alarm, providing the operator with prompt visual indication that an alarm has occurred.
c. The status of card readers, doors, monitor points and auxiliary outputs shall be requested from any graphic by simply selecting the icon representing the device and its current state will be displayed.
d. The icons on the graphic map shall dynamically indicate the status of the device they represent. For example, a door icon shall change to show the door open when the door position sensor indicates such, and shall change to the original icon when the door is again secure. Additionally, monitor points shall also change to show their current state.
e. Should the operator wish to change the current setting, simply pressing the right mouse button shall cause the appropriate command options list to appear for selection.
f. Having selected a command, confirmation shall be provided by reflecting the change in status on the display.
g. It shall be possible to import photos, graphics and drawings in the following formats: JPEG, Bitmap, Windows metafile or DXF.
h. Icons representing access points, monitoring points, switching outputs, alarm inputs, cameras or intercom call stations shall be placed on any map at the required location in a drag and drop manner.
i. It shall be possible to define on the graphic the location of card readers, access doors, alarm monitored points, output switching relays, cameras, intercom call stations and alarm panel devices.
j. The graphic display shall allow the operator to view the video stream from any video camera defined on the security management system. The graphic display shall allow the display of stored Digital Video Clips.

k. It shall be possible to define on the graphic the location of reader groups and camera groups. Such groups shall be placed and appear as a single icon, but actions taken on them shall affect the entire group.
l. It shall also be possible to change the status of card readers, reader groups, floor groups, alarm monitor points or output switching relays and confirm the successful execution of such commands from the graphical display. This functionality shall be capable of being restricted per device based on operator permissions.
m. The graphic display shall include the option to display a group of similar devices as a single icon. Once devices are grouped it shall be possible to change their status. For example, it shall be possible to unlock all entrance doors by executing a single command from the map display.
n. It shall be possible to display a device on any graphic, on multiple graphics, or on no graphics. It shall also be possible to display the same device in multiple locations on the same graphic. Systems that do not allow devices to be placed multiple times on the same or multiple graphic shall not be acceptable.

29. Manual and Automatic Commands

a. Operators shall be provided with a wide choice of manual commands embracing the control of card readers, monitor points, output switching relays and door locking devices. Also the operator shall have the ability to check the status of single, or multiple devices. This shall ensure the operator is always able to check the operational status of the system and make any adjustments as requirements change. When graphical maps are utilized, status requests shall be simply initiated by "clicking" on the device icon within the map. This functionality shall be capable of being restricted per device based on operator permissions.
b. Automatic commands shall be included and may operate on a timed or event basis.
c. Scheduled commands shall easily be defined linking complementary commands to occur at the start and stop times of any chosen timecode.
d. Event triggered commands shall provide an extremely powerful means of creating IF/THEN/WHEN associations encompassing a wide selection of IF conditions to the automatic execution of THEN commands subject to a WHEN timecode being active. A minimum of 10 THEN actions shall be available per trigger command.
e. Devices shall be managed on a partition basis by grouping card readers, monitor points and auxiliary outputs. This feature shall allow multiple devices to be actioned by a single command when using manual, timed and conditional commands. This functionality shall be capable of being restricted per device based on operator permission.
f. The Security Management System shall support an unrestricted number of automatic (scheduled and trigger) and manual commands. These commands shall be capable of spanning across multiple field controllers.
g. Triggered commands shall be executed directly within field controllers if the input initiating the command and the output of the command are held within the same controller.

30. Card Initiated Commands

a. The software shall allow authorized cardholders to initiate powerful trigger commands manually from selected card reader locations when certain models of card readers are used in conjunction with the field panels.

b. Up to 99 predefined commands shall be invoked by an authorized card allowing, for example, a patrolling guard to switch on outputs, disable monitor points, lock doors, providing remote management of the system during a patrol of the site.
c. The system shall only permit assigned users to enter command codes at keypad readers. Such assigned users shall not be restricted as to when or where they can enter a command code – such restrictions may be placed on the commands themselves.

31. User Code Mode

a. The Security Management System shall support the ability to put a keypad-equipped reader into User Code Mode. This feature shall allow a cardholder to gain access by entering the card number of a valid card at a reader keypad, therefore not requiring the holder to carry a card.
b. User code mode shall be enabled on a per reader basis and this mode shall support card number only, or card number and its assigned PIN code.

32. Visitor Management

a. Visitor Management shall be incorporated as a standard feature of software, with no separate licenses or license fees required to activate the feature. Operators shall be able to pre-enroll visitors using a Web (thin) or Standard (thick) client. The thin client shall connect to the server via thin client technologies such as Citrix and Microsoft™ Internet Explorer to permit any operator with visitor permissions assigned the ability to pre-enroll visitors without the need to install client software on their local machine.
b. Visitor Management shall be fully integrated with other key areas of the system, such as access, alarms management, muster and Video ID Badging. Visitor records shall have 50 personal data fields with user definable data titles independent from the personal data fields defined for cardholders. All visitor transactions and movements shall be recorded and may be reported on and filtered, using the extensive reporting capabilities of the software. Visitors may exist without being assigned a card number if access control is not required.
c. Data entry shall be simplified by remembering previous entries of personal data and allowing selection from a pick list to minimize repetitive typing when creating each visitor's record. The cardholder database and the history log shall also be sorted by any of the additional fields of information making them a powerful tool for filtering data.
d. Personal data fields shall support free entry text, picking an entry from a previously configured list, or picking an entry from an updatable list. Each of these entries shall further be categorized as a date, a time, general input, or customized input. Each category shall support the masking of input data to assure data integrity. For instance, a date mask might look like "mm/dd/yyyy" to indicate that the date input should be a two-digit month followed by a two-digit day followed by a four-digit year all separated by the slash character. The mask shall be required for customized input.
e. Personal data fields shall have the option of being configured as mandatory.
f. Visitor time of arrival and time of departure shall be tracked by the system. This feature shall be available even if a visitor is not issued a card or card number in the system.

g. It shall be possible to configure a reader to automatically inactivate presented visitor cards ready for reuse.
h. The system shall support a driver's license scanner including optical character recognition to ease data entry.
i. The Security Management System shall support capture of a business card image.
j. The Security Management System shall support the inclusion of a custom message for each visitor record.

33. Area Occupancy Monitor

a. The system shall include the ability to monitor the occupancy of an area.
b. Occupancy thresholds shall be configured for the maximum and minimum values, and associated with automatic conditional commands. These shall be used for applications such as to disable the entry readers when all the garage spaces are occupied and switch a garage full indicator sign on.
c. Complementary commands shall also be provided to enable the entry readers and turn off the indicator as a vehicle leaves the garage. Similarly when the garage is empty, the lights could be automatically turned off.

34. Device Configuration

a. The system shall support a notes field to be associated with each device configured on the system. The notes field shall be free-form text, and shall support a minimum of 256 characters. The notes field may be used for detailed device descriptions or for maintenance history.
b. The system shall allow a unique set of arbitrary files of any type to be associated with each device.
c. The system shall provide a hierarchical tree view of the system configuration supporting expansion and collapse of any and all branches.
d. It shall be possible to define the location of each device (card reader, door controller, camera etc.) within the system through a dedicated location field in the configuration record.

35. Windows Daylight Saving Auto Adjustment

a. The system shall support Windows TimeSrv or Windows time management.

36. History Archive and System Back up

a. The system shall be capable of retaining at least 25 years of activity in its online log file, disk storage space permitting. Systems that require offline storage of historical events shall not be acceptable.
b. The system shall allow on line archiving of history logs, along with database back-up of system configuration and cardholder details. To further ease the burden of remembering to back up your system's database, this function shall be able to be automated to occur without intervention at a pre-set time.
c. The system backup and history archive shall be to a local or remotely accessible UNC path.

37. System Health Dashboard

a. A dashboard consolidating useful system information into an intuitive, secure and easily configurable user interface.
b. Dashboard to Show Panels, Readers, Services, System Information, Licenses, and Disk Usage.
c. Display status and Firmware for F2F and OSDP Readers.
d. Display Status and Firmware for panels as well as IP Address information.

38. Support for Virtual Wallet Credentials
    a. Capability of issuing out Apple / Google Wallet credentials directly from the ACS Cardholder screen or via the PIAM Identity Screen.
    b. Support for 40-bit or 57-bit NFC Wallet credentials.

