truPortal™ 1.80
A&E Specifications
Access Control Systems and Database Management

P/N 461044001 • REV D • 28MAY19

Content

1.0 A&E Specifications

Table 1: A&E Specifications

Division 28	**Electronic Safety And Security**	
Level 1	28 10 00	Electronic access control and intrusion detection
Level 2	28 13 00	Access control
Level 3	**28 13 16**	**Access control systems and database management**
Level 4	28 13 16.00	Not applicable
Level 5	28 13 16.00.TP1.5	File reference only

This A&E Specification conforms to CSI MasterFormat 2004 guidelines.

The **bold** highlighted level above identifies the level this specification meets in the CSI MasterFormat hierarchy.

Feel free to consult with Interlogix regarding specific project requirements. For information and assistance, contact:

Interlogix
3211 Progress Drive, Lincolnton, NC 28092, USA
Internet: http://www.interlogix.com

SECTION 28 13 16

2.0 Part 1 General

2.1 Summary

A. Section Includes

1. Integrated Security Management System Performance Requirements

2. Integrated Security Management System Operator Workstation Requirements

B. Related Requirements

1. Integrated Systems and Options

a. 28 06 00 Schedules for Electronic Safety and Security

b. 28 13 00 Access Control (exclusive of this section)

c. 28 20 00 Electronic Surveillance

d. 28 30 00 Electronic Detection of Alarms

2. Related Sections

a. 26 33 53 Static Uninterruptible Power Supply

b. 27 20 00 Data Communications

2.2 References

A. NFPA 70 - National Electrical Code

B. NFPA 101 - Life Safety Code

C. UL 294 - Access Control Systems

D. UL 1076 - Proprietary Burglar Alarm Units and Systems

E. Americans with Disabilities Act - Public Law 101.336

F. FCC

G. RoHS - Restriction of the Use of Certain Hazardous Substances in Electrical and Electronic Equipment

H. CE - Conformité Européenne

2.3 Submittals

A. Single-line block diagram showing all related equipment interfaces

B. Manufacturer technical data sheets

C. Shop Drawings

D. Software: One (1) set of fully functional software in manufacturer’s original media packaging

2.4 Close-out Submittals

A. Maintenance Contracts

B. Operation and Maintenance Data or Manuals

C. Warranty Documentation

D. Record Documentation

E. Software

F. Commissioning Documentation and Check-Off List

G. As-Built Drawings

H. Training Course Materials

I. Training Presentations

J. Training Class Video Files

2.5 Warranty

A. Warranty - http://www.interlogix.com/support

3.0 Part 2 Products

3.1 Owner Furnished Equipment

A. Computer (Minimum Requirements):

1. Intel Pentium 4 2.8 GHz Processor
2. 1 GB RAM
3. 512 MB Video Card
4. 1 GB Free Disk Space
5. 10/100 Mb Ethernet Network Interface Card
6. 1024 x 768 screen resolution
7. Standard 101-key keyboard and 2-button wheel mouse

B. Computer Software:

1. Operating System: Windows 7 (32-bit or 64-bit), Windows 8 64-bit Classic, or Macintosh Operating System version 10.9

C. Operator Workstation Web Client:

1. Internet Browser: Internet Explorer 9, 10 or 11, Mozilla Firefox 32, Google Chrome 37, and Apple Safari 7.0.5

   a. Video control only supported when using ActiveX with Internet Explorer

3.2 System

A. Manufacturer

1. Provide all system access control software and related hardware as standard catalog product offering of a single manufacturer.

2. Exception: Servers, workstations, and related computing peripherals shall be specified characteristics that are in regular production by an industry-recognized computer manufacturer, provided that replaceable components are available from multiple third-party sources.

