APPENDIX E
ACCESS CONTROLS SYSTEM DESIGN GUIDELINES (TAMPA CAMPUS)

REVISED: SEPTEMBER 20, 2006
USF UNIVERSITY POLICE DEPARTMENT


**APPENDIX E – ACCESS CONTROL SYSTEM**

INDEX

<table>
<thead>
<tr>
<th>PART 1</th>
<th>GENERAL</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.1</td>
<td>SCOPE OF WORK</td>
</tr>
<tr>
<td>1.2</td>
<td>ACCESS CONTROL</td>
</tr>
<tr>
<td>1.3</td>
<td>DESCRIPTION OF WORK</td>
</tr>
<tr>
<td>1.4</td>
<td>SUBMITTALS</td>
</tr>
<tr>
<td>1.5</td>
<td>QUALITY ASSURANCE</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>PART 2</th>
<th>PRODUCTS</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.1</td>
<td>MANUFACTURER</td>
</tr>
<tr>
<td>2.2</td>
<td>MATERIALS</td>
</tr>
<tr>
<td>2.3</td>
<td>SYSTEM REQUIREMENTS</td>
</tr>
<tr>
<td>2.4</td>
<td>SOFTWARE</td>
</tr>
<tr>
<td>2.5</td>
<td>HARDWARE</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>PART 3</th>
<th>EXECUTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.1</td>
<td>SECURITY CONTRACTOR</td>
</tr>
<tr>
<td>3.2</td>
<td>PROJECT MANAGEMENT</td>
</tr>
<tr>
<td>3.3</td>
<td>PERSONNEL</td>
</tr>
<tr>
<td>3.4</td>
<td>ACCESS CONTROL SYSTEM - INSTALLATION</td>
</tr>
<tr>
<td>3.5</td>
<td>COMMISSIONING AND TRAINING</td>
</tr>
<tr>
<td>3.6</td>
<td>TESTING</td>
</tr>
<tr>
<td>3.7</td>
<td>WARRANTY, MAINTENANCE AND SERVICE</td>
</tr>
</tbody>
</table>

**PART 1  GENERAL**

1.1  **SCOPE OF WORK**

A. The scope of the work included under this division of the Specifications shall include installing a card access system for managing access to buildings. Specifically this is accomplished by using card readers on the exterior doors of the various buildings. Additional access control may be required at Department Suites Doors and open use classrooms as determined by the user group and educational outreach. The **USF ID** card will be used for this system. This will require that all students, faculty and staff who need after-hour access to have a valid USF ID card. Normally, the interior doors of the buildings will continue to have manual keys. However, the exterior doors will be re-keyed with the University Police master key to increase the security. Building occupants will no longer carry exterior door keys.

B. The integration of the Camera system and the Card access system to the USF Secure Perfect system is the responsibility of this contractor.

C. Definition:

1. **Contractor:** In this section the Contractor refers to the Access Control Integrator.
2. **Owner/User:** In this section the Owner/User refers to USF.

1.2  **ACCESS CONTROLS (As Shown in the Project CAD drawings)**

A. Contractor is to provide and install **CASI** products and ancillary products needed to fulfill the sequence of operation for each door as shown in the CAD drawings provided.

B. Contractor is to provide programming (points and alarms) and commissioning the system.

C. Installation, wiring and conduits from panel to the doors & all hardware tied into the access control system are done by this contractor (including 120 VAC).

D. It is the responsibility of this contractor to coordinate and integrate the door hardware with the access control system to deliver a fully functional system.
1.3 DESCRIPTION OF WORK
A. The Integrated Security Management System (ISMS) shall manage the security operations for a single site or for multiple sites. Installing the ISMS and bringing it to operational status requires the following major steps:
   1. Determine operational requirements and plan system to implement them.
   2. Select host computer site.
   3. Install and configure, where necessary, the communications network providing communications between the Client and Server computer workstation.
   4. Install and integrate Access Control, Alarm Monitoring and related security hardware.
   5. Configure local access panels and ISMS Server computer system to communicate with one another.
   6. Enter security system database.
   7. Connect between host system, access controllers, and related hardware.
   8. Test security system communication and operation.
   9. Train operators.

1.4 SUBMITTALS
A. Shop Drawings
   1. Provide complete shop drawings which include the following:
      a. Indicate all system device locations on architectural floor plans. No other system(s) shall be included on these plans.
      b. Include full schematic wiring information on these drawings for all devices. Wiring information shall include cable type, conductor routings, quantities, and connection details at devices.
      c. Include a complete access control system one line, block diagram.
      d. Include a statement of the system sequence of operation.
      e. The shop drawings have to be approved by the engineer of record and USF Physical Plant before any commencement of the work.

B. Product Data
   1. Provide complete product data that includes the following:
      a. Manufacturer’s data for all material and equipment, including terminal devices, local processors, computer equipment, access cards, and any other equipment provided as part of the ISMS.
      2. A system description, including analysis and calculations used in sizing equipment required by the ISMS. Description to show how the equipment shall operate as a system to meet the performance requirements of the ISMS. The following information shall be supplied as a minimum:
         a. Central processor configuration and memory size
         b. Description of site equipment and its configuration
         c. Protocol description
         d. Rigid disk system size and configuration
         e. Backup/archive system size and configuration
         f. Start up operations
         g. System expansion capability and method of implementation
         h. System power requirements and UPS sizing
         i. A description of the operating system and application

C. Contract Close-Out Submittals
   1. Provide three (3) sets of manuals including operating instructions, maintenance recommendations and parts list including wiring and connection diagrams modified to reflect as-built conditions.
   2. Submit as-built drawings (3) containing all information required in shop drawings.
D. Manuals

1. Final copies of the manuals shall be delivered within thirty (30) days after completing the installation test. Each manual's contents shall be identified on the cover. The manual shall include names, addresses, and telephone numbers of each security system integrator installing equipment and systems and the nearest service representatives for each item of equipment for each system. The manuals shall have a table of contents and labeled sections. The final copies delivered after completion of the installation test shall include all modifications made during installation, checkout, and acceptance. The manuals shall contain the following:

a. Functional Design Manual
   The functional design manual shall identify the operational requirements for the system and explain the theory of operation, design philosophy, and specific functions. A description of hardware and software functions, interfaces, and requirements shall be included for all system operating modes.

b. Hardware Manual
   The manual shall describe all equipment furnished including:
   - General description and specifications
   - Installation and check out procedures
   - Equipment layout and electrical schematics to the component level
   - System layout drawings and schematics
   - Alignment and calibration procedures
   - Manufacturers repair parts list indicating sources of supply

c. Software Manual
   The software manual shall describe the functions of all software and shall include all other information necessary to enable proper loading, testing, and operation. The manual shall include:
   - Definition of terms and functions
   - Use of system and applications software
   - Initialization, start up, and shut down
   - Alarm reports
   - Reports generation
   - Data base format and data entry requirements
   - Directory of all disk files