39. Support for Smart Cards and Biometrics

    a. The system shall have the integrated capability to capture at least two forms of biometrics – preferably fingerprint and hand geometry.
    b. Any proposed fingerprint solution shall support the enrollment and use of at least two fingerprints, which shall allow the cardholder to present either finger to gain entry.
    c. On a timed or manual basis the system shall be configurable to allow entry using the smart card only, smart card plus fingerprint or smart card plus two fingerprints, thereby raising or lowering the level of security as required.
    d. The system shall allow the assignment of a fingerprint for normal entry and a different fingerprint for duress entry. The cardholder shall have the ability to trigger a silent duress alarm by presenting the duress fingerprint. This provides the cardholder with a safe way to indicate a duress condition, without alerting anyone locally that the alarm has been triggered.
    e. An option to recall the fingerprint acceptance threshold from the smart card to override the threshold stored at the reader shall be provided. By recalling the threshold from the smart card, overall site security is not compromised by a poor quality fingerprint, which would normally require a low acceptance threshold to be set at the reader.

40. Server Hardening and Cyber Security
    1. The manufacturer of the Security Management System shall make available documentation on Server Hardening, which shall, at a minimum, detail the TCP/IP ports that are utilized by the system to allow other ports to be closed.

41. Anti-Passback

    a. The system shall support both “hard” anti-passback and “soft” anti-passback alarm reporting modes.

        i If the cardholder has access rights at a reader, but creates an anti-passback alarm, if the reader configured as hard anti-passback sends an anti-passback alarm and denies access to the door/portal.
        ii Soft anti-passback sends an anti-passback alarm, but still allows access through the door/portal.

b. The system shall support timed anti-passback. The principle of timed antipassback is simple: once a card has been used at a timed antipassback reader, the card causes an anti-passback violation if it is used again at the same or another timed anti-passback reader within a predefined period of time. The exception to this rule is when the antipassback reader has been defined to be for an exit route. In this case, the card can be used at any time without causing an alarm or event. This allows for situations where a person enters an antipassback-protected area, then wishes to exit the area immediately, perhaps, for example, because he or she forgotten something.

c. The use of an exit antipassback reader also causes the time delay for reuse of the card to be zeroed, so in the example, the person can re-enter the antipassback-protected area immediately, without having to wait. The delay can also be zeroed from the Card Holders screen or by means of an antipassback command. Sending a command may be useful if, for example, people have passed through an exit during a fire drill and the delay is long.

d. The system shall support zonal anti-passback. In the case of zonal antipassback, the building needs to be partitioned into zones. For example, zone 1 may be the main lobby, zone 2 the computer room, etc. For each reader that is defined as a zonal antipassback reader, you can specify which zone of the building the card is going from and which zone it is going to. For example, the reader may allow a card to go from zone 1 (e.g. main lobby) to zone 2 (e.g. computer room).

e. The system shall remember which zone each card is in and update this information whenever the card is used at a zonal antipassback reader. An antipassback alarm or event is generated if the reader's from zone does not match the card's currently-recorded zone. For example, an alarm or event is generated if the from zone of the reader is zone 3, but the card is currently recorded as being in zone 1. If a card's currently-recorded zone and the actual zone get out of step, either because of some violation of the system (e.g. a person has previously climbed over a turnstile) or for a legitimate reason (e.g. a person has passed through a fire exit during a fire drill), some means is obviously required to bring the two back into step. This can be accomplished from the Card Holders screen or by means of an antipassback command. Both methods put the card(s) into a "neutral zone", so that the next transaction at an antipassback reader is always accepted without violation, and the reader's to zone becomes the card's new zone.

42. Threat Level Manager Option

e. A Threat Level Manager option shall provide the ability to make system-wide changes by simply changing the threat level.

f. The Threat Level shall be selected from one of five levels that can be labeled and defined by the user. Each threat level shall also have a specified color associated.

g. The present state of the system threat level shall be visible from any view within the software.

h. The system shall restrict the ability to change threat level to the appropriate operator(s).

i. The system shall allow the configuration option to require the approval of two authorized operators to change the threat level.

j. The ability to change the threat level shall be integrated into the site graphical maps by right clicking on an appropriate icon.

k. The system shall automatically disable access rights for individuals that have a threat level threshold below the selected level. The same access rights will automatically be enabled when the threat level changes to a level below their threshold.
l. The system shall automatically modify the settings of selected card readers based on changes in threat level. For example a card reader configuration may be changed from “card only” to “card plus PIN” when the threat level changes.

43. Video Management System Option (See Section 28 23 00 for more details on Digital Video requirements)

e. The software shall allow operator to view live video from network cameras and encoders, and playback recorded video from Network Video Recorder systems. The same software option shall allow the system administrator to operate cameras attached to Network Video Recorders and Video Management Systems from all supported manufacturers simultaneously. The software shall allow instant replay of recently recorded video from any digital video source.
f. When the system is integrated with a Network Video recorder or Video Management System, it shall be possible to recall and replay stored video clips associated with the selected alarm using the alarms management screen.
g. Live video from any configured camera shall be available and viewed within the Security Management System by right-clicking on an appropriate map icon.
h. The video components including, but not limited to, supported network cameras, analog cameras connected by encoders, supported Video Management Systems, Network Video Recorders, shall be included in management reports. Management reports are to include, at a minimum:

i A tree view of all devices configured in the system,
ii Camera Configurations,
iii User audit trail of changes such as Who sent What commands that affected configuration (i.e. frame rate changes),
iv Reporting of trigger operations.

i. The video management module shall provide a graphical time and calendar tool for configuration of frame rate, resolution, pre-sets and other features.
j. Virtual Matrix

i The system shall provide a “virtual matrix” interface that shall contain:

(a) Software Pan, Tilt, Zoom and Focus (PTZF) controls which shall only be displayed when appropriate cameras are selected,
(b) Ability to view up to 36 video feeds per virtual matrix (including cameras connected to supported Video Management Systems, supported network cameras, cameras connected to supported video encoders, and other URL including web page or web interfaces to other devices),
(c) Ability to select from at least 25 pre-configured virtual matrix layouts,

(d) Ability to display active alarms in virtual matrix screen,
(e) Ability to display real-time events in virtual matrix screen,
(f) Provide a tree view of all cameras and other multimedia (such as web pages) configured in the system,
(g) Ability to save screen configurations and to restore previously saved screen configurations,
(h) Ability to perform a virtual guard tour by sequencing live video from various cameras into the main cell.
(i) The system shall support multiple instances of the virtual matrix.

ii The live video management screen shall display software pan/tilt/zoom/focus (PTZF) controls for those cameras that support such features through a software interface. The software shall also have a means of sending the PTZ camera to a pre-set position. At least 999 pre-set positions shall be supported by the Video Management software.

iii The video functions (live video display, instant replay of recently recorded video, playback of stored video, and configuration of the video functions) shall be available to any operator (with appropriate privileges) on any workstation connected to the system.

iv System shall provide (through graphical map interface or through the virtual matrix) a simple means for a guard or other operator to quickly initiate recording on a specific camera (if it were not otherwise recording).

v The system shall permit the operator to use drag-and-drop functionality to select cameras from the tree view of available sources and place them in desired positions on the virtual matrix. A double-click operation shall display the video feed from the selected camera in the next available cell.

k. Video Playback

i The system shall provide a video playback interface that shall support the following functionality as a minimum requirement:

(a) Ability to replay up to four recoded video streams simultaneously in a 2 x 2 virtual matrix.
(b) Ability to synchronize the video playback time of up to four recorded video streams.
(c) A video playback time line will show the start and end time of the selected video stream
(d) The video playback time line shall highlight any gaps in the selected video.
(e) The video playback time line shall indicate in a different color any alarm activity that relates to the recorded video.

(f) The video playback timeline shall show the alarm description and time when the mouse is positioned over the alarm in the timeline.

(g) Ability to change the video playback speed to include the following options: 0.5x, 1x, 2x, 4x, 8x, 16x, 32x, 64x, and 128x normal speed.

ii The video management module shall support still image capture and video clip export from the video stream.

iii The video management module shall support the export of video clips to CD or removable flash memory for archiving and for off-line review. The archived data shall playback on standard video viewers such as Microsoft Windows Media Player or Apple QuickTime Viewer.

l. The system shall limit operator access to video based on individual permissions.

m. Events received from Intrusion Detection Systems, Access Control, or others shall be capable of triggering video recording, to stop video recording, to display live video in the virtual matrix (or otherwise modify the view of the virtual matrix), and to display video playback.

n. The system shall allow the programming of event-based triggers to cause:

i Live video from a named camera to be displayed in a particular cell of the virtual matrix,

ii Live video from a named camera to be displayed in the next available cell of the virtual matrix,

iii Reconfiguration of the virtual matrix display based on previously stored data,

iv Playback of pre- and post-event video.