3. Exception: Controlled devices, such as electric locks, door actuators, sensors, etc., are specified elsewhere.

4. This specification is based on TruPortal 1.72 manufactured by Interlogix, 3211 Progress Drive, Lincolnton, NC 28092, USA. http://www.interlogix.com

B. Description

1. The system is an IP-based access control appliance.

2. The system is a card-reader security system to control access to buildings.

3. The system is a self-contained access control system.

4. The system is an out-of-the-box, all-in-one basic access control system bundled into a Web-based package.

5. Utilizes a System Controller and related peripherals.

6. Provides management, control, and monitoring of access and alarm components.

7. Setup and configuration of system application and database.

3.3 Performance Criteria

A. System Architecture:

1. Web-based application integrating multiple security functions including management, control, and monitoring of:

   a. Access control

   b. Alarm management

   c. Video surveillance interface

2. Operational on the Windows 7 (32-bit or 64-bit), Windows 8 (64-bit) and Windows 10 (64-bit) operating systems

   a. Multi-user capability

3. Standard Transmission Control Protocol (TCP/Internet Protocol (IP) networking communication protocol between client workstations, video surveillance system(s) and database subsystems

   a. Support 10/100/1000 MB Ethernet connectivity over Local Area Network (LAN)/Wide Area Network (WAN) network typologies

4. Support Dynamic Host Configuration Protocol (DHCP) or fixed IP address

   a. System Controller shall provide solutions to be programmed either in DHCP or fixed IP address

5. Support network configuration

6. System Controller supports Network Time Protocol (NTP)

7. Support Secure Socket Layer (SSL)-encrypted communications between the Web browser client and the System Controller

8. Support Advanced Encryption Standard (AES)-encrypted communications between the System Controller and door controllers
9. Support the ability to create Certificate Signing Requests (CSR), and import signed certificates, or generate and install self-signed certificates
    a. Fully Qualified Domain Name (FQDN) or SSL can be used in certificates
10. Shall automatically adjust for Daylight Saving Time (DST) (if the selected World Time Zone supports DST)
11. Reader Interface
    a. Controller only supports Wiegand interface
    b. Reader interface between controller and reader must be Wiegand
12. Support up to ten (10) user-defined personnel fields
13. Support up to 10,000 person photos in GIF, JPG, and PNG format
    a. Photos up to 200 KB in size can be uploaded
    b. Photos are automatically resized to 8 KB or less
    c. Total photo storage size: 80 MB
14. Support viewing of the most recent 65,535 events
15. Support extended door strike and door held times for ADA requirements
    a. Option to enable or disable extended times is defined on a per credential basis
    b. Extended time durations are defined on a per door basis
16. Allow current system settings and data to be saved as custom settings
17. Support auto-discovery of panels and downstream modules
18. User Wizards
    a. Provide step-by-step guidance for certain common user tasks
19. Event and Person Search
    a. Support search (filtering) of records
20. Shall allow user to create a new record based on an existing record
21. Support tooltips when user hovers over certain user interface elements
22. System status indicator
    a. Shall be visible from any screen
23. Support generation of reports
24. Support elevator control
    a. Support up to eight (8) elevators
    b. Support up to 64 floors
25. Support mustering mode
26. Support for secure access from external locations with a global access address
27. Audit log
    a. Maintain record(s) of actions performed in system over a period of time
    b. Produce report of audit log

B. Door Controller

1. Support Dual Door Interface Module

   a. Modules support two (2) doors and can be configured for one (1) or two (2) readers per door

   b. Supports 64 readers

      1) 64 doors wired for reader-in only

      2) 32 doors wired for read-in/read-out

2. Support Internet Protocol (IP)-based Single Door Controllers (IPSDCs)

   a. Modules support one (1) door and can be configured for one (1) or two (2) readers per door

      1) Supports 62 IPSDCs

      2) Supports 64 doors wired for read-in/read-out

3. Support for Wiegand-output wireless locks

   a. Schlage AD-400 (requires use of PIM-400 TD2)

   b. Assa Abloy Aperio™ (requires use of AH20 Standard Wiegand Interface Communication Hub)

