SECTION 28 1300
ACCESS CONTROL

PART 1 GENERAL

1.01 RELATED DOCUMENTS

A. Drawings and general provisions of the Contract, including General and Supplementary Conditions and Division 01 Specification Sections, apply to this Section.

1.02 SUMMARY

A. This Section includes a security access system consisting of a Central Station, operating system and application software, and field-installed Controllers connected by a high-speed electronic data transmission network. The security access system shall have the following:
   1. Access Control:
      a. Regulating access through doors and gates specified by Spectrum Physical Security Team.
      b. Surge and tamper protection.
      c. Secondary alarm annunciator.
      d. Credential cards and readers.
      e. RS-232 ASCII interface.
      f. Monitoring of field-installed devices.
      g. Reporting.

B. Related Sections include the following:
   1. Division 28 Section "Video Surveillance" for interface devices and communications protocol to integrate motion detection and video camera selection and positioning into security access system.

1.03 DEFINITIONS

A. ABA Track: Magnetic stripe that is encoded on track 2, at 75-bpi density in binary-coded decimal format; for example, 5-bit, 16-character set.

B. CCTV: Closed-circuit television.

C. Central Station: A PC with software designated as the main controlling PC of the security access system. Where this term is presented with initial capital letters, this definition applies.

D. Controller: An intelligent peripheral control unit that uses a computer for controlling its operation. Where this term is presented with an initial capital letter, this definition applies.

E. CPU: Central processing unit.

F. Credential: Data assigned to an entity and used to identify that entity.

G. dpi: Dots per inch.

H. DTS: Digital Termination Service: A microwave-based, line-of-sight communications provided directly to the end user.

I. File Server: A secure server-based access control network.

J. GFI: Ground fault interrupter.

K. Identifier: A credential card, keypad personal identification number or code, biometric characteristic, or other unique identification entered as data into the entry-control database for the purpose of identifying an individual. Where this term is presented with an initial capital letter, this definition applies.

L. I/O: Input/Output.

M. LAN: Local area network.

N. LED: Light-emitting diode.

O. Location: A Location on the network having a PC-to-Controller communications link, with additional Controllers at the Location connected to the PC-to-Controller link with RS-485 communications loop. Where this term is presented with an initial capital letter, this definition

applies.

P. PC: Personal computer. This acronym applies to the Central Station, workstations.

Q. PCI Bus: Peripheral component interconnect; a peripheral bus providing a high-speed data path between the CPU and peripheral devices (such as monitor, disk drive, or network).

R. PDF: (Portable Document Format.) The file format used by the Acrobat document exchange system software from Adobe.

S. RF: Radio frequency.

T. ROM: Read-only memory. ROM data are maintained through losses of power.

U. RS-232: An TIA/EIA standard for asynchronous serial data communications between terminal devices. This standard defines a 25-pin connector and certain signal characteristics for interfacing computer equipment.

V. RS-485: An TIA/EIA standard for multipoint communications.

W. TCP/IP: Transport control protocol/Internet protocol incorporated into Microsoft Windows.

X. TWAIN: (Technology without an Interesting Name.) A programming interface that lets a graphics application, such as an image editing program or desktop publishing program, activate a scanner, frame grabber, or other image-capturing device.

Y. UPS: Uninterruptible power supply.

Z. WAN: Wide area network.

AA. WAV: The digital audio format used in Microsoft Windows.

BB. Wiegand: Patented magnetic principle that uses specially treated wires embedded in the credential card.

CC. Windows: Operating system by Microsoft Corporation.

DD. Workstation: A PC with software that is configured for specific limited security system functions.

EE. WYSIWYG: (What You See Is What You Get.) Text and graphics appear on the screen the same as they will print.

1.04 SYSTEM DESCRIPTION

A. System shall be the extension of the proprietary access control system, and field-installed Controllers, connected by a high-speed electronic data transmission network.
   1. System Software: Maintained by the the system owner.

B. Network connecting the Central Station and controllers shall be a WAN using Microsoft Windows-based TCP/IP with a capacity of connecting up to 99 workstations.

C. Network(s) connecting Controllers shall consist of one or more of the following:
   1. Local area, IEEE 802.3 Fast Ethernet 10 BASE-T, star topology network based on TCP/IP.