44. Data Connect Option

e. The system shall provide an option to import and/or export both cardholder details (including facial images and signatures) and system alarm information to/from an external source. This option may be used to speed initial commissioning of the Security Management System's database, or in some cases, to allow synchronization with other employee management systems. This option may also be used to pass common data to other employee-related systems or databases. It shall be possible to manually start or schedule the data import. It shall also be possible to start the data import process from an external application, thus providing the means for real time import.

f. The interface requirements shall be fully defined and support either a comma delimited ASCII text file or a Microsoft SQL® database import mechanism. Fully detailed supporting documentation shall be provided to enable a third party to design and implement this facility without needing reference to the system's manufacturer.

g. Imported data shall reside in an intermediary table within the database until an integrity check can be applied. Only after satisfying this test will data be included in the Security Management System data tables.

h. The data connect option shall be provided without extra charge for Enterprise sized Security Management Systems.

45. XML Developers Toolkit Option

e. The system shall support the ability to send and receive commands to/from external web services through an XML interface, the XML Developers Toolkit. All operations through this interface shall be accompanied by a logon username and password that will be associated in the Security Management System with operator privileges, which will limit what is permissible. The interface shall use standard security provided by web services.
f. The XML Developers Toolkit shall support the import of cardholder details. An external software system may use web services, for example, to add new cardholders, delete cardholders, modify existing cardholder data, make cards inactive, and change access rights.
g. The XML interface shall allow an external software system to obtain the details of cardholders that are already in the Security Management System database.
h. The XML interface shall allow an external software system to view, acknowledge, and clear outstanding Security Management System alarms.
i. The XML interface shall allow an external software system to send a command to a device already defined in the Security Management System (e.g. to open a door or display video from a network camera).
j. The XML interface shall allow an external software system to view the status of an Security Management System device (e.g. to determine whether a door is locked or unlocked).
k. The XML interface shall allow an external software system to import alarms from external equipment, such as intrusion systems.

46. Smart Card Encoding Option

e. The system shall provide the ability to encode contactless smart cards with access control information. The system shall support encoding either MIFARE or DESFire.
f. The software shall support the NXP Pegoda, GemPlus, and the HID OmniKey CardMan contactless card readers for the encoding and reading of Mifare and MIFARE DESFire cards.
g. The system shall be capable of capturing fingerprint biometrics and storing them on a contactless smart card, which will then be read and used to verify the cardholder during an access control transaction.
h. Any proposed fingerprint solution shall support the enrollment and use of at least two fingerprints, which shall allow the cardholder to present either finger to gain entry.
i. An option to store the fingerprint acceptance threshold in the smart card or at the reader shall be provided. By storing the threshold in the smart card, overall site security is not compromised by a poor quality fingerprint, which would normally require a low acceptance threshold to be set at the reader.

47. Guard Tour Option

e. This feature shall allow Guard Tour patrol sequences to be created consisting of a number of designated clocking points, which the patrolling guard has to visit.

f. A guard tour sequence shall define the order in which the clocking points are to be visited and also how long the guard should take to move between each clocking point location. A window of tolerance shall be included to add a +/- value to these timings.
g. The system operator shall initiate the required guard tour patrol and declares the guard who is to undertake the tour of the premises. The system shall then automatically monitor the guards progress around the patrol tour, reporting alarms if the clocking points are either out of sequence, or the guard arrives too early, or becomes overdue. The operator shall be notified as each point is clocked to allow the guard's progress around the site to be monitored. A patrol tour shall be able to be suspended, if required, and will automatically resume when the next point is then clocked.
h. Guard tour patrols shall be configurable on a per company basis when multiple companies are required on a site. Management reports shall be created from the history log to confirm when each guard tour was carried out, including any deviations or incidents during the tour.

48. Mustering Option

e. The Security Management System shall support an option to generate a muster report. The muster report shows a list of people who may be in the building (or on the site), including visitors. It is intended to be used during fire or other emergencies to support the emergency services identifying who may be left in the building, and where they may be located.
f. The muster report shall support manual or automatic operation. The report shall be initiated manually from the operator workstation or automatically when a monitor point is triggered. Once initiated, the report will regenerate automatically until there is no one left on the report or the process is manually stopped.
g. The system shall send the report automatically to nominated printers or to the screen.
h. The system shall support the use of muster readers at the muster points. As soon as a person makes a transaction at a muster reader he/she is removed from the report. A set of muster readers can be defined by assigning a reader group. The system shall automatically enable and places these readers into card-only mode when the report is started.
i. Cards with a status of inactive, expired or not yet valid shall not appear on the muster report. Once made active, the cardholder or visitor must perform a transaction at an on-site reader to be included in the report.
j. If a cardholder has more than one card, each card shall be reported individually.
k. The muster report shall include the date and time of each person's last transaction and the name of the reader used. The report shall support the ability to be subdivided/sorted according to a personal data title. For example, by choosing a personal data title of Department in the Configure/Muster screen, the report can list people under their respective departments.
l. The muster report feature shall support a time delay between starting the report and the first report appearing on the printer or on the screen. This shall give the majority of people enough time to leave the building and reach the muster point within a safe period of time. Thereafter, the report shall be automatically repeated at regular intervals. As people make a transaction at a muster reader (or other off-site reader), each new report should list fewer people than the previous. Reports stop being generated automatically when there is no one to include on the report.

m. The muster report feature shall support a delay of the first generated report until fewer than a specified number of people are left to muster.
n. The Security Management System shall support monitoring of the progress of the muster by using the View/Muster screen. This screen shall appear automatically if the muster starts automatically from a monitor point. This screen gives an immediate view of the number of people left on site.
o. The Security Management System shall support the ability to reset the muster once the emergency (or drill) is over. Resetting the muster shall automatically, if so configured, put all cardholders who had mustered back into the on-site group such that everyone would be included in another muster report, should it be started immediately after the one being reset.
p. A muster reset shall allow the operator to choose whether to disable the muster readers automatically after the reset and whether to set all cards to neutral for anti-passback.
q. For partitioned databases, the Security Management System shall support a mustering report for each partition independently.
r. Musters shall be configurable for different areas of a site. It shall also be permitted for different areas to overlap, be entirely contained within other areas or to be completely separate.

49. Intercom Integration Option (See Section 28 50 00 for more details on Security Communications requirements)

e. The system shall support a serial or other high-level connection to an intercom system. The intercom system shall be accessed by users through a call station; typically sited outside the building at doors, parking barriers, etc.
f. Visitors or other personnel generally ask permission to gain entry at the intercom call stations. These are known as call requests. The Security Management System shall allow call requests to be answered and managed by using a dedicated screen within the Security Management System application - the View/Intercom Control screen. The screen shall list all outstanding call requests, and allow the operator to communicate with the callers using simple screen buttons. The screen shall contain a Command button that is associated with commands programmed for use with the intercom. Typically, the command is used to open a door or barrier for the caller.
g. It shall also be possible to answer a call request by using the Connect button in the Acknowledge Alarms screen (if the call request is set up as an alarm) and from maps in the View/Maps screen.
h. Various alarm and/or event messages shall be associated with the use of the intercom interface. These shall be included in transaction reports generated by the Security Management System.

50. Integrated Intrusion Detection Option (See 28 xx yy spec on IDS)

e. The system shall offer a field controller range (not necessarily within all field controller models) offering an option for basic area arming, disarming, and status without the need for separate or additional panels or hardware. Systems requiring additional or separate panels to provide basic area arming, disarming, and status from keypad readers shall not be considered.

f. Integrated Intrusion Detection shall provide comprehensive control and status capabilities at the reader, including but not limited to:

    i Display area status at the reader
    ii Allow cardholder to arm or disarm the system, depending on permissions
    iii Provide visual and audible indication of entry and exit delays
    iv Automatically disarm an area upon valid access grant at any entry reader in the area

g. The system shall prevent access control readers from granting access while an area is armed, unless programmed to allow certain readers and cardholders to automatically disarm on valid access grant.
h. The system shall allow multiple, individually controlled intrusion areas to be defined on a single DBU. Systems that allow only one area to be defined per DBU shall not be acceptable.

    i The system shall allow any intrusion keypad reader on a node to control any area defined on the node.

i. For panels that include integrated intrusion, facilities shall be provided to lock out host-based modifications to configuration and access.
j. In addition to native intrusion functionality, the system must also simultaneously have the ability to control the arming and disarming of external DMP XR500 or XR550 Intrusion panels from the system's native intrusion keypads. Solutions that do not allow arming and disarming of DMP panel intrusion areas from the system's native keypad readers shall not be acceptable.