4. Support digital inputs via Input Expansion Board

   a. Each module supports 16 inputs

      1) Support four (4) auxiliary inputs on the panel

      2) Support two (2) auxiliary outputs on the panel

5. Support relay outputs via Relay Output Circuit Boards connected to 8 Relay Output Expansion Board via the RS-485 SNAPP bus interface

   a. Each output module supports eight (8) outputs

6. Support downstream modules via multi-drop RS-485 communications

7. Support removable terminal blocks for all connections to downstream modules and digital inputs, relay outputs, and readers

8. Support on-board diagnostic LEDs on the System Controller

9. End Of Line (EOL) Supervision resistors

   a. Configurable

   b. Single or double

   c. 1K or 4K7

10. Report door forced alarms

11. Report door held alarms

12. Report system alarms

13. Report tamper alarms

C. Installation Wizard

1. Separate standalone installation utility

2. Supported by Windows 7 (32-bit or 64-bit) or Windows 8 (64-bit) Classic operating system

3. Shall support multiple languages

4. Shall allow user to perform initial configuration

   a. Shall allow user to install Microsoft .NET Framework 4.5 and Bonjour prerequisites

   b. Shall allow user to change the default Administrator password to enhance security

c. Shall allow user to set the time zone, date, and time

d. Shall allow user to set System controller IP address and DHCP or static IP

e. Shall allow user to select network options, including Static or DHCP, IP address, service port, Hypertext Transfer Protocol (HTTP) or HTTP Secure (HTTPS) protocol

5. Shall detect the System Controller on the LAN

6. Shall provide link to launch System application for the selected System Controller

D. Import/Export Wizard

1. Separate standalone utility to import and export data in Comma Separated Values (CSV) format

2. Supported by Windows 7 (32-bit or 64-bit) or Windows 8 (64-bit) Classic operating system

3. Shall support multiple languages

4. Shall allow user to import persons and credentials data in CSV format

a. Shall load a CSV file where each record contains person data and optional data for one credential

b. Shall allow mapping of CSV fields to System data

c. Shall allow user to declare CSV file to be used for add or update or delete operation (on a per file basis, not per record)

d. Shall allow all settings to be saved or restored to or from a file

e. Shall process all records in CSV file without requiring user interaction

f. Shall allow mapping of access level names in CSV file to existing access level names in System

g. Shall support importing of person photo via locally accessible files whose path is a field on the CSV file

h. Shall support selecting which fields uniquely identify a record

5. Shall allow user to export persons and credentials data in CSV format

a. Shall allow user to select person and credential data for export

b. Shall always export all available records

c. Shall allow user to select which fields and what field order (within a record) to export

d. Shall support export of person photos

e. Shall output records in pre-defined sort order

f. Shall allow all settings to be saved or restored to or from a file

g. Shall output all records to CSV file without requiring user interaction

6. Shall handle special characters

7. Shall produce an HTML-formatted report with summary information of import or export

8. Shall allow user to delete persons and credentials data in batch mode

9. Shall allow user to export events that provide an historical record of system activity

10. Support for data migration from Topaz application

a. Support the migration of persons records, credential records, and photos via CSV files

b. Topaz Migration Tool is available on the product DVD for dealers

c. Data can be extracted to an output folder for import into TruPortal using the Import/Export Wizard

E. Upgrade Wizard

  1. Separate standalone utility that allows users to upgrade the System Controller from an earlier version
  2. Supported by Windows 7 (32-bit or 64-bit) or Windows 8 (64-bit) Classic operating system
  3. Shall support multiple languages
  4. Shall support remote upgrades
  5. Shall update both the firmware and core code of the System Controller
  6. Shall allow user to backup data before the upgrade and restore data afterward
     a. Does not backup historical events kept for recordkeeping purposes only