1.05 PERFORMANCE REQUIREMENTS

A. Security access system shall use a single database for access-control and credential-creation functions.

B. Distributed Processing: System shall be a fully distributed processing system so that information, including time, date, valid codes, access levels, and similar data, is downloaded to Controllers so that each Controller makes access-control decisions for that Location. Do not use intermediate Controllers for access control. If communications to Central Station are lost, all Controllers shall automatically buffer event transactions until communications are restored, at which time buffered events shall be uploaded to the Central Station.

C. System Network Requirements:
   1. Interconnect system components and provide automatic communication of status changes, commands, field-initiated interrupts, and other communications required for proper system operation.

2. Communication shall not require operator initiation or response, and shall return to normal after partial or total network interruption such as power loss or transient upset.
3. System shall automatically annunciate communication failures to the operator and identify the communication link that has experienced a partial or total failure.
4. Communications Controller may be used as an interface between the Central Station display systems and the field device network. Communications Controller shall provide functions required to attain the specified network communications performance.

D. Central Station shall provide operator interface, interaction, display, control, and dynamic and real-time monitoring. Central Station shall control system networks to interconnect all system components, including workstations and field-installed Controllers.

E. Field equipment shall include Controllers, sensors, and controls. Controllers shall serve as an interface between the Central Station and sensors and controls. Data exchange between the Central Station and the Controllers shall include down-line transmission of commands, software, and databases to Controllers. The up-line data exchange from the Controller to the Central Station shall include status data such as intrusion alarms, status reports, and entry-control records. Controllers are classified as alarm-annunciation or entry-control type.

F. System Response to Alarms: Field device network shall provide a system end-to-end response time of 1 second or less for every device connected to the system. Alarms shall be annunciated at the Central Station within 1 second of the alarm occurring at a Controller or device controlled by a local Controller, and within 100 ms if the alarm occurs at the Central Station. Alarm and status changes shall be displayed within 100 ms after receipt of data by the Central Station. All graphics shall be displayed, including graphics-generated map displays, on the console monitor within 5 seconds of alarm receipt at the security console. This response time shall be maintained during system heavy load.

G. Data Line Supervision: System shall initiate an alarm in response to opening, closing, shorting, or grounding of data transmission lines.

H. Door Hardware Interface: Coordinate with Division 08 Sections that specify door hardware required to be monitored or controlled by the security access system. The Controllers in this Section shall have electrical characteristics that match the signal and power requirements of door hardware. Integrate door hardware specified in Division 08 Sections to function with th e controls and PC-based software and hardware in this Section.

1.06 SUBMITTALS

A. Product Data: For each type of product indicated. Include operating characteristics, furnished specialties, and accessories. Reference each product to a location on Drawings. Test and evaluation data presented in Product Data shall comply with SIA BIO-01.

B. Shop Drawings:
1. Diagrams for cable management system.
2. System labeling schedules, including electronic copy of labeling schedules that are part of the cable and asset identification system of the software specified in Parts 2 and 3.
3. Wiring Diagrams. Show typical wiring schematics including the following:
   a. Workstation outlets, jacks, and jack assemblies.
   b. Patch cords.
   c. Patch panels.
4. Cable Administration Drawings: As specified in Part 3 "Identification" Article.
5. Battery and charger calculations for Central Station, workstations, and Controllers.

C. Project planning documents as specified in Part 3.

D. Samples: For workstation outlets, jacks, jack assemblies, and faceplates for color selection and evaluation of technical features.

E. Field quality-control test reports.

F. Operation and Maintenance Data: For security system to include in emergency, operation, and maintenance manuals. In addition to items specified in Division 01 Section "Operation and Maintenance Data" include the following:

1. Microsoft Windows software documentation.
2. PC installation and operating documentation, manuals, and software for the PC and all installed peripherals. Software shall include system restore, emergency boot diskettes, and drivers for all installed hardware. Provide separately for each PC.
3. Hard copies of manufacturer's specification sheets, operating specifications, design guides, user's guides for software and hardware, and PDF files on CD-ROM of the hard-copy submittal.
4. System installation and setup guides, with data forms to plan and record options and setup decisions.