51. Intrusion Detection Panel Integration Option

e. The Security Management System shall support a high-level (serial or network interface) to an intrusion detection system (IDS). The third-party IDS shall be UL 1076 listed. The Security Management System shall support events to be recorded and displayed from the IDS system on the alarm management screen and in the transaction history reports.
f. The integration to the IDS shall support, at a minimum, secondary monitoring of all IDS alarm transactions while allowing it to still be monitored by a central station, if desired.
g. The IDS integration shall also include the ability to arm and disarm the IDS from the Security Management System user interface. This feature may not be available with all IDS products.
h. IDS alarms shall be capable of triggering a series of Security Management System events. For instance, when the IDS reports that the system was armed, the Security Management System shall be able to lock all doors.
i. IDS alarms shall be viewable on the Security Management System graphical map interface.
j. The communication with the IDS control panel shall be monitored, and the Security Management System shall produce an alarm in the event of a communications failure.

k. The Security Management System must provide integration with both the DMP communication with the IDS control panel shall be monitored, and the Security Management System shall produce an alarm in the event of a communications failure.

52. Thin Client Access Option

e. The system shall provide for an option of thin client access to the Security Management System. The thin client interface shall utilize Citrix or Microsoft Remote Desktop Services to provide the same look and feel of the thick client to minimize training time and expense. The thin client shall be capable of the same functionality of a thick client with the exception of functionality that requires access to ports on the thin client computer – Microsoft Remote Desktop Services does not sufficiently support such access.
f. The system shall provide for an option of thin client access specifically for the visitor management system. The thin client interface shall utilize Citrix or Microsoft Remote Desktop Services to provide the same look and feel of the thick client to minimize training time and expense. The thin client shall be restricted to Visitor Management functions.

53. Web Client Option

a. The system shall provide a web browser interface to facilitate Security Management System operations using Windows Internet Information Services web server technology.
b. The Security Management System web client shall allow users to easily manage cardholders, visitors and alarms from any standard web browser.
c. Users shall be able to enter cardholder and visitor details, print and encode badges, sign visitors in and out, view card status, view the last 25 valid card transactions and manage alarms.
d. Language translations shall be available together with a documented process for adding further languages at a later date.
e. User interface language selection shall include the ability to manually override automatic system detection.
f. Language selection shall determine localized input field formats (dates for example dd/mm/yyyy, mm/dd/yy etc.)
g. There shall be no requirement to install additional software on the client machine hosting the web browser.

2. Alarm Workflow Option

a. The Security Management System shall provide the ability to create, find, view modify, copy or delete workflows.
b. A workflow shall be triggered automatically when a selected alarm or task based action is performed such as opening or acknowledging a new alarm or task.
c. When a trigger event occurs, the configured workflow action(s) shall be performed (for example, opening an Security Management System window, clearing a specified alarm type, displaying an instruction or sending an email)

d. Each workflow trigger shall allow more than one action to be performed.
e. Workflow actions shall allow question prompts and answer inputs. Answers shall be able to determine the path for further actions.
f. The order in which the actions are placed within each workflow shall determine the order in which they are executed.
g. Multiple Workflows shall be allowed for each trigger. The priority of multiple workflows for a single trigger shall be configurable.
h. Workflow Manager shall utilize a graphical flow chart design.
i. Workflow Manager shall be able to execute predefined commands.
j. Different workflows shall have the ability to automatically initiate for any device or any alarm type.
k. Workflows must have the ability to display alarm instructions.
l. Workflows shall have the ability to send automated emails or create tasks in the Task Manager.

3.02 PROFESSIONAL SERVICES (PSG)

A. Manufacturer shall provide Professional Services for direct end user support through the awarded contractor.

1. All contractors shall provide Professional Services direct from the Manufacturer as follows:

a. Bench Testing and Commissioning.
b. Custom reporting.
c. Human Resource Integrations.
d. Conversions.
e. Third party integrations.
f. Disaster recovery commissioning testing .

B. Maintenance proposal should identify option for manufacturer provided Professional Services to include Life Cycle Management for ongoing system support

1. Optional elements for support should include:

a. Program Management regularly scheduled calls to include manufacturer, integrator and end user.
b. Routine manufacturer audits and scheduled maintenance.
c. Manufacturer provided annual upgrade services.

2. Bundled professional service options should be provided direct from the Manufacturer

3.03 ACCESS MONITORING & CONTROL SCHEDULES

A. see Addendum 1

3.04 SUBMITTALS

A. Product Data: Product Data submittal shall only be required if the Contractor requests a substitution or a particular brand product is not specified or recommended.

B. Procedures

1. Provide submittals to **[CLIENT]**'s Project Manager.
2. Submit three (3) copies of each submittal.

C. Shop Drawings

1. General Shop Drawings for the project as described elsewhere.
2. Provide other Shop Drawings only if specifically requested by **[CLIENT]**'s Project Manager.

D. Manufacturers Installation and Programming Instructions

1. Provide Manufacturers Installation and Programming Instructions as requested in the various Specification Sections.

E. Project Record Drawings

1. Definition: Project Record Drawings are drawings that completely record and document all aspects and features of the Work. (Also known as "as-built" drawings.)
2. The purpose of Project Record Drawings is to provide factual information regarding all aspects of the Work, to enable future service, modifications, and additions to the Work.
3. Project Record Drawings are an important element of this Work. Contractor shall accurately maintain Project Record Drawings throughout the course of this project. Project Record Drawings shall include documentation of all Work, including the documentation of existing equipment, wiring, conduits, and raceways that are to be reused in the Work.
4. **[CLIENT]** Project Manager shall furnish Contractor with two (2) sets of site plans for Contractor's use in preparing Project Record Drawings. One set shall be used as a working set, the other shall be used to prepare the final record set.
5. Contractor shall maintain the working set of Project Record Drawings at the project site throughout the course of the Work. The working set shall be updated on a daily basis as the Work progresses.
6. Project Record Drawings shall accurately show the physical placement of the following:

    a. Equipment and devices.
    b. Conduit and raceways.
    c. Junction and pull box locations.
    d. End-of-line resistor locations.
    e. Interfaces to external equipment.
    f. Connections to power and telephone circuits.

F. Project Record Drawings shall show the physical placement of each device and conduit or aerial center line, to be accurate to within one foot (1') of the nearest landmark. Where the site plan furnished by **[CLIENT]** Project Manager conflicts with actual conditions, Contractor shall

amend site plan as required. Indicate exact description of conduit runs (above ground, two foot trench, along outside wall of building, etc.).

G. Project Record Drawings shall show wire and cable runs, zone numbers, tamper circuit configuration, panel/circuit breaker numbers from which equipment is powered, and splice points. Such information may be shown on the site plans.

H. Project Record Drawings shall be available for inspection by **[CLIENT]** Project Manager on a daily basis. Incomplete or inaccurate Project Record Drawings may be cause for delay of Contractor's payment.

I. Upon completion of Work, and prior to Final Acceptance, Contractor shall prepare and submit to **[CLIENT]** Project Manager a final record set of Project Record Drawings. This set shall consist of all data transferred from the working set, supplemented by Riser Diagrams and other information. The final record set of Project Record Drawings shall be drafted by a skilled draftsperson, under the supervision of Contractor. All final Project Record Drawings shall be provided to **[CLIENT].**

J. System Documentation

1. Definition: System Documentation is a complete collection of all installation, programming, operation, and maintenance manuals and work sheets relating to the equipment provided as part of the Work.
2. Contractor shall maintain a file of System Documentation at the project site throughout the course of the Work. Such file shall be updated with new information as equipment is received and installed. System Documentation shall be available for inspection by **[CLIENT]** Project Manager on a daily basis.
3. Upon completion of Work, and prior to final Acceptance, Contractor shall prepare and submit to **[CLIENT]** Project Manager three (3) sets of System Documentation.

K. Closeout Submittals

1. Provide a set of as-built drawings and manuals to the **[CLIENT]** Project Manager

   a. As-Built Drawings
   b. Mounting Details
   c. Product Data
   d. Installation Manuals
   e. Operating Manuals
   f. Maintenance/Service Manuals

2. Provide the **[CLIENT]** Project Manager- with all programming sheets, keys to the equipment cabinets, as-built drawings, operating manuals, maintenance/repair manuals, spare fuses, all programming sheets and keys to the equipment cabinets, tools for tamper-resistant enclosures and tools for manual resetting devices.