F. Email Support

  1. Shall support the ability to configure an internal or external Simple Mail Transfer Protocol (SMTP) server
  2. Shall allow user to create email distribution lists
  3. Automated emails can be generated after:
     a. Scheduled backups occur
     b. Action triggers are executed

G. Backup and Restore

  1. Support full backup and restore of database to or from a file
  2. Backups can be scheduled to occur automatically
     a. Shall support automated emails to notify users about successful or failed backups
     b. Shall support the copying of backup files to shared network resources
  3. Backup and restore shall include all records and settings that a user can configure through the User Interface with the exception of:
     a. Network configuration settings
     b. Door or reader states set manually via the Door page
     c. Events
  4. Support separate backup of events to a file for recordkeeping purposes
  5. Support the ability to restore the System Controller to its original factory settings

H. Diagnostics

  1. Informational simple diagnostics
  2. Visual indicators for common failure modes that allow end users to troubleshoot
  3. Power and hardware status
  4. Resource usage
  5. System and device capacities
  6. Supports the ability to gather system information and log files into an encrypted file that can be sent to Technical Support

I. System Functions

1. Perform a scan for hardware changes
2. Control access of doors based on user-defined access control schedules
3. Create and configure schedules, holidays, and access levels
4. Manage persons and credentials
5. Control system functions remotely
    a. Monitor events, event video, and alarms
    b. Inputs and outputs
    c. Action triggers
    d. Schedules
    e. Secure, lockout, and open doors
    f. Reset Anti-passback (APB)
6. Manage alarms
7. Configure doors and readers
8. Grant access to users according to time and place
9. Update access rights
10. Send automated emails
11. Configure group permission policies
12. Configure automated action triggers that are executed when a set of conditions are satisfied
13. Configure shared network resources where scheduled backup files can be sent
14. Configure elevators and floors
15. Enable or disable mustering mode
16. Maintain record of actions in audit log

J. System Capacity:

1. Provide for a maximum of 10,000 persons
2. Provide for a maximum of 10,000 credentials
3. Provide for a maximum of five (5) credentials per person
4. Provide for a maximum of 64 access levels
5. Provide for a maximum of eight (8) access levels per credential
6. Provide for a maximum of 64 schedules
7. Provide for a maximum of six (6) time intervals per schedule
8. Provide for a maximum of eight (8) holiday groups per schedule
9. Provide for a maximum of eight (8) holiday groups
10. Provide for a maximum of 32 holidays per holiday group
11. Provide for a maximum of 255 holidays
12. Provide for a maximum of 64 areas
13. Provide for a maximum of 64 reader groups
14. Provide for a maximum of 32 operator roles
15. Provide for a maximum of 10 user-defined fields
16. Provide for a maximum of 64 video layouts

17. Provide for a maximum of eight (8) card formats

18. Provide for a maximum of 10 email lists

19. Provide for a maximum of 32 action triggers

20. Provide for a maximum of 32 Dual Door Interface modules

21. Provide for a maximum of 62 IP-based Single door controllers

22. Provide for a maximum of 64 doors

23. Provide for a maximum of 64 readers

24. Provide for a maximum of eight (8) Input Expansion Board modules

25. Provide for a maximum of one (1) 8 Relay Output Expansion Board per Input Expansion Board

26. Support a maximum of five (5) concurrent active clients

27. Maximum of four (4) DVRs and 64 cameras

28. Maximum of four (4) RS-485 SNAPP bus ports

29. Maximum of eight (8) elevators and 64 floors

30. Maximum of 32 One Time Events

K. Operator Interface:

1. Use a Web-based client user interface for system configuration, administration, management, and monitoring operations

   a. Flash plug-in required for Web-based client

2. Provide online context-sensitive help files to assist operators in system configuration and operation

3. Support for multiple languages

   a. User Interface, events, and online documentation shall be localized in the following languages:

      1) English (en-US) available in base configuration

      2) Spanish (es-ES) available in base configuration

      3) French (fr-FR) available in base configuration

      4) Dutch (nl-NL) available in base configuration

      5) Portuguese (pt-BR) available via language pack download from website

      6) German (de-DE) available via language pack download from website

      7) Italian (it-IT) available via language pack download from website

      8) Swedish (sv-SE) available via language pack download from website

      9) Turkish (tr-TR) available via language pack download from website

      10) Finnish (fi-FI) available via language pack download from website

      11) Simplified Chinese (zh-CHS) available via language pack download from website

   b. A primary System Language can be configured to determine the language used for functions performed by the System, such as assigning default device names, scheduled backups, and automated emails

   c. Languages can be added and removed; up to four languages can be active in a System at any one time

   d. Individual users can select from available, active languages

L. Operator Roles

   1. Provide up to 32 operator roles

   2. Each role shall have a fixed set of permissions and shall be able to be configured for different permission levels

   3. Include five (5) pre-defined roles

M. Cards

   1. Support card formats with total bit lengths of 20—200 bits (total card length and includes bits for card number, facility code, issue code, and parity bits)

   2. Maximum card number limited to 128 bits

   3. Maximum credential ID value that a user can enter when creating a credential shall depend on the defined card formats in the system

   4. If no formats are defined, the maximum shall be based on 128 bit card number and shall allow numbers between one (1) and 2128-1

   5. If any formats are defined, the user can enter numbers between 1 and 2N-1, where N is the largest card number bit length of all defined formats

   6. System shall include pre-defined card format types:

      a. 26 Bit (H10301) Wiegand Facility Code 200

      b. 32 Bit 14443 Cascade 1

      c. 37 Bit (I10304) Facility 40

      d. 40 Bit CASI 4002

   7. Support keypad readers for card and PIN access

   8. Support expiration dates for credentials

N. Cardholders:

   1. Support up to 10,000 persons and credentials

   2. All credentials in the system must be assigned to a person

   3. Supports RF Ideas credential card readers that can be used to read ID badge data and insert credential information into the User Interface

O. Access Control Management:

   1. Monitor all secured areas and initiate alarm notification when reader-controlled doors are breached

   2. Allow secured doors to open without generating an alarm condition upon:

      a. Valid card read and/or PIN entry

      b. Exit request using egress device

      c. Manual unlocking of door via authorized remote command

   3. Events

      a. Shall allow for the viewing of events which have occurred on the system

      b. Access Granted, Access Denied, Access Granted – Door Unlocked, and Access Denied – Door Locked

      c. Shall list the cardholder who initiated the event along with the time that the event occurred, event description, device, date/time (in format of language pack), and photo if available

      d. View and sort events

      e. Export events in sorted order

      f. View events based on door activity

   g. Shall support filtering of events
   h. Localization of event-related text into System Language

4. Normal Grant Access Time
   a. Amount of time a door temporarily opens when access is granted
5. Extended Grant Access Time
   a. Amount of time a door temporarily opens when a person has Use extended strike/held times enabled on their badge
6. Open Time
   a. Amount of time that a door is open after a Request to Exit (RTE) event occurs
7. Suppress door strike functionality
   a. Allows administrator to prevent the door strike from energizing when the RTE contact closes
8. Held Time
   a. Amount of time that a door can remain open after a successful access grant or RTE event
9. Alarm Enabled option
   a. Allows the system administrator to determine whether door held and door forced alarm events are triggered
10. RTE Inputs
    a. Shall be able to choose how to handle RTE inputs
11. Door Monitoring Input
    a. Shall be able to choose how to handle door monitoring input
12. PIN Timeout
    a. Shall be able to determine the PIN timeout
13. Attempt Limit
    a. Shall be able to determine attempt limit
14. Failed Attempt Lockout Time
    a. Shall be able to determine the failed attempt lockout time
15. Access Method
    a. Shall be able to determine the access method
16. Scheduled Lock and Unlock
    a. Support door lock and unlock functionality via schedules that can be independently assigned to doors
17. Timed Unlock
    a. Support timed unlock for user-defined period of time
    b. Door shall unlock when access is granted and shall remain unlocked until specified unlock time expires
18. Lock On Close
    a. Support lock on close
    b. Door shall unlock when access is granted and shall remain unlocked until either the specified unlock time expires, or the door is opened and closed, whichever occurs first
19. Full Host-Independent or Offline Operation
20. Unlock All Doors on Fire