D. Operators Manual
   The operator's manual shall fully explain all procedures and instructions for the operation of the system including:
   - Computers and peripherals
   - System start up and shut down procedures
   - Use of system, command, and applications software
   - Recovery and restart procedures
   - Graphic alarm presentation
   - Use of report generator and generation of reports
   - Data entry
   - Operator commands
   - Alarm messages and reprinting formats
   - System access requirements

e. Maintenance Manual
   The maintenance manual shall include descriptions of maintenance for all equipment including inspection, periodic preventive maintenance, fault diagnosis, and repair or replacement of defective components.
E. As-Built Drawings
   1. During system installation, the Contractor shall maintain a separate hard copy set of
drawings, elementary diagrams, and wiring diagrams of the ISMS to be used for
record drawings. This set shall be accurately kept up to date by the Contractor with all
changes and additions to the ISMS. In addition to being complete and accurate, this set
of drawings shall be kept neat and shall not be used for installation purposes. Copies of
the final as-built drawings shall be provided to the end user in DWG format using
AutoCAD Architectural Desktop 2004 or newer. Three (3) hard copies shall be
submitted in addition to electronic copies on two (2) CDs.

1.5 QUALITY ASSURANCE
   A. The manufacturers of all hardware and software components employed in the system shall be
established vendors to the access control/security monitoring industry for no less than five (5)
years.
   B. The security system integrator shall have been regularly engaged in the installation and
maintenance of integrated access control systems similar in size and scope to that outlined
herein for a period of no less than five (5) years.
   C. The security system integrator shall supply information attesting to the fact that their firm is an
authorized product dealer for the system proposed.
   D. The security system integrator shall supply information attesting to the fact that their
installation and service technicians are competent factory trained personnel capable of
maintaining the system and providing reasonable service time.
   E. The security system integrator shall provide a minimum of three (3) references whose
systems are of similar complexity and have been installed and maintained by the security
system integrator in the last five (5) years.
   F. There shall be a local representative and factory authorized local service organization that
shall carry a complete stock of parts and provide maintenance for these systems. Local shall
be defined as an area in a fifty (50) mile radius of installed location.

PART 2 PRODUCTS
2.1 MANUFACTURERS
2.1.1 PRODUCTS
   A. Approved Software & Field Hardware:
      Secure Perfect 6.1 or the latest version
   B. Integrated Security Management System:
      GE Interlogix

2.1.2 CONTRACTORS
   A. Any approved GE Interlogix Partner:
      (i.e. installer Security One, BEST, SIEMENS, ADT, etc.).

2.2 MATERIALS
   A. This Section covers the provision of an Integrated Security Management System (ISMS) for
the USF facility located at 4202, E Fowler Avenue, Tampa, Florida including all items and
subsystems shown on drawings or otherwise required by these Specifications for USF
Building.
   B. The requirements for these specifications shall be understood to be the USF Standard.
The requirements shall be expanded as necessary to ensure quality. However, unless USF
prior written approval is obtained, the requirement herein shall not be deleted or revised.
   C. USF shall be hereinafter referred to in this document as the OWNER and the bid
respondents shall be referred to as the SECURITY CONTRACTOR. The term OWNER
includes direct employees and other appointed OWNER agents such as architects or
consultants. These agents may be requested by the OWNER to represent the OWNER in
undertaking certain project tasks.
D. If any statement in this or any other specification is in conflict with any provision of the General Terms and Conditions of the contract, the provision stated in the General Terms and Conditions shall be precedence. Any questions that require additional interpretation and guidance shall be immediately brought to the OWNER’S attention.

2.2.1 SECTION INCLUDES
A. This section covers the provision of ISMS including all items and Subsystems shown on drawings or otherwise required by these specifications.
   1. ISMS Computer, Hardware, software, and control panels for access control and alarm management.
   2. Card readers and other security input/output devices for access control and alarm monitoring of secured areas.
   3. Automatic Doors & operators:
   4. Video Surveillance System

2.2.2 RELATED SECTIONS
A. Conduit, Raceways and Cable trays: Division 16 Section 16111.
B. Fire stopping Penetration through Rated Construction: Division 16.
C. Electrical, Cabling, and Wiring: Division 16 Section 16180.
D. Door Hardware: Division 8

2.3 SYSTEM REQUIREMENTS
A. Architecture:
   1. The ISMS shall consist of personal computer-based hardware and software capable of integrating multiple security functions, including management, control and monitoring of card access, alarms, photo ID card production, interfacing with video surveillance and database subsystems.
   2. The ISMS shall be a true 32 bit multi-threading client/server application, designed for the Microsoft Windows 2000/XP platform; with multi-user and multi-tasking capability, developed in a high level "C" language.
   3. The ISMS shall use a commercially available standard database that is SQL and ODBC compliant, certified for the Microsoft Windows 2000/XP platform.
   4. The ISMS shall support user definable database partitioning, for defining limited views of the ISMS database.
   5. The ISMS shall conform to the standard TCP/IP networking communications protocol between the application/database server, operator workstations, control panels, video surveillance system(s) and database subsystems; using 10/100Mb Ethernet connectivity over LAN/WAN network typologies.
   6. The ISMS shall be flexible and scalable in architecture, permitting expansion of both capacity and functionality, to be implemented progressively as needed, through software licensing and/or software upgrades.
   7. The ISMS shall provide a real-time display of all system status and data, at all operator workstations.
   8. The ISMS shall monitor status and record activity transactions of all secured areas and alarm input/output points; visually and audibly annunciate alarms upon change of status, for assessment and response at all operator workstations.
   9. The ISMS shall monitor and record card access, alarm, and operator activity to an online history/archive database for reporting. A database-reporting interface shall be accessible from all operator workstations.
   10. The ISMS shall operate spanning across multiple time zones with automatic adjustment for daylight savings time. The host server, operator workstations, control panels, and video surveillance system(s) shall be capable of residing in different time zones while processing, recording, and displaying activity occurrences in their respective local time.
   11. The ISMS shall employ distributed processing technology, allowing the host to function almost entirely as an application/database server. The majority of the real-time, day-to-day decisions shall be made locally by intelligent control panels. The control panels shall
be the direct field interface for all access control, alarm sensing, and input/output-controlled devices.

12. Each control panel shall be able to continue access control and alarm-monitoring operations autonomously, in the event of ISMS hosting failure.
13. The ISMS shall manage and automatically download in real-time, all database changes made from all operator workstations, to the control panels that require notification of the specific database changes or updates.