3.05 QUALITY ASSURANCE

A. Qualifications Of Contractor

1. Contractor shall be an installation and service contractor regularly engaged in the sale, installation, maintenance and service of access control systems.
2. Contractor shall have three years experience with the installation, start-up and programming of systems of a similar size and complexity to the one proposed.
3. Contractor shall be a factory authorized dealer of the system proposed for at least two years.
4. Contractor shall provide factory certified technicians to perform the installation of all intelligent controller components in this project. Evidence of the certification shall be in writing from the manufacturer and shall be on the technicians person at all times while on site.

B. Supervision Of Work

1. Contractor shall employ a competent Foreman to be in responsible charge of the Work. Foreman shall be on the project site daily during the execution of the Work.
2. Contractor's Foreman shall be a regular employee, principle, or officer of Contractor, who is thoroughly experienced in projects of a similar size and type. Contractor shall not use contract employees or Subcontractors as Foremen.

C. Qualifications Of Technicians

1. All electronic systems Work shall be performed by electronic technicians thoroughly trained in the installation and service of specialty low-voltage electronic systems.
2. Journeyman Wireman electrical workers may be used to install conduit, raceways, wiring, and the like, provided that final termination, hook-up, programming, and testing is performed by a qualified electronic technician, and that all such Work is supervised by the Contractor's Foreman.
3. All incidental Work, such as cutting and patching, lock hardware installation, painting, carpentry, and the like, shall be accomplished by skilled craftspersons regularly engaged in such type of work. All such Work shall comply with the highest standards applicable to that respective industry or craft.
4. All 120 VAC power wiring and connections are to be performed by a qualified Journeyman Wireman, licensed to perform such Work in the **[CLIENT].**

D. Subcontractors

1. Definition: A Subcontractor is a person or entity who has a direct contract with the Contractor to perform any of the Work at the site.
2. Use of any Subcontractor is subject to the approval of **[CLIENT]**. The Contractor shall identify all Subcontractors on the Bid Form. The Contractor shall make no substitution for any Subcontractor previously selected without approval from **[CLIENT].**
3. Contractor's Foreman shall be on the project site daily during all periods when Subcontractors are performing any of the Work. Contractor's Foreman shall be in responsible charge of all Work, including any Work being performed by Subcontractors.
4. By an appropriate written agreement, the Contractor shall require each Subcontractor, to the extent of the Work to be performed by the Subcontractor, to be bound to the Contractor by the terms of the Drawings and Specifications, and to assume toward the Contractor all the obligations and responsibilities which the Contractor, by these documents, assumes toward **[CLIENT].**

E. Supervision And Construction Procedures

1. The Contractor shall supervise and direct the Work, using his best skill and attention. Contractor is solely responsible for all construction means, methods, and techniques.
2. The Contractor shall employ a competent foreman who shall be in attendance at the project site during the progress of the Work. The foreman shall represent the Contractor and all communications given to the foreman shall be as binding as if given to the Contractor.

F. Regulatory Requirements

1. All Work is to conform to all building, fire, and electrical codes and ordinances applicable in the **[CLIENT]**. In case of conflict between the Drawings/Specifications and codes, the codes shall govern. Notify **[CLIENT]** Project Manager of any such conflicts.
2. Contractor shall secure and pay for all licenses, permits, plan reviews, engineering certifications, and inspections required by regulatory agencies. Contractor shall prepare, at Contractor's expense, any documents, including drawings, that may be required by regulatory agencies.

G. Permits

1. The Contractor shall make application for and obtain any and all permits required by federal, state, county, city, or other authority having jurisdiction over the work.

3.06 DELIVERY, STORAGE, AND HANDLING

A. Security of Contractor’s Tools and Equipment: **[CLIENT]** is not responsible for the care, storage or security of any of the Contractor's tools or equipment.

3.07 PROJECT/SITE CONDITIONS

A. Environmental Conditions

1. Power: Electrical power will be supplied by **[CLIENT]** to the extent that the usage is compatible with available facilities in the vicinity of the work.
2. Telephone: Contractor may use a telephone designated by **[CLIENT]** for local and toll-free calls. The costs of long distance calls are the responsibility of the Contractor and shall not be charged to **[CLIENT].**
3. Rest room Facilities: Contractor may use existing Rest room facilities designated by **[CLIENT].**
4. Parking: **[CLIENT]** reserves the right to limit or restrict Contractor parking based upon the daily requirements of the other contractors on site.
5. Dust Control: Make provisions to control all dust, dirt, and foreign material caused by the performance of the Work.
6. Use of explosive type fastening equipment is prohibited.
7. Notify **[CLIENT]** immediately of any damage or possible damage to any other equipment.

B. Clean-Up

1. Contractor shall clean-up, on a daily basis as the Work progresses, all dirt, dust and debris caused by Contractor's operations. Clean-up shall be completed by the end of each workday to the satisfaction of **[CLIENT]**'s on-site representative.
2. In the event that Contractor fails to clean-up, **[CLIENT]** may elect to have clean-up performed by others, with the costs of such clean-up being charged to the Contractor.

C. Construction Aids

1. Definition: Construction Aids are facilities and equipment required by personnel to facilitate the execution of the Work. Construction Aids include scaffolds, staging, ladders, platforms, hoists, cranes, lifts, trenchers, core drillers, protective equipment, and other such facilities and equipment.
2. Contractor shall provide all Construction Aids required in the execution of the Work. Construction Aids that are the property of **[CLIENT]** or other contractors shall not be used without permission.
3. Storage of Construction Aids shall be coordinated with **[CLIENT]**'s on-site representative.

D. Safety

1. The Contractor shall be responsible for initiating, maintaining, and supervising all safety precautions and programs in connection with the Work.
2. Contractor shall comply with all local, state, and federal regulations and laws for the safety of the work place.

E. Accident Reports

1. Serious or fatal accidents shall be reported immediately by telephone or radio to the **[CLIENT]**'s Project Manager.

F. Existing Conditions

1. **[CLIENT]** does not warrant the condition of any portion of the existing wiring, conduit or raceway systems. Prior to submitting his proposal, Contractor shall examine all existing conditions and determine to what extent the existing wiring, conduit, and raceway systems may be reused.
2. Contractor's proposal price shall include the cost of replacing existing wiring, conduit, and raceways as required.

3.08 SEQUENCING

A. Description

1. This implementation plan describes the general approach that shall be followed in order to minimize the time for the access control systems to be operational.

B. Approach

1. Contractor shall plan and schedule all work in such a sequence as to minimize the time before the system is operational. The following is a suggested work sequence:

   a. Order all equipment needed and notify any subcontractors to schedule their participation.
   b. Perform all system layout work.
   c. Insure there are an adequate number of power receptacles available to operate all security equipment and coordinate with **[CLIENT]** as to where power is available.
   d. Provide shop drawings to verify location of all equipment, conduit runs, power connections, etc. Submit shop drawings to **[CLIENT]** Project Manager.
   e. Coordinate with **[CLIENT]** to provide space in each building's Communications Room for mounting of processors.
   f. Provide training on how to fill out the programming sheets for access levels.
   g. Prepare and pre-test all equipment to the greatest extent possible.
   h. Install all equipment.
   i. Provide training on the programming other various options.
   j. Test and inspect all systems.
   k. Perform all other Work as required.
   l. Perform the Acceptance Test.
   m. Provide training.
   n. Provide as-built drawings.

3.09 SCHEDULING

A. The Contractor, within five (5) days after being awarded the contract, shall prepare and submit for **[CLIENT]**'s information, an estimated progress schedule for the Work. The progress schedule shall be related to the entire project, and shall indicate start and completion dates.

3.10 WARRANTY

A. Contractor warrants that all Work furnished (material and labor) under this Contract will be of good quality, free from faults and defects, and in conformance with the Project Drawings and Specifications.

B. Contractor shall provide a parts and labor guarantee on all Work. Unless otherwise specified herein, Contractor's guarantee shall be for a period of two (2) years from date of Acceptance, except where any specific guarantees from a supplier or equipment manufacturer extends for a longer time.

C. Contractor's guarantee shall cover all costs associated with troubleshooting, repair, and replacement of defective Work, including costs of labor, transportation, lodging, materials, and equipment.

D. Guarantee shall not cover any damage to material or equipment caused by accident, misuse, unauthorized modification or repair by **[CLIENT]**, or acts of god.

E. Contractor shall promptly respond to **[CLIENT]**'s requests for service during the guarantee period. Contractor shall provide repair service as soon as reasonably possible upon request from [CLIENT], but in no case shall service response exceed 8 hours from time of request.