a. Support unlocking all doors based on inputs or based on operator action

21. Fallback Mode Operation

a. Support a fallback mode for offline door controllers

b. The selected mode is common to all doors and shall be configured at the controller level

c. Available modes:

1) No Access = No access (default)

2) Site Code Access = Access if credential site code matches site code defined in card formats

3) All Access = Access if credential format is recognized

4) Use Local Cache Table = (For IPSDCs only) Access if credential matches one of the last 50 credentials used to successfully gain access

22. Holidays

a. Single Date

b. Yearly Recurring Date

c. Yearly Recurring Day or Week or Month

23. Reader or floor groups

a. Groups shall provide a logical grouping to facilitate creating access levels

24. Anti-passback (APB)

a. Users shall be able to define areas and assign those areas as entry or exit areas to readers, as well as define the APB mode for the areas

b. The system shall track a credential’s current area (APB is tracked and enforced by credential, not by person)

c. Hard and soft APB enforcement shall be allowed

1) Hard requires manual reset of credential

2) Soft merely logs the event

d. Shall support configurable APB auto-reset per area

P. One Time Events:

1. Support for 32 One Time Events spanning to any number of doors

2. Each door affected by a One Time Event will stay unlocked for the duration of that Event

3. A door will no longer be a part of a One Time Event if the user performs any door operation - such as "Lock out" or "Reinstate door"

Q. Schedules:

1. Support up to a fixed number of time schedules

2. Each schedule can define one or more weekly time intervals, and one or more Holiday Groups

3. The system shall include pre-defined schedules that can be deleted by the user:

a. All Days 24/7

b. Weekdays 8 AM – 5 PM

c. Weekdays 9 AM – 6 PM

d. Weekdays 7 AM – 7 PM

R. Reporting

1. System shall provide predefined reports

a. Historical

1) Access History

2) Audit Log

b. Temporal

1) Person or Roster

2) Credential

3) Reader Access

4) Roll Call

2. Allow limited filtering based on report type

3. Generated in HTML format and viewed in separate browser instance (or tab) from User interface

4. Fixed output fields and layout

5. Printable via Internet browser functionality

6. Export to CSV file

7. Permission controlled

S. Video Integration:

1. Support viewing of live and recorded video

2. Support creation of video clips

3. Support PTZ control of cameras from within the application window

4. Supported recording devices include:

a. TVN 10

b. TVN 20

c. TVN 21

d. TVN 50

e. TVN 70

f. TVR 10

g. TVR 11

h. TVR 11-C

i. TVR 12

j. TVR 41

k. TVR 42

l. TVR 60

m. TVR 12 HD

n. TVR 44 HD

If the model of the TruVision recorder is not listed, configuration may be attempted with the selection of TruVision Recorder as a generic type from the list of devices.