B. System Capacity: Provide total system capacity to accommodate the following:
1. Cardholder Database: A minimum of twenty-five-thousand (25,000) access control cards upgradeable to one-hundred-thousand (100,000). Multiple access control cards assignable per cardholder, each tracked separately. Access control cards shall be unique four to twelve (4 -12) digit numbers without facility code dependency.
3. General Purpose Alarm Inputs: A minimum of three-hundred-twenty (320) alarm input points upgradeable to twenty-thousand-forty-eight (20,048).
4. General Purpose Outputs: A minimum of two-hundred-fifty-six (256) relayed or TTL level output points upgradeable to sixteen-thousand-three-hundred-eighty-four (16,384).
5. Control Panels: A minimum of thirty-two (32) upgradeable to two-hundred-fifty-six (256).
6. Workstations: A minimum of five (5) upgradeable to twenty-five (25).
7. Centralized on-line storage of historical transactions, a minimum of one-million (1,000,000) events.
8. Time Schedules: Unlimited definable in system database, up to one-thousand-twenty-four (1,024) concurrently active per control panel.
9. Access Rights: Unlimited definable in system database, up to ninety-six (96) concurrently active per access card per control panel.

C. Control Panel Capacities:
1. Field Configurable Control Panel:
   a. Card Readers: Capable of supporting up to sixteen (16) card readers.
   b. General Purpose Alarm Points: Capable of supporting up to eighty (80) four-state supervised alarm input points.
   c. General Purpose Outputs: Capable of supporting up to sixty-four (64) relay or TTL level output points.
   d. Access Control Card Memory: Up to twenty-eight-thousand (28,000).
   e. Offline-History Transaction Buffer: Up to sixteen-thousand (16,000).
   f. Time Schedules: Up to one-thousand-twenty-four (1,024).
   g. Access Rights: Up to ninety-six (96) per access control card.
   h. Uninterruptible Power Supply: Battery rated for a minimum two (2) hours of continuous operation at full load.
2. Fixed Configuration Control Panel for small distributed installations:
   b. General Purpose Alarm Points: Support ten (10) four-state supervised alarm input points.
   c. General Purpose Outputs: Support eight (8) relay output points.
   d. Access Control Card Memory: Up to twenty-eight-thousand (28,000).
   e. Offline-History Transaction Buffer: Up to sixteen-thousand (16,000).
   f. Time Schedules: Up to one-thousand-twenty-four (1,024).
   g. Access Rights: Up to ninety-six (96) per access control card.
   h. Uninterruptible Power Supply: Battery rated for a minimum two (2) hours of continuous operation at full load.

D. Operator Interface:
1. The ISMS shall use a single Windows based client application interface for system configuration, administration, management, and monitoring operations.
2. The ISMS shall provide a mouse-driven, Windows based, graphical user interface allowing operator(s) to open and work on multiple windows simultaneously, at host server and workstation(s) with minimal degradation to system performance.

3. The ISMS shall provide on-line contact sensitive help files to facilitate operators in the configuration and operation of the ISMS. Standard Windows help commands for Contents, Search, Back, and Print shall be supported.

4. The ISMS shall implement National Language Support (NLS) in a manner that allows simultaneous multi-lingual operation, based on individual operator language preference. The graphical user interface and on-line help shall support English and [Spanish] [French] [Portuguese] [Italian] [German] [Dutch] [Polish] [Chinese] [Korean] [Japanese].

5. The ISMS shall support defining an unlimited number of operators; application access via workstation(s) shall be restricted by operator login and password. Operator profiles shall be configurable to include form level permissions, database partition views, and language preference.

E. Cardholder Management:
   1. The ISMS shall provide an operator interface for enrollment, modification, and deletion of cardholder’s personnel and access control information. The ISMS shall allow enrollment of cardholder’s personnel and access control information in advance, without requiring assignment of access control card(s). The cardholder’s personnel and area access information shall include the following data:
      a. First Name.
      b. Middle Name 1.
      c. Middle Name 2.
      d. Last Name.
      e. Employee Number.
      f. Personnel Type (Selectable from a user defined list that shall include at a minimum; Permanent, Temporary, Contractor, and Visitor classifications).
      g. Department (Selectable from a user defined list).
      h. Facility (Selectable from a user defined list of database partitioned views).
      i. Trace Activity (Enable/Disable).
      j. Address 1 (User definable label).
      k. Address 2 (User definable label).
      l. Address 3 (User definable label).
      m. Address 4 (User definable label).
      n. Address 5 (User definable label).
      o. Telephone.
      q. Access Right(s) (Multiple assignments).
      r. Access Card(s) (Multiple assignments).

F. Card ID Management:
   1. The ISMS shall provide an operator interface for enrollment, modification, and deletion of access control card ID information in advance, without requiring assignment to a cardholder and shall include the following data:
      a. Description.
      b. Card ID number (4 to 12 digit, unique access control identifier).
      c. Pin Number (4 digit number for authenticating cardholder in card & keypad reader applications).
      d. Status (Issuable, Active, Lost, Suspended, Remake).
      e. Assigned Cardholder (Selectable from predefined list of cardholders).
      f. Issue Date.
      g. Return Date.
      h. Expire Date (Required to automatically expire access control card ID numbers at control panel level in real-time without ISMS host notification).
G. Access Control Management:
1. The ISMS shall allow or deny access to secured areas, arm and disarm intrusion zones, and provide output control via access control readers, based on validation of a cardholder’s assigned access rights.
2. The ISMS shall support defining an unlimited number of access rights in a manner that associates reader(s) with a specific time schedule. The time schedule shall define the specific time(s) of day and day(s) of the week for which access will be granted for the associated reader(s) and/or controlled output(s).
3. The ISMS shall allow cardholders to be assigned multiple access rights and multiple access control cards, without requiring duplicate database entry of cardholder personnel information.
4. Any and all access control cards assigned to a cardholder, shall automatically inherit all of the access rights assigned to the cardholder.
5. The ISMS shall monitor all secured areas and process an alarm notification whenever a reader controlled door is opened, unless door is opened pursuant to a valid card read, exit request through egress device, or door has been manually unlocked via remote command from an authorized system operator.
6. The ISMS shall be user configurable to operate in either global or local mode, controlling IN and OUT access of secured areas for anti-passback and time & attendance applications.

H. Time Schedule and Mode Management: The ISMS database shall support defining an unlimited number of schedules. Schedules shall define time, day, and date intervals for automatically executing ISMS functions, events, and mode changes.

1. Time schedules: Shall define start and stop interval(s) by time of day and day of week or mode. Each time schedule shall support multiple intervals per day and multiple days per week. Time schedules shall be applicable to the following ISMS functions:
   a. Cardholder access rights to secured areas.
   b. Readers online/offline.
   c. Doors lock/unlock.
   d. Alarm monitoring on/off.
   e. Inputs enabled/disabled.
   f. Outputs on/off.
   g. Transaction routing for alarm and card activity.