3.11 SYSTEM STARTUP

A. Power shall only be applied to the system after re-checking for proper grounding of the system and measuring all loops for lack of shorts, grounds, and open circuits.

3.12 OWNER'S INSTRUCTIONS

A. Coordination With **[CLIENT]**

1. Contractor shall closely schedule and coordinate his activities with designated **[CLIENT]** representatives.
2. Contractor shall provide **[CLIENT]**'s Project Manager with a work plan on a weekly basis. Such work plan will describe locations of intended activities, types of activities, and potential conflicts to facility operations.

B. **[CLIENT]**'s Representatives

The following are **[CLIENT]**'s designated representatives:

1. PROJECT MANAGER
   [John Doe
   Telephone (123) 456-7890]
2. PROJECT ARCHITECT
   [Jane Doe
   Telephone (123) 456-7890]
3. PROJECT ENGINEER
   [Donald Doe
   Telephone (123) 456-7890]
4. PROJECT CONSULTANT
   [Fred Doe
   Telephone (123) 456-7890]

C. **[CLIENT]**'s Right To Carry Out The Work

1. If the Contractor defaults or neglects to carry out the Work in accordance with the Project Drawings and Specifications and fails within seven days after receipt of written notice from **[CLIENT]** to commence and continue correction of such default or neglect with diligence and promptness, **[CLIENT]** may, after seven days following receipt of an additional written notice and without prejudice to any other remedy **[CLIENT]** may have, make good such deficiencies. In such case, an appropriate Change Order shall be issued deducting from the payments then or thereafter due the Contractor the cost of correcting such deficiencies.

D. Minor Changes In The Work

1. **[CLIENT]** shall have the authority to order minor changes in the Work not involving an adjustment in the Contract Sum or an extension of the Contract Time and not inconsistent with the intent of the Project Drawing and Specifications. Such changes shall be provided by written order.

3.13 COMMISSIONING

A. Manufacturer shall provide the opportunity for Professional Services to assist Contractor with commissioning.

B. After all Work is completed, and prior to requesting the Acceptance test, Contractor shall conduct a final inspection, and pre-test all equipment and system features. Contractor shall correct any deficiencies discovered as the result of the inspection and pre-test.

C. Contractor shall submit a request for the Acceptance test in writing to the **[CLIENT]** Project Manager, no less than fourteen days prior to the requested test date. The request for Acceptance test shall be accompanied by a certification from Contractor that all Work is complete and has been pre-tested, and that all corrections have been made.

D. During Acceptance test, Contractor shall demonstrate all equipment and system features to **[CLIENT]**. Contractor shall remove covers, open wiring connections, operate equipment, and perform other reasonable work as requested by **[CLIENT]**.

E. Any portions of the Work found to be deficient or not in compliance with the Project Drawing and Specifications will be rejected. **[CLIENT]** Project Manager will prepare a list of any such deficiencies observed during the Acceptance test. Contractor shall promptly correct all deficiencies. Upon correction of deficiencies, Contractor shall submit a request in writing to **[CLIENT]** Project Manager for another Acceptance Test.

F. If, at the conclusion of the Acceptance Test, all Work is found to be acceptable and in compliance with the Project Drawings and Specifications, **[CLIENT]** Project Manager will issue a letter of Acceptance to Contractor and **[CLIENT]**.

3.14 MAINTENANCE

A. Provide full procedures for all database back-ups.

B. Provide full procedures for server/workstation hard drive maintenance, such as defrag, etc.

C. Provide full procedures for maintaining physical and software firewalls.

D. Provide full procedures for upgrading software.

E. Provide full procedures for testing battery condition on all field panels for adequate back-up time.

F. Provide full procedures for any other tasks that must be performed to ensure the warranty remains intact.

PART 4 - PRODUCTS

4.01 GENERAL

A. All products not provided by **[CLIENT]** shall be new and unused, and shall be of manufacturer's current and standard production.

B. Where two or more equipment items of the same kind are provided, all shall be identical and provided by the same manufacturer.

C. Drawings and Specifications indicate major system components, and may not show every component, connector, module, or accessory that may be required to support the operation specified. Contractor shall provide all components needed for complete and satisfactory operation.

D. Product Availability

1. Contractor, prior to submitting a proposal, shall determine product availability and delivery time, and shall include such considerations into his proposed Contract Time.
2. Certain products specified may only be available through factory authorized dealers and distributors. Contractor shall verify his ability to procure the products specified prior to submitting a proposal.

E. Wire And Cable

1. General: Provide all wire and cable required to install systems as indicated. Wire and cable shall be sized to provide minimum voltage drop and minimum resistance to the devices being supplied.
2. All cables shall be specifically designed for their intended use (direct burial, aerial, etc.).
3. Comply with equipment manufacturers recommendations for wire and cable size and type.
4. Comply with all applicable codes and ordinances.

F. Conduit And Raceway Systems

1. General: The placing of surface mounted conduit on the exterior of any building shall be approved by **[CLIENT]** prior to its installation.
2. Interior Conduit:

    a. Electrical Metallic Tubing (EMT)
    b. Flexible Metal Conduit
    c. Provide fittings and connectors as required for installation of EMT or flexible conduit.

3. Surface Raceways:

    a. Sheet metal channel with fitted cover, suitable for use as surface metal raceway, WIREMOLD or approved equal.
    b. Provide fittings, elbows, and connectors designed for use with raceway system.

4. Exterior Conduit: (any of the following as determined by local code requirements):

   a. Rigid Steel Conduit
   b. Rigid Aluminum Conduit
   c. Rigid Nonmetallic Conduit (only if buried 18" below ground surface).
   d. Intermediate Metal Conduit
   e. Provide rain-tight fittings and connectors as required for installation of exterior conduit.

5. Exterior Flexible Conduit:

   a. Liquidtight Flexible Conduit: Flexible metal conduit with PVC jacket.
   b. Provide rain-tight fittings and connectors as required for installation of Liquidtight Flexible Conduit.

G. Junction And Pull Boxes

1. Interior Boxes: Sheet Metal Outlet Boxes: Sizes to be determined in accordance with code requirements for conductor fill. No box shall be smaller than a single gang 1-1/2 deep. Provide box covers as required.
2. Exterior Boxes: All exterior boxes shall NEMA 4 or NEMA 3R, watertight and dust-tight
3. All interior and exterior boxes shall have their covers fastened using security screws.

H. Lightning Protection

1. The Contractor shall provide suitable lightning protection for all processors/controllers.
2. All lightning protection equipment shall be UL listed.

4.02 ACCESS CONTROL SYSTEM - SYSTEM SPECIFICATIONS

A. Workstation (Minimum)

1. Intel Core i5 processor, 2.5GHz quad core.
2. Professional/Enterprise Edition client: 8GB, or 16GB for a client that is used to manage communication with more than one LAN chain.
3. 1Gbit/s LAN Speed

B. Server (Enterprise)

1. Intel Xeon Silver (or equivalent), 3.0GHz, 12 core.
2. 64GB RAM. This can be reduced to 32GB if SQL Server is not installed on the Symmetry Server.
3. 1Gbit/s LAN Speed
4. A "full" version of Microsoft SQL Server must be installed on the Symmetry server or on a separate database server before the Symmetry software is installed..

C. Software Only (owner-provided head-end CPU hardware)

1. AMAG Symmetry v10 Enterprise Platform Software, Standard Edition
    a. ENT-PLAT-V10 (For non-cluster)
    b. ENT-PLAT-CA-V10 (for MS or NEC Cluster)
2. Symmetry Enterprise Reader Licenses – ENT-LIC-xxx-V10
3. Symmetry Enterprise Client – ENT-CLIENT-V10
4. Optional Threat Level Manager – THREAT-LEVEL-V10
5. Optional SymmetryWeb Management Platform
    a. SWEB-PLAT-V10
    b. SWEB-xx-USER-V10
6. Optional Digital Video Management (only if Third Party integration)
    a. VID-CAM-xxx-V10
7. Optional XML Developer's Toolkit – XML-DEV-KIT-V10
8. Optional Intercom Integration – INTERCOM-KIT- V10
9. Optional Intrusion Detection Integration
    a. INTRUSION-PNL-01-V10
    b. INTRUSION-PNL-04-V10
    c. INTRUSION-PNL-16-V10
    d. INTRUSION-PNL-32-V10
10. Optional Guard Tour – GUARD-TOUR-V10
11. Optional Wireless Lock Integration License – AUTON-LIC-xxx-V10
12. Optional Workflow Manager – WORKFLOW-V10
13. Optional Muster – MUSTER-KIT-V10
14. Optional Encoding in Symmetry – CARD-ENCODING-V10