5. Support integration with video surveillance systems

a. Video recorders:

1) Provide an integrated digital video recorder and camera management interface for video command and control

2) Provide a multi-window video management console for real time video device monitoring and control from any operator workstation

3) Display video recorders, cameras and assigned presets in a navigation pane for operator access

4) Support request for live and recorded video transmission from video recording units at various resolutions and display sizes, independent of actual resolution settings for local recorded video, user configurable to facilitate network adaptability

5) Support multiple video recording devices

6. Requires Internet Explorer to allow install of ActiveX control

7. Video shall be associated with door and reader alarms

8. Video shall be played by the timestamp recorded with the door or reader event

T. Mobile Device Support

1. Support for iOS7 devices, including iPad 2 or later and iPhone 3GS or later

   a. Apps available via iTunes® and the Apple® App Store

2. Support for Android phones that support Android 4.0 or later

   a. App available via the Google Play store

3. Live and event-related video can be displayed via the TVRMobile app

   a. App available from iTunes, the App Store, or the Google Play store

U. Migration Wizard

1. Separate standalone utility that allows users to migrate data from TruPortal to OnGuard 7.0, 7.1, 7.2, or 7.3

2. Supported by Windows 7 (32-bit or 64-bit) or Windows 8 (64-bit) Classic operating system

3. Shall update both the firmware and core code of the System Controller

4. Shall allow user to migrate persons records, credential records, and photos

5. Shall allow mapping of access levels and fields to existing access level and field names in System

6. Shall produce reports with instructions for configuring new OnGuard system (where manual configuration is required)

V. TruPortal Connector Integration Application

1. Web-based application allows users to integrate person, credential, access level, panel or event data between TruPortal 1.72 and OnGuard 7.2 or OnGuard 7.3 (when available)

2. Supported by Windows 7 (32-bit or 64-bit) or Windows 8 (64-bit) Classic operating system

4.0 Part 3 Execution

4.1 Installers

A. Contractor requirements:

1. Local installation and service organization.
2. Provide three (3) references (minimum) whose systems are of similar complexity.
3. Installed by this contractor in the last five (5) years.
4. Presently maintained by this contractor.
5. Provide satisfactory evidence of liability insurance and Workmen's Compensation coverage for employed personnel as required by law.

B. Ensure that all personnel working on the project are registered with the state or local jurisdiction licensing board as provided for by current state or municipal statutes.

1. At time of bid, the contractor shall be licensed by the state or local jurisdiction to perform security work within the state.
2. Contractors who have security licenses or permits pending shall not be considered acceptable for bidding on this project.

C. Installer and technician requirements:

1. Must be experienced and qualified to accomplish all work promptly and satisfactorily.
2. Provide proof that designated service and support personnel have successfully completed the appropriate manufacturer offered hardware and software training and certification for installation, service and maintenance of the specified system.
3. Advise owner in writing of all designated service and support personnel responsible for installation as well as pre and post warranty service.

4.2 Examination

A. Inspect the installation site prior to bidding the job.

B. Report any discrepancies between the project specification and bid documents and the site examination prior to the bid opening date.

4.3 Preparation

A. Order all required parts and equipment upon notification of award.

B. Bench test all equipment prior to delivery to the job site.

C. 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. Verify the availability of communication infrastructure where required.

E. Arrange for obtaining all programming information including access times, free access times, door groups, operator levels, etc.

4.4 Installation

A. Requirements

1. Install all system components and appurtenances in accordance with the manufacturer's specifications, referenced practices, guidelines, and applicable codes.
2. Furnish all necessary interconnections, services, and adjustments required for a complete and operable system as specified.
3. Control signal, communications, and data transmission line grounding shall be installed as necessary to preclude ground loops, noise, and surges from adversely affecting system operation.
4. Carefully follow the instructions in the manufacturers' installation manual to ensure all steps have been taken to provide a reliable, easy to operate system.
5. Perform all work as indicated in the project specifications and bid documents.
6. Pre-program system and load onto owner's host computer.

B. Systems Integration

1. Coordinate with the owner's IT Department prior to connecting to the owner's network.
2. Work in harmony with all other trades.
3. Integrate related system and sub-systems.

4.5 Quality Control

A. Workmanship

1. Comply with highest industry standards, except when specified requirements indicate more rigid standards or more precise workmanship.
2. Perform work with persons experienced and qualified to produce workmanship specified.
3. Maintain quality control over suppliers and subcontractors.
4. Quality of workmanship is considered important. Owner's representative will have the authority to reject work which does not conform to the project documents.