2. Event Schedules: Shall define specific time(s) for an event to occur by time of day and day of week or mode. Each event schedule shall support multiple events per day and multiple days per week. Event schedules shall be applicable to the following ISMS functions:
   a. Changing reader modes of operation between card only, card-plus-keypad, and card or keypad.
   b. Changing alarm monitoring sense times.
   c. Resetting anti-pass-back and/or time and attendance IN/OUT status of all cardholders in control panel databases.
   d. Initiating a scheduled dial from host to communicate to remote dialup control panels.

3. Mode Schedules: Shall define specific times and dates for indicating to system control panels which time and event scheduled functions to execute.
   a. A minimum of four (4) distinct mode classifications will be supported for categorizing time and event scheduled functions. Mode classifications shall include Normal and three (3) user definable modes such as holiday, evacuation, lock-down, or others.
   b. Mode changes can either be scheduled to occur at a specific date and time or manually changed by an operator.

I. Reader / Door Control:
1. The ISMS shall allow access control readers to be individually configured for different applications and modes of operation and shall support the following:

   a. **Physical Reader Type:** Each reader’s physical mode of operation shall allow to be manually changed by an operator, or automatically via a system event schedule, for increasing or decreasing the level of security required for accessing secured areas at any time.
      1) Card Only.
      2) Card-plus-keypad.
      3) Card or Keypad.

   b. **Logical Reader Type:** Each reader’s logical mode of operation shall be configurable to support the following:
      1) Normal.
      2) Anti-pass back IN, configurable to operate in enforced or passive mode.
      3) Anti-pass back OUT, configurable to operate in enforced or passive mode.
      4) Time & Attendance IN, configurable to operate in enforced or passive mode.
      5) Time & Attendance OUT, configurable to operate in enforced or passive mode.
      6) IN Required, configurable to operate in enforced or passive mode.
      7) Elevator Control.

d. Maximum unlock time after a valid card read shall be configurable from zero to two-hundred-fifty-five (0 - 255) seconds.

e. Alarm sense time for allowing a door to remain open after a valid card read, before reporting a door held open alarm, shall be configurable from zero to one-hundred-twenty-seven (0 - 127) seconds.

e. Door relock after a valid card read shall be configurable to support the following:
   1) Lock on duration.
   2) Lock on open.
   3) Lock on close.

   f. **Reader / Door State:**
      1) Each reader shall support operating in a default online or offline state, allowing to be manually changed by an operator, or automatically under a time of day and day of week schedule.
      2) Each door shall support operating in a default locked or unlocked state, allowing to be automatically changed under a time of day and day of week schedule.

   g. **Reader Transaction Routing:**
      1) Transactions for valid, invalid, and lost cards from each reader shall be independently configured for default routing to history/archive, system printer, and/or all operator workstations.
      2) Valid card transaction from each reader shall be independently configured to support routing under time of day and day of week schedule to history, system printer, and/or all operator workstations.

   J. **Elevator Control:**
      1. The ISMS shall provide the ability to control access for calling of elevators cabs and selecting floor destination. The following elevator applications and configurations shall be supported:

      a. **Elevator Cab Access:** Elevator cab call buttons shall be illuminated and enabled for selection when valid access via reader is granted.

      b. **Floor Access:** Floor access shall be controlled via a reader located inside of each elevator cab; a minimum of sixty-four (64) floors serviced by elevator cab(s) shall be controlled. Floor access shall support the following:
1) **Non Floor Tracking:** when an authorized card is presented to the reader located inside the elevator cab, only the floor buttons for the cardholder’s corresponding assigned access will be illuminated and enabled for a user definable length of time to allow selection.

2) **Floor Tracking:** when an authorized card is presented to the reader located inside the elevator cab, the cardholder shall be allowed to enter a two (2) digit floor code on the reader’s keypad to which they have corresponding assigned access. The floor selected by the cardholder shall be a recorded transaction in the card history/archive database.

K. **Input/Output Control:**
   1. The ISMS shall allow control panel input and output points to be individually defined, configured, and controlled in the following manner:
      a. Input point(s) shall be user configurable for specific applications. The following application types shall be supported:
         1) **Alarm:** digital input used to trigger an alarm and any selected output.
         2) **Digital Output:** digital input used to trigger a selected input without alarm notification.
         3) **Elevator:** digital input used for elevator control.
         4) **Inactive:** digital input is disabled.
      b. Input point(s) shall support a user configurable sense time from zero to sixty-four (0 - 64) seconds. Sense time changes shall be supported via event schedules.
      c. Input point(s) shall allow the active state to be configured as open or closed.
      d. Input point(s) shall be user configurable to control a primary and/or secondary output. Input point(s) configured for output control shall allow being enabled or disabled via time schedule.
         1) The primary output shall be configurable to follow the input point’s state change or activate for its defined output duration.
         2) The secondary output shall be configurable to follow the input point’s state change or remain activated until manually reset or scheduled off.
      e. Output point(s) shall support a user configurable duration time from zero to sixty-four (0 - 64) seconds.
      f. Output point(s) shall allow the active state to be configured as on or off.
      g. Output point(s) shall be automatically controlled via time schedule to turn on or off.
      h. Output points shall allow grouping to facilitate activating multiple output points, on or off, via time schedule.
      i. Output point(s), including reader controlled doors, shall allow manual control by authorized operators in the following manner:
         1) Activate/unlock for duration.
         2) Activate/unlock indefinitely.
         3) Deactivate/Lock.
         4) Schedule override.
         5) Text entry explaining reason for manual operator control shall be recorded in operator history/archive database.

L. **Intrusion Control:**
   1. The ISMS shall provide the ability to define local intrusion zones that consist of
      a. One or more access control readers
      b. One or more alarm inputs
      c. An input point to designate arm or disarm status
      d. An output point to designate arm or disarm status
   2. The ISMS shall provide the ability to arm or disarm intrusion zones by a. Access control reader, using card and keypad
b. Digital Input state change

c. Manual Operator control

3. The ISMS shall provide the ability to arm or disarm intrusion zones from outside the protected area.
   a. Readers assigned to an armed intrusion zone shall deny access to card holders unless the intrusion zone is disarmed.
   b. Readers assigned to an intrusion zone shall flash LED indicators on the reader to annunciate the intrusion zone status.
   c. Cards shall be authorized as to which intrusion zones they can arm and disarm.
   d. Users of the system will enter keypad information to tell the system to arm or disarm and then they will present their card.
   e. If the user is authorized to arm zone, and they have an active access right for the reader, then the intrusion zone shall be armed and any readers associated with the intrusion zone (other than the arm/disarm reader) shall be placed offline, any inputs associated with the intrusion zone shall be monitored on. An output shall be able to be generated based on the arm event. A history record shall be generated for this event.
   f. If the user is authorized to disarm the intrusion zone, and they have an active access right for the reader, then the intrusion zone shall be disarmed and all readers associated with the intrusion zone will return to normal operation, any inputs associated with the intrusion zone shall be monitored off. An output shall be able to be generated based on the disarm event. A history record shall be generated for this event.
   g. If the user is not authorized to disarm the intrusion zone, but the user has an active access right for the reader, then access will be denied, and a history record shall be generated.