D. Field Controllers

1. AMAG Technology model M2150 Series Controller
    a. M2150-DBU (20K cardholders)
    b. EN-DBU Network Database Unit (20K cardholders)
    c. M2150 Memory Expansion
        i M2150-MEM-050K
        ii M2150-MEM-100K
        iii M2150-MEM-250K
    d. M2150-8DBC-OSDP
    e. M2150-4DBC
    f. M2150-8DC-OSDP
    g. M2150-4DC

h. M2150-AC24/4 (24 inputs, 4 outputs)
i. M2150-OC4/24 (4 inputs, 24 outputs)
j. M2150 power supply – MN-PSU-6
k. M2150 Network interface:

i MN-NIC-5 (with 100baseT)
ii MN-NIC-5-ENC (with 100baseT and AES Encryption)

l. MN-AC8/4 module (8 inputs, 4 outputs)
m. MN-OC4/8 module (4 inputs, 8 outputs)
n. Wiegand interface module

i WIM2
ii WIM4
iii WIM8

2. AMAG Technology model EN Edge Network Controller

a. EN-1DBC-PLUS PoE+ Single Door Controller
b. EN-2DBC PoE+ Two Door Controller
c. EN-LDBU Lock Database Unit (for Aperio wireless locks, 20K cardholders)

E. Cards Readers & Cards

1. AMAG Technology Smart Card Series

a. S874 Javelin wallswitch reader
b. S874-KP Javelin wallswitch reader with keypad
c. S874-EX-KP Javelin wallswitch reader with keypad – extreme temperature
d. S884-KP Javelin wallswitch reader with 4 line display
e. S853 Contact, Contactless, keypad, and LCD
f. S844/849 Contactless, optional keypad, optional LCD, optional Magstripe
g. S813 Biometric reader (fingerprint, contactless, keypad and LCD)
h. DESFire ISO 14443 smart cards

2. AMAG Technology Proximity Series

a. S870 Javelin wallswitch reader
b. S870-KP Javelin wallswitch reader with keypad
c. S870-EX-KP Javelin wallswitch reader with keypad – extreme temperature
d. S880-KP Javelin wallswitch reader with 4 line display
e. S830 Mullion card reader
f. 1326-* Standard proximity cards
g. 1386-* ISO series proximity cards

3. AMAG Technology Symmetry Blue Readers

a. 929S Symmetry Blue 929S (Wiegand + OSDP) Mullion Reader - Black - for Bluetooth / LF + HF

b. 939S Symmetry Blue 939S (Wiegand + OSDP) Wallplate Reader - Black - for Bluetooth / LF + HF
c. 939S-KP Symmetry Blue 939S-KP (Wiegand + OSDP) Keypad Reader - Black - for Bluetooth / LF + HF
d. 929F Symmetry Blue 929F Mullion Reader - Black - for Bluetooth / LF / HF - F2F.
e. 939F Symmetry Blue 939F Wallswitch Reader - Black - for Bluetooth / LF / HF - F2F
f. 929M Symmetry Blue 929M Mullion Reader - Black - for Bluetooth / LF / HF - MCLP
g. 939M Symmetry Blue 939M Wallswitch Reader - Black - for Bluetooth / LF / HF - MCLP
h. 939M-KP Symmetry Blue 939M-KP Wallswitch Reader with Keypad - Black - for Bluetooth / LF / HF – MCLP
i. 936 – USB Enrollment of Android and iOS Smartphones
j. 937-USB (USB) Symmetry Blue 937-USB Desktop Encoder, for credential enrollment to & encoding from, Symmetry v9.1 or later using iOS/Android BLE phones

4. The Contractor shall provide _____ cards with the system.

F. Electric Locks

1. xxxxxxxxxx model xxxxxxx electric strikes
2. xxxxxxxxxx model xxxxxxx electromagnetic locks
3. xxxxxxxxxx model xxxxxxx electric mortise locks
4. xxxxxxxxxx model xxxxxxx electric latch bolts
5. xxxxxxxxxx model xxxxxxx electric hinges
6. xxxxxxxxxx model xxxxxxx electric power transfers
7. xxxxxxxxxx model xxxxxxx latch bolt monitors

G. Request-to-Exit Devices

1. xxxxxxxxxx model xxxxxxx touch sense bars
2. xxxxxxxxxx model xxxxxxx electronic push bars
3. xxxxxxxxxx model xxxxxxx passive infrareds
4. xxxxxxxxxx model xxxxxxx passive infrareds with built-in audible alarm
5. xxxxxxxxxx model xxxxxxx push button switches
6. xxxxxxxxxx model xxxxxxx photoelectric beams
7. xxxxxxxxxx model xxxxxxx pressure mats

H. Wiring

1. xxxxxxxxxx model xxxxxxx Network Connections
2. xxxxxxxxxx model xxxxxxx DBU to DBU
3. xxxxxxxxxx model xxxxxxx DBU to door controller
4. xxxxxxxxxx model xxxxxxx door controller to reader
5. xxxxxxxxxx model xxxxxxx door controller to electric lock
6. xxxxxxxxxx model xxxxxxx door controller to door status switch
7. xxxxxxxxxx model xxxxxxx door controller to request-to-exit device
8. xxxxxxxxxx model xxxxxxx DBU to power supply

PART 5 - EXECUTION

5.01 ACCEPTABLE INSTALLERS

A. The system shall only be provided by Contractors who are factory authorized to install, service and maintain the system by the access control manufacturer.

B. The Contractor must have been a factory authorized dealer with the proposed manufacturer for a period of at least two (2) years before the Bid Opening Date.

C. The Contractor's installers and technicians must also be factory trained and certified to perform such tasks.

5.02 EXAMINATION

A. The Contractor shall be required to visit the installation site prior to bidding the job.

B. The Contractor shall report any discrepancies between the Specifications, Drawings, and Site Examination prior to the Bid Opening Date.

5.03 PREPARATION

A. The Contractor shall order all required parts and equipment upon notification of award of the Work.

B. The Contractor shall bench test all equipment prior to delivery to the job site.

C. The Contractor shall verify the availability of power where required. If a new source of power is required, a licensed electrician shall be used to install it.

D. The Contractor shall arrange for obtaining all programming information including access times, free access times, door groups, operator levels, etc.

5.04 INSTALLATION

A. The Contractor shall coordinate with the **[CLIENT]**'s IT Department if connecting to their network.

B. The Contractor shall carefully follow the instructions in the manufacturers' Installation Manual to insure all steps have been taken to provide a reliable, easy to operate system.

C. The Administrator Terminal shall be connected to the remote terminals before connecting to any card reader processors.

D. The Contractor shall coordinate with the **[CLIENT]**'s locksmith if converting from mechanical to electric locks.

E. Perform all Work as indicated in the Drawings and Specifications.

F. The Contractor shall install the appropriate cable from the CPU to readers, door contacts, request-to-exit devices, and electric locks at each door and/or gate.

G. All communications cables shall be kept away from power circuits.

H. The Contractor shall install the power supply(s) for electric locks in locations where they won't interfere with other operations.

I. The Contractor shall also execute adequate testing of the system to insure proper operation.

J. The Contractor shall provide adequate training of the system users to insure adequate understanding to prevent operating errors.

5.05 WORKMANSHIP

A. Comply with highest industry standards, except when specified requirements indicate more rigid standards or more precise workmanship.

B. Perform Work with persons experienced and qualified to produce workmanship specified.

C. Maintain quality control over suppliers and Subcontractors.

D. Quality of workmanship is considered important. **[CLIENT]** Project Manager will have the authority to reject Work which does not conform to the Drawings and Specifications.

5.06 EQUIPMENT PRE-TEST

A. All equipment shall be bench tested prior to delivery to job site and prior to installation. Bench test per manufacturer's installation instructions.

5.07 WIRE AND CABLE

A. Design, layout, size, and plan new wire and cable runs as required.

B. All wire and cable from the processors to all devices at each door shall be "home-run" unless otherwise specified.

C. All wire and cable, including any wire and cable that is existing and will be reused in the Work, shall be installed in conduit or surface metal raceway, except as follows:

D. Wire or cable, in lengths of less than ten (10) feet, that is "fished" within walls, ceilings, and door frames.

E. All wire and cable passing thru metalwork shall be sleeved by an approved grommet or bushing.

F. Avoid splicing conductors. All splices shall be made in junction boxes (except at equipment). Splices shall be made with an approved crimp connection. Wire nuts shall not be used on any low-voltage wiring.