B. Site Tests and Inspections

1. Execute adequate testing of the system to insure proper operation.
2. 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 and inspection of the complete system.
3. Submit the Record Drawings (as-builts) to owner's representative for review prior to inspection.
4. During the formal test and 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.
5. If corrections are needed, the contractor will be provided with a punch list of all discrepancies. Perform the needed corrections in a timely fashion.
6. Notify owner when ready to perform a re-inspection of the installation.

C. Software Engineering Support

1. Provide software engineer services to assist the owner in coordinating the interfaces between the security management system and the staff databases or other remote systems.
2. Software engineer shall be certified by or employed by the system manufacturer, and shall be thoroughly knowledgeable of the system applications.
3. Software engineer 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.

4.6 System Start-up

A. Provide initial programming and configuration of the security management system.

B. Programming shall include defining hardware, doors, monitor points, clearance codes, time codes, door groups, alarm groups, operating sequences, camera call-ups, etc. Input of all program data shall be by contractor. Consult with owner's representative to determine operating parameters.

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

D. Maintain hard copy worksheets which fully document the system program and configuration

1. Worksheets shall be kept up to date on a daily basis until final acceptance by owner.
2. Worksheets shall be subject to inspection and approval by owner.
3. Provide final copies to owner prior to project close-out.

E. Maintain a complete, up-to-date backup of the system configuration and cardholder database.

1. Backup shall be maintained throughout programming period until final acceptance by owner.
2. Submit back-up media to owner upon Final Acceptance.

F. Provide follow-up assistance with system configuration sixty (60) days after start-up of system as requested by owner. Include a labor allowance for follow-up assistance in base bid price.

4.7 Closeout Activities

A. Commissioning

1. Place entire system into full and proper operation as designed and specified.
2. Verify that all hardware components are properly installed, connected, communicating, and operating correctly.
3. Verify that all system software is installed, configured, and complies with specified functional requirements.
4. Perform final acceptance testing in the presence of owner's representative, executing a point by point inspection against a documented test plan that demonstrates compliance with system requirements as designed and specified.
5. Submit documented test plan to owner at least fourteen (14) days in advance of acceptance test, inspection and check-off.
6. Conduct final acceptance tests in presence of owner's representative, verifying that each device point and sequence is operating correctly and properly reporting back to control panel and control center.
7. Acceptance by owner is contingent on successful completion of check-off; if check-off is not completed due to additional work required, re-schedule and perform complete check-off until complete in one pass, unless portions of system can be verified as not adversely affected by additional work.

8. System shall not be considered accepted until all acceptance test items have been successfully checked-off. Beneficial use of part or all of the system shall not be considered as acceptance.

B. Training

1. Provide system operations, administration, and maintenance training by factory trained personnel qualified to instruct.

   a. Training shall be oriented to the specific system being installed under this contract as designed and specified.

   b. Provide training sessions at owner's facility, and schedule at the owner's convenience.

   c. Provide written training outline and agenda for each training session prior to scheduling.

   d. Record and provide copies of training programs for owner knowledgebase.

2. Owner will designate personnel to be trained.

   a. Provide classroom instruction for people selected by owner.

   b. Provide two (2) hours of individual hands-on training for each person.

      1) Hands-on training shall include the opportunity for each person to operate the system.

      2) Hands-on training shall include practice of each operation that an operator would be expected to perform.

   c. Provide printed training materials for each trainee including product manuals, course outline, workbook or student guides, and written examinations for certification.

3. Cover all operating features of the system, including the following:

   a. System set-up and cardholder database configuration.

   b. Access control features.

   c. Alarm monitoring features.

   d. Report generation and searches.

   e. Card management.

   f. Database backup procedures.

   g. Routine maintenance and adjustment procedures.

END OF SECTION