4. The ISMS shall provide the ability to arm or disarm intrusion zones by manual control
   a. A properly permissioned operator shall be able to manually arm or disarm an intrusion zone
   b. Intrusion zone shall be partitioned to limit restrict which operator can view which intrusion zones.

M. Alarm Management:
   1. The ISMS shall allow alarms to be individually defined, configured, and controlled in the following manner:
      a. Configure if monitoring of the alarm is enabled or disabled. An alarm shall allow monitoring to be controlled manually by an authorized operator and automatically via time schedule.
      b. Configure if operator acknowledgement of the alarm is required before the alarm can be cleared from the alarm monitor window from any operator workstation.
      c. Ten (10) priority levels for prioritizing the processing and display of alarms.
      d. Configure if remotely connected control panels via modem, shall initiate communications to the host server to report the alarm condition.
      e. Configure if the alarm shall be routed to the history/archive database and/or printed on a host/server alarm printer.
      f. User definable instructions shall be assignable to each alarm, required to display in the alarm monitor window at all operator workstations for alarm assessment and response.
      g. Alarm(s) shall be user configurable to trigger a primary and/or secondary output.
         1) The primary output shall be configurable to follow the alarm’s state change or activate for its defined output duration.
         2) The secondary output shall be configurable to follow the alarm’s state change or remain activated until manually reset or scheduled off.
h. Alarms shall allow grouping to facilitate monitoring multiple alarms, on or off, via time schedule and changing alarm sense times via event schedules.

i. Alarms shall support regrouping via event schedules, allowing alarms to be reassigned to different alarm groups.

N. System Monitoring: The ISMS shall provide multiple monitoring application windows dedicated for displaying real-time information of ISMS card access and alarm activity as well as control panel and operator workstation status.

1. Card Access Activity Monitor: shall display card access activity from all ISMS readers that are online, active, and configured to route to monitor. The monitor window shall provide operator controls to clear, pause, and resume scrolling display of card access activity. The following card access activity information shall be displayed:
   a. Transaction date & time
   b. Transaction types:
      1) Valid.
      2) Invalid.
      3) Lost.
      4) Unknown.
      5) Anti-Passback IN invalid.
      6) Anti-Passback OUT invalid.
      7) Time & Attendance IN invalid.
      8) Time & Attendance OUT invalid.
      9) Valid floor.
     10) Invalid floor.
     11) Card ID number for unknown or unassigned cards.
     12) Floor selection for elevator control.
   c. Reader description
   d. Cardholder name

2. Alarm Activity Monitor: shall display alarm activity for all ISMS alarms configured or scheduled as monitored. The alarm activity monitor shall provide alarm notification and interaction for alarm assessment including acknowledgement and response. All operator acknowledgements and responses shall be recorded in the operator and alarm history/archive database. The following alarm activity information shall be displayed:
   a. Priority.
   b. Description (to be provided by owner)
   c. Reference type or additional alarm information.
   d. Alarm state:
      1) Alarm.
      2) Reset.
      3) Cut.
      4) Short.
   e. Process state:
      1) Acknowledged.
      2) Unacknowledged.
   f. Occurrence Count.
   g. Host date and time.
   h. Control panel date and time.
   i. Predefined alarm instructions for operator assessment.
   j. Entry for operator alarm response in free form text or from pick list of predefined alarm responses.
   k. Acknowledgement button.
3. **Alarm Graphics Monitor:** shall graphically display alarm states represented by icons located on multilayer map views. The alarm graphics monitor shall support and provide the following:
   a. Importing and scaling of maps in Windows standard Metafile (WMF) or Enhanced Metafile (EMF) formats.
   b. Provide an icon database and the ability to import images in (ICO) format into the icon database.
   c. Associate icons with map views, alarm points, and alarm states.
   d. Navigate between map views.
   e. Bidirectional navigation between alarm graphics monitor and alarm activity monitor.

4. **Control Panel Monitor:** shall provide communications status and manual control of all ISMS control panels. The control panel monitor shall support and provide the following:
   a. Display control panel properties, firmware version, and communications status.
   b. The ability to remotely reset, configure online/offline, force database downloads, and update control panel firmware.

5. **Operator Workstation Monitor:** shall provide communications status and connectivity control of all ISMS operator workstations.

6. **Database Reporting:** The ISMS shall provide online database reporting without degrading system performance. The following reporting functions and capabilities shall be supported:
   1. Predefined reports with the ability to create and save user definable templates for grouping, sorting, and filtering data. A minimum number of predefined reports shall be furnished covering the following topics:
      a. Cardholder and card ID information.
      b. System administration and device configurations.
      c. System schedules and events.
      d. Reader access.
      e. Floor access.
      f. Roll call / Muster.
      g. Time and attendance.
      h. Alarm history.
      i. Badge history.
      j. Operator history.
   2. Reports shall allow operators to perform page setup, preview report online, print, and export reports to multiple file formats and destinations.
      a. Export file formats supported shall include:
         1) Crystal Reports.
         2) Data Interchange Format.
         3) Excel.
         4) HTML.
         5) Lotus.
         6) ODBC.
         7) Paginated Text.
         8) Report Definition.
         10) Tab Delimited Text.
         11) Unformatted Text.
         12) Word.
      b. Export destinations supported shall include:
         1) Disk File.
         2) Exchange Folder.
         3) Lotus Domino Database.
4) **Microsoft Mail**

3. The ISMS shall support direct database connectivity for facilitating report generation from external 3rd party database applications. The following applications shall be supported:
   a. Microsoft SQL Server.
   c. Web reporting interface to Crystal Reports for enterprise information delivery.

**P. Database Import Interface:** The ISMS shall support direct database connectivity for importing cardholder and card ID data from external systems and/or database applications. The ISMS shall facilitate interfacing by providing the following capabilities:
   1. Real-time and batch processing of data via ODBC over a network connection.
   2. Insert, update, and delete record information.
   3. Automatic download of data to ISMS control panels based on database changes.
   4. Provide audit trail in the operator history/archive database for all database changes initiated by the interface.

**Q. Video Surveillance Interface:** The ISMS shall support software interfacing with video surveillance systems for facilitating real-time response to monitored events processed by the ISMS.