1.07 QUALITY ASSURANCE

A. Installer Qualifications: An employer of workers trained and approved by manufacturer.
   1. Cable installer must have on staff a registered communication distribution designer certified by Building Industry Consulting Service International.

B. Testing Agency Qualifications: An independent agency, with the experience and capability to conduct the testing indicated, that is a nationally recognized testing laboratory (NRTL) as defined by OSHA in 29 CFR 1910.7, and that is acceptable to authorities having jurisdiction.

C. Source Limitations: Obtain Central Station, workstations, Controllers, Identifier readers, and all software through one source from a single manufacturer.

D. Electrical Components, Devices, and Accessories: Listed and labeled as defined in NFPA 70, Article 100, by a testing agency acceptable to authorities having jurisdiction, and marked for intended use.

E. Comply with NFPA 70, "National Electrical Code."

F. Comply with [SIA DC-01 and]SIA DC-03[and SIA DC-07].

1.08 DELIVERY, STORAGE, AND HANDLING

A. Central Station, Workstations, and Controllers:
   1. Store in temperature- and humidity-controlled environment in original manufacturer's sealed containers. Maintain ambient temperature between 50 and 85 deg F (10 and 30 deg C), and not more than 80 percent relative humidity, noncondensing.
   2. Open each container; verify contents against packing list, and file copy of packing list, complete with container identification for inclusion in operation and maintenance data.
   3. Mark packing list with designations that have been assigned to materials and equipment for recording in the system labeling schedules that are generated by cable and asset management system specified in Part 2.
   4. Save original manufacturer's containers and packing materials and deliver as directed under provisions covering extra materials.

1.09 PROJECT CONDITIONS

A. Environmental Conditions: System shall be capable of withstanding the following environmental conditions without mechanical or electrical damage or degradation of operating capability:
   1. Control Station: Rated for continuous operation in ambient conditions of 60 to 85 deg F (16 to 30 deg C) and a relative humidity of 20 to 80 percent, noncondensing.
   2. Interior, Controlled Environment: System components, except central-station control unit, installed in air-conditioned interior environments shall be rated for continuous operation in ambient conditions of 36 to 122 deg F (2 to 50 deg C) dry bulb and 20 to 90 percent relative humidity, noncondensing. NEMA 250, Type 1 enclosure.
   3. Interior, Uncontrolled Environment: System components installed in non-air-conditioned interior environments shall be rated for continuous operation in ambient conditions of 0 to 122 deg F (minus 18 to plus 50 deg C) dry bulb and 20 to 90 percent relative humidity, noncondensing. NEMA 250, Type 3R enclosures.
   4. Exterior Environment: System components installed in locations exposed to weather shall be rated for continuous operation in ambient conditions of minus 30 to plus 122 deg F (minus 34 to plus 50 deg C) dry bulb and 20 to 90 percent relative humidity, condensing.

Rate for continuous operation where exposed to rain as specified in NEMA 250, winds up to 85 mph (137 km/h) and snow cover up to 24 inches (610 mm) thick. NEMA 250, Type 3R enclosures.

1.10 WARRANTY AND WARRANTY SERVICE

A. Warranty
   1. The completed work as specified herein, including all materials and labor shall be warranted by the Security Contractor for a period of not less than one year from the date of acceptance, to be free from defects in design workmanship and materials. Parts having a manufacturer's warranty in excess of the one (1) year shall be warranted for the duration of the manufacturer's warranty. Further, the Security Contractor shall warrant that the completed systems including all components (except those which are NIC) are of sufficient size and capacity to fulfill satisfactorily the requirements of these specifications.
   2. The one year warranty period shall begin upon final acceptance of the completed work.
      a. For purposes of warranty consideration, the date of final acceptance shall be defined as the date on which the system test has been completed, the punch list items have been corrected, and all of the required documentation has been received and approved by the COTR and OPS. A memo of record from the Owner's representative shall formally acknowledge the acceptance of the completed work and the date of acceptance. The warranty will not begin on beneficial use of the system.
      b. In the event, corrective action on a reported defect has not been taken prior to the warranty expiration date, the warranty period shall be extended at no additional charge until all reported defects have been corrected.
      c. The contractor shall provide a statement indicating which items are covered by warranties in excess of the base contract requirement
   3. The Security Contractor shall not be responsible for repair or maintenance of any NIC equipment unless these systems or equipment have been specified as being part of this contract. The Security Contractor shall notify the Owner in writing if such equipment requires repairs to operate properly with the systems.
   4. The warranty shall include full preventative maintenance and service on all equipment, components and systems. Preventative maintenance shall include, at a minimum, quarterly inspections and servicing of all equipment to insure continued operation in accordance with manufacturers' specifications as well as the specifications stated herein. Visits shall be scheduled 72 hours in advance with the Smithsonian Institution Office of Protection Services.
   5. A manufacturers' software maintenance agreement shall be included with the one (1) year warranty period and shall include all software updates, revisions and telephone service assistance twenty four (24) hours per day, seven days per week.