G. Identify all wire and cable at terminations and at every junction box. Identification shall be made with an approved permanent label, Brady or equal.

5.08 WIRE AND CABLE TERMINATIONS

A. Identify all inputs and outputs on terminal strips with permanent marking labels.

B. Neatly dress and tie all wiring. The length of conductors within enclosures shall be sufficient to neatly train the conductor to the terminal point with no excess. Run all wire and cable parallel or normal to walls, floors and ground.

C. Install connectors as required by equipment manufacturers.

D. Terminations shall be made so that there is no bare conductor at the terminal. The conductor insulation shall bear against the terminal or connector shoulder.

E. Do not obstruct equipment controls or indicators with wire or cable. Route wire and cable away from heat producing components such as resistors, regulators, and the like.

5.09 CONDUIT AND RACEWAY INSTALLATION

A. Design, lay-out, size and plan new conduit and raceway systems as required.

B. Indoor Requirements:

1. Route exposed conduit and raceway parallel and perpendicular to walls and adjacent piping.
2. Maintain minimum six (6) inch clearance between conduit and piping.
3. Group conduit in parallel runs where practical and use conduit rack constructed of steel channel with conduit straps or clamps.
4. Use conduit bodies to make sharp changes in direction, as around beams. Fasten conduits and raceways to structural steel using approved spring clips or clamps.
5. Where conduit penetrates fire-rated walls and floors, seal opening with UL listed fire rated sealer or other methods as approved by codes.
6. No exposed conduit, raceway, or junction box shall be installed within any office area.
7. Install all boxes straight and plumb.

8. Do not support conduit from mechanical, plumbing, or fire sprinkler systems.
9. Drill or core drill all holes in walls, ceilings, or floors where required for new conduits. Do not cause damage to any structural steel or other structural support member by drilling or cutting.
10. Do not use flexible conduit in lengths longer than six (6) feet.

C. Outdoor Requirements:

1. Where conduit penetrates exterior walls, seal opening around conduit in an approved manner to make watertight.
2. Use galvanized straps and fasteners on all exterior conduit.
3. All exterior boxes will only be used to aid in pulling the cable between points.

5.10 PENETRATIONS

A. Do not penetrate any roof, flashing, exterior wall, or parapet without prior approval from **[CLIENT]**'s designated Construction Project representative.

B. When penetrating a fire wall for passage of cables and/or conduit, always provide a fire-stop system that complies with code and the local authority having jurisdiction.

5.11 FIRE RATED DOORS AND FRAMES

A. Do nothing to modify a UL. rated door or frame that would void the UL. label or fire rating.

5.12 GROUNDING

A. Provide earth-grounding of equipment as required by equipment manufacturer. Earth ground shall be connected to ground rod or approved cold water pipe. Electrical or telephone ground connections shall not be used as earth grounds. Connections to mounting posts or building structural steel shall not be used as earth grounds.

5.13 POWER TO SECURITY EQUIPMENT

A. Power all equipment from 120 VAC circuit dedicated for security use, except as noted. Mark all panel circuit breakers with labels worded "Security Equipment - Do Not Operate", or equivalent.

B. All plug-in transformers shall be located at the security control panels. Secure all low-voltage plug-in transformers to outlet with screw or strap. Clearly label all transformers to identify purpose and use.

5.14 CUTTING AND PATCHING

A. The Contractor shall be responsible for all cutting, fitting or patching that may be required to complete the Work.

5.15 PAINTING

A. **[Not Applicable.**

Or

B. **All surface raceway systems shall be painted to match the surfaces they are attached to.]**

5.16 PLYWOOD BACKING

A. Install the processor(s), power supplies, and all other related equipment on a plywood backboard for testing in the shop. The mounted assembly will then be transported "as is" to the job site for mounting in the Communication Room.

B. Fasten the plywood backing to the wall using a hanger bolt at the four corners which align with pre-drilled holes in the plywood. Secure with flat washers and a nut.

5.17 FIELD QUALITY CONTROL

A. Upon reaching Substantial Completion, perform a complete test and inspection of the system. If found to be installed and operating properly, notify **[Client]** of your readiness to perform the formal Test & Inspection of the complete system.

B. Submit the Record Drawings (as-builts) to **[Client]** for review prior to inspection.

C. During the formal Test & Inspection (Commissioning) of the system, have personnel available with tools and equipment to remove devices from their mounts to inspect wiring connections. Provide wiring diagrams and labeling charts to properly identify all wiring.

D. If corrections are needed, the Contractor will be provided with a Punch-List of all discrepancies. Perform the needed corrections in a timely fashion.

E. Notify **[Client]** when ready to perform a re-inspection of the installation.

5.18 INITIAL PROGRAMMING AND CONFIGURATION

A. Contractor shall provide initial programming and configuration of the Security Management System. Programming shall include defining hardware, doors, monitor points, clearance codes, time codes, door groups, alarm groups, operating sequences, camera call-ups, and the like. Input of all program data shall be by Contractor. Contractor shall consult with Security Consultant and Owner to determine operating parameters.

B. Contractor shall develop and input system graphics, such as maps and standby screens. Owner shall provide floor plan drawings as the basis for the creation of maps. Development of maps shall include the creation of icons for all doors, monitor points, and tamper circuits. Owner shall

provide floor plan drawings, in the form of AutoCAD .DWG or .DXF files, as the basis for the creation of maps.

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

D. Contractor shall maintain hard copy worksheets which fully document the system program and configuration. Worksheets shall be kept up to date on a daily basis by Contractor until final Acceptance by Owner. Worksheets shall be subject to inspection and approval by Owner. Provide final copies to Owner prior to Project Close-out.

E. Contractor shall maintain a complete, up-to-date magnetic tape backup of the system configuration and cardholder database. Backup shall be maintained throughout programming period until final Acceptance by Owner. Submit back-up tapes to Owner upon Final Acceptance.

F. Approximately sixty (60) days after start-up of system, Contractor shall return to project to provide follow-up assistance with system configuration as requested by Owner. Contractor shall include an allowance of forty (40) hours of labor for follow-up assistance in his Base Bid price.

5.19 TRAINING

A. Contractor shall provide complete operator training on the Security Management System. Training shall consist of thirty-two hours of classroom instruction for ten people selected by Owner, plus two (2) hours of individual hands-on training for each of ten people selected by Owner. Hands-on training shall include the opportunity for each person to operate the system, and to practice each operation that an operator would be expected to perform.

B. Training shall cover all operating features of the system, including the following:

1. System set-up and cardholder database configuration.
2. Access control features.
3. Alarm monitoring features.
4. Report generation and searches.
5. Card management and Badge Design/Printing
6. Disk backup procedures
7. Routine maintenance and adjustment procedures.

C. Training sessions are to be held at Owner’s facility, and are to be scheduled at the convenience of Owner. Contractor shall provide written training outline and agenda for each training session prior to scheduling.

D. Weekly format of training sessions shall be as follows:

1. Monday: Afternoon Session: Control Center Training
2. Tuesday: All Day: System Administrator Training
3. Wednesday: All Day: System Administrator Training
4. Thursday: All Day: System Administrator Training

5. Friday: Morning Session: Control Center Training

E. Contractor shall provide written training materials for each of ten (10) people.

5.20 OPERATOR TRAINING

A. Contractor shall provide complete operator training on the Security Management System. Two types of operator training shall be provided:

1. System Administrator Training: Three-day comprehensive training course for system managers and maintenance personnel. Provide two (2) separate on-site training sessions.

B. Training sessions shall include the opportunity for each person to operate the system, and to practice each operation that an operator would be expected to perform.

C. Contractor shall provide written training materials for each of ten (10) people at each training session.

D. Training sessions are to be held at Owner's facility, and are to be scheduled at the convenience of Owner. Some training sessions may be required to be held during evening hours and on weekends to accommodate users whose schedule does not permit attendance during regular hours.

E. Contractor shall provide written training outline and agenda for each training session prior to scheduling.

5.21 MANUFACTURER PROFESSIONAL SERVICES

A. Contractor shall coordinate with the manufacturer to provide the manufacturer's professional services team to assist the Owner in coordinating the interfaces between the Security Management System and other on-site systems as necessary.

B. Professional Services personnel shall be employed by the manufacturer of the Security Management System and shall be thoroughly knowledgeable of the Security Management System applications.

C. Professional Services personnel shall be on-site and available to meet with Owner's representatives for a period of not less than two consecutive days. On-site visit shall be scheduled at the convenience of the Owner.

END OF SECTION