1. **CCTV Matrix Switcher Interface:** The ISMS shall provide a Closed Circuit TV (CCTV) matrix switcher interface that supports the following functionality:
   a. Serial interface support via industry standard RS232 communications protocol.
   b. Interface with multiple CCTV matrix switchers locally and remotely, via ISMS host server and network connected operator workstations.
   c. The ability to define and assign CCTV “Enable”, “Disable”, and “Camera Alarm” messages to ISMS alarms.
   d. The ISMS shall process alarms and transmit applicable “Enable”, “Disable”, and “Camera Alarm” messages to the CCTV matrix switcher in real-time.
   e. The ISMS shall support a supervised bi-directional communications interface for receiving “video loss alarms” and detecting communication failure, should the specific CCTV matrix switcher interface provide that support.
   f. The ISMS shall support the following CCTV matrix switcher interfaces:
      1) American Dynamics 168 and 2150.
      2) PHILIPS/Burle Allegiant TC8500 to TC8901 series.
      3) Kalatel KTD 312 and 348.
      4) Pelco 9760.

2. **Digital Video Multiplexer/Recorder Interface:** The ISMS shall provide a fully integrated digital video multiplexer/recorder interface that supports the following functionality:
   a. Support network connectivity to multiple digital video multiplexer/recorders (DVMR) via ISMS host server and network connected operator workstations.
   b. The communications interface between the ISMS and all DVMR units shall be via 10/100Mb Ethernet connectivity using industry standard TCP/IP protocol.
   c. Define and assign CCTV cameras and presets to ISMS alarm and card access events; for real-time video event tagging and access to live and recorded video from any ISMS operator workstation.
   d. ISMS operators shall be able to simultaneously view and control multiple live video cameras across multiple DVMR units. Camera control shall be mouse driven on-screen and shall support pan, tilt, zoom, iris, focus, and preset call functions.
   e. ISMS operators shall be able to access and playback recorded video events. On-screen playback controls for recorded video events shall support play forward, play reverse, fast forward, fast reverse, single frame advance, single frame reverse, pause, and stop functions.
f. ISMS operators shall be able to quickly access live and pre-event recorded video in near real-time without requiring a database query search. Quick, near real-time access to video shall be available directly from ISMS card access and alarm monitoring application windows as tagged transactions are displayed.

g. Playback tagged video events stored locally on DVMR units, based on date, time, and event query search from ISMS history/archive database.

h. The ISMS shall support request for live and recorded video transmission from DVMR units at various resolutions and display sizes, independent of actual DVMR resolution setting for local recorded video. Such a feature shall be user configurable from the ISMS to facilitate network adaptability.

i. The DVMR interface shall not interfere with local operator control and monitoring of video surveillance systems.

j. The ISMS shall monitor status of all DVMR units for processing and reporting the following conditions:
   1) Online / Offline.
   2) Record status.
   3) Disk capacity status.
   4) Camera video loss.
   5) Camera alarm.

k. The ISMS shall support the following digital video multiplexer/recorders:
   1) Kalatel DVMRe 4 Channel Duplex and Triplex.
   2) Kalatel DVMRe 10 Channel Duplex and Triplex.
   3) Kalatel DVMRe 16 Channel Duplex and Triplex.

l. The ISMS shall support the following camera control protocols:
   1) Kalatel.
   2) Pelco.
   3) Panasonic.
   4) Checkpoint.

R. Web Reporting Interface: The ISMS shall support a web based reporting system which shall be available to any authorized user on the network.

   1. The web reporting shall be partitioned by facility
   2. The web reporting shall be accessed via username and password
   3. The web reporting shall provide pre-defined reports for
      a. Personnel Reports
      b. Badge Reports
      c. Device Configuration Reports
      d. System Configuration Reports
      e. Badge History Reports
      f. Alarm History Reports
      g. Operator History Reports
   4. The web reporting shall provide the ability to define new reports using tools similar to Crystal Report Designer.
   5. The web reporting shall provide the ability to save report configurations.
   6. The web reporting shall allow up to fifty (50) concurrent users

S. Application Program Interface: The ISMS shall support application programming interface (API), which allows authorized software connections between the ISMS and external systems. The API for the ISMS shall facilitate real-time response to monitored events processed by the ISMS.

   1. The ISMS shall only allow authorized connections through the API.
   2. The ISMS shall allow five (5) concurrent connections to external systems through the API.
3. The API for the ISMS shall expose these parts of the ISMS:
   a. Bi-directional alarm event processing for monitoring and acknowledgement
   b. Receiving ISMS badge events
   c. Receiving digital input events
   d. Receiving intrusion zone events
   e. Control of alarm point monitoring On/Off
   f. Control of digital input points Enable/Disable
   g. Control of digital output points Open/Close
   h. Control of intrusion zones Arm/Disarm

4. The manufacturer of the ISMS shall have a development support program that facilitates third party developers developing applications that integrate with the ISMS.
5. The manufacturer of the ISMS API shall have sample code available to support developers in their efforts to integrate with the ISMS.

2.4 SOFTWARE
2.4.1 Host Server Software:
   A Existing Software.

2.4.2 Operator Workstation Software:
   A Existing Software.

2.4.3 Security Management Software:
   A Existing GE Interlogix, CASI Secure Perfect 6.0.

2.5 HARDWARE
2.5.1 Host Server and Operator Workstations: Existing server and workstations.
2.5.2 Control Panels: GE Interlogix, Micro/5PXN. The ISMS control panels shall be intelligent and fully stand-alone processor capable, making all local access control and alarm monitoring decisions without host server dependency. Control panels shall support and provide the following:
   A. UL listed under UL 294 and UL 1076; FCC Part 15 and CE compliant.
   B. Direct on-board support for industry standard RS232, RS422, Dial-up modem AT command set, and 10/100Mb Ethernet communications interfaces to ISMS hosting server or operator workstations.
   C. Dual PCMCIA socket support for commercially available 10/100Mb Ethernet and modem PCMCIA cards.
   D. Support redundant communications to ISMS hosting server or operator workstations; primary communications via 10/100Mb Ethernet with automatic switchover to secondary communications via dial-up modem when detecting network failure.
   E. RS232 and RS422 communications ports for cascading/clustering multiple control panels via a single communications port interface to ISMS hosting server or operator workstations.
   F. Flashable memory support for facilitating remote firmware updates from ISMS host server and operator workstations; control panels shall remain on-line and operational during firmware update process.
   G. Control panel cabinet shall be of an industrial grade enclosure with knockouts for field wiring and have a key-locked and tamper protected door.
   H. Low voltage power supply with uninterruptible battery backup allowing continued operations for a minimum of two (2) hours at full load.