B. Warranty Service
   1. In the event that defects in the materials and/or workmanship are identified during the warranty period, the Security Contractor shall provide all labor and materials as may be required for prompt correction of the defect at no additional cost to the Owner. The Security Contractor shall perform the correction of defects such that interruption of the Owner's normal business operations is minimized.
   2. During the warranty period, the Owner shall have the sole authority to determine if the failure is catastrophic or non-catastrophic. Catastrophic system failures are defined as any system failure that places Smithsonian Institution employees, collections or facilities at increased risk. The Security Contractor shall, upon receipt of a request for service from the Owner, have service personnel to the Owner's premises, repair and restore the device or equipment to service as follows:
      a. Catastrophic failures – Response shall be four (4) hours with a repair time not to exceed eight (8) hours. This response shall be in effect 24 hours per day, 7 days per week.
      b. Non-catastrophic failure - Response shall be eight (8) hours with a repair time not to exceed twenty-four (24) hours. This response shall be in effect during normal business hours that are defined as 7:30 AM to 5:00 PM Monday through Friday.

3. All warranty service and repair work shall be performed by personnel who have been manufacturer trained, certified and experienced in the operation and maintenance of the installed system(s).
    a. Warranty service shall include the replacement of any and all parts and/or components as required to restore normal system operation. In the event that the system parts or components must be removed for repair, it shall be the responsibility of the Security Contractor to furnish and install temporary parts and/or components as required to restore normal system operation until the repaired parts or components can be repaired or re-installed.
    b. It shall be the responsibility of the Security Contractor to maintain an inventory of spare parts or to arrange for manufacturers' parts support as required to insure correction of all critical component failures or malfunctions within twenty-four (24) hours of the Owner's request for service. Critical parts shall be defined as those, which govern or affect the normal operation of more than one (1) field device (card reader, electric lock, door position switch, etc.). The Security Contractor shall provide a list of recommended spare parts with his bid proposal.
    c. The Security Contractor's warranty obligation shall include correction of any software defects, which may be identified during the warranty period. Any failure of the software to perform as specified by the software manufacturer at the time of final acceptance shall be defined as a software error.
    d. In the event that the Security Contractor determines and successfully demonstrates to the Owner that service or repairs are required as a result of misuse, abuse or abnormal wear and tear, the Security Contractor shall be compensated for such service or repairs at the Security Contractor's hourly rates. Similarly, such compensation to the Security Contractor shall apply in the event that repairs are required for devices and equipment not provided by the Security Contractor but incorporated in the completed systems.
    e. Immediately following the completion of the warranty repair or service call, the Security Contractor's service personnel shall submit a written report to the Owner which details the service work performed, the cause of the trouble and any outstanding work which is required to restore complete and normal operation. Owner personnel must sign off on all repair or service calls to verify completion of work.

1.11 EXTRA MATERIALS

A. Furnish extra materials described below that match products installed and that are packaged with protective covering for storage and identified with labels describing contents.
    1. Fuses of all kinds, power and electronic, equal to 10 percent of amount installed for each size used, but no fewer than three units.

PART 2 PRODUCTS

2.01 MANUFACTURERS

A. In other Part 2 articles where titles below introduce lists, the following requirements apply to product selection:
    1. Manufacturers: Subject to compliance with requirements, provide products by one of the manufacturers specified.