2.5.3 Control Panel Interfaces: The ISMS control panels shall support on board and/or expansion interface boards for access control readers, alarm monitoring, and input/output control. Control panels shall support and provide the following as required:
   1. Access Control Reader Interfaces:
      a. Shall support hard-wired connections to readers, including power and communications. Connections shall be supported at a minimum distance of two-
thousand (2,000) feet (or 610 meters) utilizing 22 AWG 2-pair shielded and unshielded cabling.
b. Shall support supervision, monitoring, and processing of the following:
   1) Reader tamper and communications.
   2) Status changes from locally wired door sensor and request to exit device.
c. Shall support card only and card-plus-keypad style readers of the following technologies:
   1) Proximity.
   2) Smart Card.
   3) Magnetic Stripe.
   4) Wiegand.
   5) Barcode.
   6) BaFe Touch.
   7) Biometrics.

 2. Input / Output Point Interfaces:
   a. Shall support 4-State supervised alarm inputs.
   b. Shall support relay and TTL level output points.

D. Access Control Card Readers:
   1. Reader Technology: As specified by selected card technology and application requirements; compatible with ISMS control panels and commercially available from industry leading manufactures that include but not limited to:
      a. GE Interlogix, CASI
      b. HID
      c. Motorola
      d. Other approved equals.
   2. The specified card and reader manufacturer shall support a full product line that offers multiple models and/or styles to fit various installation and application requirements including:
      a. Card only and card-plus-keypad style readers.
      b. Rugged, weatherized enclosures rated for indoor and outdoor mounting.
      c. Rated for mounting on metal and non-metal surfaces.
      d. Provide audible and visual indicators for reader status and validation of granted and denied access.
   3. Provide quantities for each model and/or style indicated on drawings.

E Electric Door Hardware:
   1. Electronic locking devices shall have a separate power supply to support the locks specified below. The unit shall incorporate integral battery charging capabilities and a fused line voltage input for a minimum of eight (8) individual locks. All power supplies shall be equipped with optional battery pack for up to forty-eight (48) hours. The unit shall be equipped with a module to accommodate fire alarm NC contacts when a fire alarm activates.
   2. All locks shall be fail-secure unless otherwise specified by the Security Consultant/Designer. Locks specified, as being fail-safe shall be installed in accordance to Section 5-2.1.6.2 of NFPA Life Safety Code 101.
   3. The SECURITY CONTRACTOR shall coordinate with the OWNER approved Fire Alarm and Sprinkler Contractors for the interconnection of the specified ISMS.
   4. Specified Products:
      a. Electric Strike: [Sargent or Von Duprin]*
      b. Magnetic Locks are not allowed on this campus unless pre approved in writing by the University Physical Plant.
c. Crash Bar: [Sargent or Von Duprin].*
d. Electric Mortise Lock: [Sargent or Von Duprin] *
   * Must be coordinated with the rest of building hardware.

5. Provide quantities for each model indicated on drawings.

F. Door Hardware Configuration:
1. Card access controlled doors shall be equipped with a passive infrared request-to-exit
device specifically designed for electromechanical lock release. Device shall be equipped
with a DPST (NO & NC) 1-amp contact.
2. Card access controlled doors shall be equipped with a non-illuminating emergency exit
button to momentarily deactivate the magnetic lock. The device shall be equipped with
DPDT contacts with one side sending a REX to the ISMS control panel and the other
directly interrupting power to the magnetic lock. The device shall fit into a single gang
electrical box.
3. Card access controlled doors shall be equipped with a touch sense exit device to
momentarily deactivate the magnetic locking device. The device shall be 24 VDC and
equipped with DPST (NC & NO) contacts.

G. Intrusion Detection Devices:
1. Door Sensor Contacts:
   a. Recessed magnetic door contacts shall be provided for all card access doors and
doors requiring intrusion detection. Door contacts shall be provided on single doors
and both leaves of double doors at locations indicated on drawings. Color to match
existing finish.
   b. Where building structure makes it impossible to install conduit within the wall or
doorframe, the SECURITY CONTRACTOR shall substitute surface-mount contacts
with armored cable for the specified contacts.
   c. Heavy-duty door contacts with armored cable shall be provided for all Roll-Up Doors
where indicated on the drawing.
   d. All devices shall be wired point to point and to the nearest ISMS control panel
interface.
2. Motion Detectors:
   a. WALL MOUNTED or CEILING MOUNTED passive infrared (PIR) motion detectors
shall be provided where indicated on drawings. Motion detectors shall be masked or
oriented to minimize the likelihood of nuisance alarms caused by environmental
conditions.
   b. All devices shall be wired point to point and to the nearest ISMS control panel
interface.
   c. A 12 VDC centralized power supply shall be utilized to power motion detectors.

PART 3 EXECUTION

3.1 SECURITY CONTRACTOR
A. The SECURITY CONTRACTOR shall be a local installation and service organization,
currently as a factory authorized representative by the manufacturer of the specified system.
B. The SECURITY CONTRACTOR shall provide a minimum of three (3) references whose
systems are of similar complexity and have installed and maintained by the SECURITY
CONTRACTOR in the last five (5) years.
C. At time of bid, the SECURITY CONTRACTOR shall be licensed by the state or local
jurisdiction to perform security work within the state. Contractors who have security licenses
or permits pending shall not be considered acceptable for bidding on this project.
D. The SECURITY CONTRACTOR shall assure that all personnel working on the project are
registered with the state or local jurisdiction Systems Licensing Board as provided for by
Current state statutes.
E. At the time of bid, the SECURITY CONTRACTOR shall provide satisfactory evidence of liability insurance and Workmen’s Compensation coverage for employed personnel as required by law.

3.2 PROJECT MANAGEMENT
A. The SECURITY CONTRACTOR shall provide an on-site, factory-trained technician to assist, advice and manage installing personnel.
B. All of the SECURITY CONTRACTOR’S personnel and operating forces including subcontractors and delivery personnel, shall be made aware of, and shall comply at all times, with the regulations, project requirements, and directions of responsible OWNER personnel.

3.3 PERSONNEL
A. The SECURITY CONTRACTOR’S personnel shall be qualified to accomplish all work promptly and satisfactorily. The OWNER shall be advised in writing of all designated service and support personnel responsible for installation as well as pre and post warranty service.
B. The SECURITY CONTRACTOR’S shall provide proof that designated service and support personnel have successfully completed the appropriate level of both hardware and software training offered by the manufacturer for installation and maintenance of the specified system.
C. STUDENT, STAFF AND FACULTY INTERACTION: All technicians must uphold the highest level of professionalism. USF is an environment where unprofessional conduct is not tolerated. All company employees shall be identifiable by their name and company apparel clearly visible at all times.

3.4 ACCESS CONTROL SYSTEM - INSTALLATION
A. General: The contractor shall install all system components and appurtenances in accordance with the manufacturer’s instructions, and shall furnish all necessary interconnections, services, and adjustments required for a complete and operable system as specified and shown. 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. Provide mounting hardware as required.
B. Installation: All low voltage wiring outside the control console, cabinets, boxes, and similar enclosures, shall be plenum rated where required by code. Cable shall not be pulled into conduits or placed in raceways, compartments, outlet boxes, junction boxes, or similar fittings with other building wiring.
C. Device Wiring and Communication Circuit Surge Protection: All inputs shall be protected against surges induced on device wiring. Outputs shall be protected against surges induced on control and device wiring installed outdoors and as shown. All communications equipment shall be protected against surges induced on any communications circuit. All cables and conductors, except fiber optics, which serve as communications circuits from security console to field equipment, and between field equipment, shall have surge protection circuits installed at each end.
D. All low voltage wiring outside the control console, cabinets, boxes, and similar enclosures, shall be plenum rated where required by code.
E. All wiring conductors connected to terminal strips shall be wired individually. Each cable or wiring group being extended from a panel or cabinet to a building mounted device shall be identified with the name and name of the particular device as identified and shown on building drawings.
F. All exposed wiring inside and outside the control console, cabinets, boxes, and similar enclosures, shall be dressed down neatly and secures with wiring cleats or wire ties.
G. All exposed metallic flexible conduit and armored cable shall be dressed down neatly and secured with low profile, metal fasteners.
H. All cabinets, boxes, and similar enclosures containing security system components and/or cabling and which are accessible to employees or to the public shall be provided with a lock.
Boxes above ceiling level in occupied areas of building shall not be considered to be accessible.

I. All junction boxes and small device enclosures below ceiling level and easily accessible to employees or the public shall be covered with a suitable cover plate and secured with tamper proof screws.

J. End -of-line resistors shall be installed at the field device location and not at the controller panel location.

K. System devices identified on building drawings are intended to generally indicate areas where such devices are to be located. Security Contractor shall be responsible for determining final location of these devices in accordance with OWNER’S requirements.

L. Riser diagrams are schematic and do not show every conduit, wire box, fitting, or other accessories. Provide such materials as necessary for a complete and functioning installation. Install in accordance with referenced codes and these specifications. Use weatherproof equipment or covers where installed in areas exposed to weather.

M. All control wiring shall be labeled at both ends and wire label shall be indicated in as-built drawing.

3.5 COMMISSIONING AND TRAINING

A. General: The contractor shall conduct training courses for personnel designated by the owner. Training shall cover the maintenance and operation of the ISMS. The training shall be oriented to the specific system being installed under this contract including central processor. Training manuals shall be delivered for each trainee with two additional copies delivered for archiving at the project site. The manuals shall include an agenda, defined objectives for each lesson, and a detailed description of the subject matter for each lesson. The contractor shall furnish audiovisual equipment and other training materials and supplies as necessary. Where the contractor presents portions of the course by audiovisual material, copies of the audiovisual material shall be delivered to the owner on the same media as that used during the training session. Up to forty (40) hours of training shall be provided for in the base contract.

3.6 TESTING

A. General: The contractor shall perform pre-delivery testing, site testing, and adjustment of the completed ISMS. The contractor shall provide all personnel, equipment, instrumentation, and supplies necessary to perform all testing. Written notification of planned testing shall be given to the owner at least fourteen (14) days prior to the test and in no case shall notice be given until after the contractor has received written approval of the specific test procedures? Test procedures shall explain in detail, step-by-step actions and expected results demonstrating compliance with the requirements of the specification. Test reports shall be used to document results of the tests. Reports shall be delivered to the owner within seven (7) days after completion of each test. The test procedures are determined and written by the A/E.

B. Performance Verification Test: The contractor shall demonstrate that the completed ISMS complies with the contract requirements. Using approved test procedures, all physical and functional requirements of the project shall be demonstrated and shown.

C. The SECURITY CONTRACTOR is required to place entire system into full and proper operation as designed and specified.

1. Verify that all hardware components are installed properly, connected, communicating, and operating correctly.
2. Verify that all system software is installed, configured, and complies with specified functional requirements.

D. The SECURITY CONTRACTOR shall 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.
1. Submit documented test plan to CM/A&E/OWNER at least fourteen (14) days in advance of acceptance test, inspection and check-off.

2. 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.

3. Acceptance by OWNER is contingent on successful completion of check-off; is check-off not completed due to additional work required, re-scheduled and perform complete check-off until complete in one pass, unless portions of systems can be verified as not affected by additional work. Industry standard is for the architect to determine substantially complete, which includes beneficial occupancy.

4. The 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.

E. The SECURITY CONTRACTOR shall provide system operations, administration, and maintenance training by factory trained personnel qualified to instruct:

1. OWNER will designate personnel to be trained.
2. Provide printed training materials for each trainee including product manuals, course outline, workbook or student guides, and written examinations for certifications.
3. Provide hands-on training with operational equipment.
4. Training shall be oriented to the specific system being installed under this contract as designed and specified.

3.7 WARRANTY, MAINTENANCE AND SERVICE

A. Warranty: The ISMS shall be warranted by the contractor for one (1) year from the date of final system acceptance/substantial completion.

B. Maintenance and Service: The contractor shall provide all services required and equipment necessary to maintain the entire ISMS in an operational state as specified for a period of one (1) year after formal written acceptance of the system, and shall provide all necessary material required for performing scheduled adjustments or other nonscheduled work.

C Description of Work: The adjustment and repair of ISMS includes computer equipment, software updates, signal transmission equipment, access control equipment, facility interfaces, and support equipment. Responsibility shall be limited to contractor installed equipment. Provide the manufacturers required adjustments and other work as necessary.

D Personnel: Service personnel shall be qualified to accomplish all work promptly and satisfactorily. Provide proof that Service personnel have successfully completed the appropriate level of both hardware and software training offered by the system manufacturer. The owner shall be advised in writing of the name of the designated service representative and of any change in personnel.

E Inspections: The contractor shall perform two inspections at six (6) month intervals or more often if required by the manufacturers. This work shall be performed during regular working hours, Monday through Friday, excluding Federal holidays. These inspections shall include:

1. Visual checks and operational tests of the central processor, local processors, monitors, keyboards, system printers, peripheral equipment, ISMS equipment, power supplies, and electrical and mechanical controls.
2. Clean system equipment, including interior and exterior surfaces.
3. Perform diagnostics on all equipment.
4. Check and calibrate each ISMS device.
5. Run system software and correct diagnosed problems.
6. Resolve previous outstanding problems.

F Emergency Service: The owner shall initiate service calls when the ISMS is not functioning properly. Qualified personnel shall be available to provide service to the complete SMCS. The owner shall be furnished with the telephone number where the contractor’s service supervisor can be reached at all times. Service personnel shall be at the site within four (4)
hours after receiving a request for service. The ISMS shall be restored to proper operating condition after one (1) calendar day.

G Software: Existing USF software.