2.02 SECURITY ACCESS SYSTEM

A. Manufacturers:
    1. Andover Continuum.

2.03 APPLICATION SOFTWARE

A. System Software: Maintained by the system owner.

B. Workstation Software:
    1. Password levels shall be individually customized at each workstation to allow or disallow operator access to program functions for each Location.
    2. Workstation event filtering shall allow user to define events and alarms that will be displayed at each workstation. If an alarm is unacknowledged (not handled by another

workstation) for a preset amount of time, the alarm will automatically appear on the filtered workstation.

C. Controller Software:
   1. Controllers shall operate as an autonomous intelligent processing unit. Controllers shall make decisions about access control, alarm monitoring, linking functions, and door locking schedules for its operation, independent of other system components. Controllers shall be part of a fully distributed processing control network. The portion of the database associated with a Controller and consisting of parameters, constraints, and the latest value or status of points connected to that Controller, shall be maintained in the Controller.
   2. Functions: The following functions shall be fully implemented and operational within each Controller:
      a. Monitoring inputs.
      b. Controlling outputs.
      c. Automatically reporting alarms to the Central Station.
      d. Reporting of sensor and output status to Central Station on request.
      e. Maintaining real time, automatically updated by the Central Station at least once a day.
      f. Communicating with the Central Station.
      g. Executing Controller resident programs.
      h. Diagnosing.
      i. Downloading and uploading data to and from the Central Station.
   3. Controller Operations at a Location:
      a. Location: Up to 100 Controllers connected to RS-485 communications loop. Globally operating I/O linking and anti-passback functions between Controllers within the same Location without central-station or workstation intervention. Linking and anti-passback shall remain fully functional within the same Location even when the Central Station or workstations are off line.
      b. In the event of communications failure between the Central Station and a Location, there shall be no degradation in operations at the Controllers at that Location. The Controllers at each Location shall be connected to a memory buffer with a capacity to store a minumum of 1,000 events; there shall be no loss of transactions in system history files until the buffer overflows.
      c. Buffered events shall be handled in a first-in-first-out mode of operation.
   4. Individual Controller Operation:
      a. Controllers shall transmit alarms, status changes, and other data to the Central Station when communications circuits are operable. If communications are not available, Controllers shall function in a stand-alone mode and operational data, including the status and alarm data normally transmitted to the Central Station, shall be stored for later transmission to the Central Station. Storage capacity for the latest 1000 events shall be provided at each Controller.
      b. Card-reader ports of a Controller shall be custom configurable for at least 120 different card-reader or keypad formats. Multiple reader or keypad formats may be used simultaneously at different Controllers or within the same Controller.
      c. Controllers shall provide a response to card-readers or keypad entries in less than 0.25 seconds, regardless of system size.
      d. Controllers that are reset, or powered up from a nonpowered state, shall automatically request a parameter download and reboot to its proper working state. This shall happen without any operator intervention.
      e. Initial Startup: When Controllers are brought on-line, database parameters shall be automatically downloaded to them. After initial download is completed, only database changes shall be downloaded to each Controller.
      f. Failure Mode: On failure for any reason, Controllers shall perform an orderly shutdown and force Controller outputs to a predetermined failure mode state, consistent with the failure modes shown and the associated control device.
      g. Startup After Power Failure: After power is restored, startup software shall initiate self-test diagnostic routines, after which Controllers shall resume normal operation.

h. Startup After Controller Failure: On failure, if the database and application software are no longer resident, Controllers shall not restart, but shall remain in the failure mode until repaired. If database and application programs are resident, Controllers shall immediately resume operation. If not, software shall be restored automatically from the Central Station.

5. Communications Monitoring:
   a. System shall monitor and report status of RS-485 communications loop of each Location.
   b. Communication status window shall display which Controllers are currently communicating, a total count of missed polls since midnight, and which Controller last missed a poll.
   c. System shall report communication loss of controllers and controller modules as critical alarms.
   d. Communication status window shall show the type of CPU, the type of I/O board, and the amount of RAM memory for each Controller.
6. Operating systems shall include a real-time clock function that maintains seconds, minutes, hours, day, date, and month. The real-time clock shall be automatically synchronized with the Central Station at least once a day to plus or minus 10 seconds. The time synchronization shall be automatic, without operator action and without requiring system shutdown.

D. Controller-to-Controller Communications:
1. Controller-to-Controller Communications: RS-485, 4 or 6-wire, point-to-point, regenerative (repeater) communications network methodology.
2. RS-485 communications signal shall be regenerated at each Controller.

2.04 SYSTEM DATABASE

A. Database and database management software shall be maintained by owner.

2.05 SURGE AND TAMPER PROTECTION

A. Surge Protection: Protect components from voltage surges originating external to equipment housing and entering through power, communication, signal, control, or sensing leads. Include surge protection for external wiring of each conductor-entry connection to components.
1. Minimum Protection for Power Connections 120 V and More: Auxiliary panel suppressors complying with requirements in Division 26 Section "Transient-Voltage Suppression for Low-Voltage Electrical Power Circuits."
2. Minimum Protection for Communication, Signal, Control, and Low-Voltage Power Connections: Comply with requirements in Division 26 Section "Transient-Voltage Suppression for Low-Voltage Electrical Power Circuits" as recommended by manufacturer for type of line being protected.

B. Tamper Protection: Tamper switches on enclosures, control units, pull boxes, junction boxes, cabinets, and other system components shall initiate a tamper-alarm signal when unit is opened or partially disassembled. Control-station control-unit alarm display shall identify tamper alarms and indicate locations.

2.06 CENTRAL-STATION HARDWARE

A. Maintained by Owner.

2.07 CONTROLLERS

A. Controllers: Intelligent peripheral control unit, complying with UL 294, that stores time, date, valid codes, access levels, and similar data downloaded from the Central Station or workstation for controlling its operation.

B. Subject to compliance with requirements in this Article, manufacturers may use multipurpose Controllers.

C. Battery Backup: Sealed, lead acid; sized to provide run time during a power outage of 90 minutes, complying with UL 924 .

D. Alarm Annunciation Controller:

1. The Controller shall automatically restore communication within 10 seconds after an interruption with the field device network[with dc line supervision on each of its alarm inputs].
    a. Inputs: Monitor dry contacts for changes of state that reflect alarm conditions. Provides at least eight alarm inputs, which are suitable for wiring as normally open or normally closed contacts for alarm conditions.
    b. Alarm-Line Supervision:
        1) Supervise the alarm lines by monitoring each circuit for changes or disturbances in the signal[, and for conditions as described in UL 1076 for line security equipment] [by monitoring for abnormal open, grounded, or shorted conditions] using dc change measurements. System shall initiate an alarm in response to an abnormal current, which is a dc change of 5 percent or more for longer than 500 ms.
        2) Transmit alarm-line-supervision alarm to the Central Station during the next interrogation cycle after the abnormal current condition.
    c. Outputs: Managed by Central Station software.
2. Auxiliary Equipment Power: A GFI service outlet inside the Controller enclosure.

E. Entry-Control Controller:
1. Function: Provide local entry-control functions including one- and two-way communications with access-control devices such as card readers, keypads, biometric personal identity verification devices, door strikes, magnetic latches, gate and door operators, and exit push-buttons.
    a. Operate as a stand-alone portal Controller using the downloaded database during periods of communication loss between the Controller and the field-device network.
    b. Accept information generated by the entry-control devices; automatically process this information to determine valid identification of the individual present at the portal:
        1) On authentication of the credentials or information presented, check privileges of the identified individual, allowing only those actions granted as privileges.
        2) Privileges shall include, but not be limited to, time of day control, day of week control, group control, and visitor escort control.
    c. Maintain a date-, time-, and Location-stamped record of each transaction. A transaction is defined as any successful or unsuccessful attempt to gain access through a controlled portal by the presentation of credentials or other identifying information.
2. Processor:
    a. Model # NC2-R-000000000.
3. Access Controlled Entry Points:
    a. Card Reader or Keypad.
    b. Card and Reader Formats 240+ including FIPS/TWIC
4. Data Line Problems: For periods of loss of communications with Central Station, or when data transmission is degraded and generating continuous checksum errors, the Controller shall continue to control entry by accepting identifying information, making authentication decisions, checking privileges, and controlling portal-control devices.
    a. Store up to 1000 transactions during periods of communication loss between the Controller and access-control devices for subsequent upload to the Central Station on restoration of communication.
5. Controller Power: NFPA 70, Class II power supply transformer, with 12- or 24-V ac secondary, backup battery and charger.
    a. Backup Battery: Premium, valve-regulated, recombinant-sealed, lead-calcium battery; spill proof; with a full 1-year warranty and a pro rata 19-year warranty. With single-stage, constant-voltage-current, limited battery charger, comply with battery manufacturer's written instructions for battery terminal voltage and charging current recommendations for maximum battery life.
    b. Backup Battery: Valve-regulated, recombinant-sealed, lead-acid battery; spill proof. With single-stage, constant-voltage-current, limited battery charger, comply with battery manufacturer's written instructions for battery terminal voltage and charging

current recommendations for maximum battery life.

c. Backup Power Supply Capacity: 90 minutes of battery supply. Submit battery and charger calculations.

d. Power Monitoring: Provide manual dynamic battery load test, with automatic disconnection of the Controller when battery voltage drops below Controller limits. Report by using local Controller-mounted LEDs and by communicating status to Central Station. Indicate normal power on and battery charger on trickle charge. Indicate and report the following:
   1) Trouble Alarm: Normal power off load assumed by battery.
   2) Trouble Alarm: Low battery.
   3) Alarm: Power off.

6. Controller shall be Andover Continuum Netcontroller II ~~DSX Model 1048~~

2.08 SECONDARY ALARM ANNUNCIATOR

A. Secondary Alarm Annunciation Site: A workstation with limited I/O capacity, consisting of a secondary alarm annunciation workstation [to allow the operator to duplicate functions of the main operator interface, and to show system status changes] [to display alarms or system status changes only].

2.09 CARD READERS

A. Power: Card reader shall be powered from its associated Controller, including its standby power source.

B. Response Time: Card reader shall respond to passage requests by generating a signal that is sent to the Controller. Response time shall be 800 ms or less, from the time the card reader finishes reading the credential card until a response signal is generated.

C. Enclosure: Suitable for surface, semiflush, or pedestal mounting. Mounting types shall additionally be suitable for installation in the following locations:
   1. Indoors, controlled environment.
   2. Indoors, uncontrolled environment.
   3. Outdoors, with built-in heaters or other cold-weather equipment to extend the operating temperature range as needed for operation at the site.

D. Display: LED or other type of visual indicator display shall provide visual[and audible] status indications and user prompts. Indicate power on/off, whether user passage requests have been accepted or rejected, and whether the door is locked or unlocked.

E. Dual Factor Authentication Read and/or Read/Write Only Multi-technology Contactless Smart Card reader iCLASS SE RK40, SE R40, SE R10, or SE R15 Reader
   1. Multi-technology contactless smart card reader shall read access control data from both 125 kHz and 13.56 MHz contactless smart cards. The multi-technology contactless smart card reader shall be optimally designed for use in access control applications that require reading both 125 kHz Proximity and 13.56 MHz contactless smart cards by providing:
   2. Unique read selection that enables iCLASS, proximity, or both technologies at the same time.
   3. Dual authentication of identity supported through combined contactless card presentation and entry of personal identification number (PIN) through an integrated 12-key keypad in highly sensitive areas specified by the Spectrum Physical Security Team.
   4. A migration platform to upgrade from the most popular 125 kHz proximity technologies to iCLASS by reading both 125 kHz proximity technology and 13.56 MHz contactless smart card technology.
   5. Guaranteed compatibility to read all HID data formats and ensuring card-to-reader interoperability in multi-location installations and multi-card/reader populations when used with Genuine HID products
   6. Secure access control data exchange between the smart card and the reader utilizing key diversification and mutual authentication routines.
   7. Universal compatibility with most access control systems.
   8. Ease of installation through identical wiring methods as legacy 125 KHz proximity readers.

9. The ability to read expanded smart card data format lengths up to 144 bits.
10. Backwards compatibility with legacy 125 KHz proximity access control formats (E.g.16-bit, 26-bit, 32, 35-bit, 37-bit, 56-bit, and HID Corporate 1000 formats).
11. Optimal read range and read speed for increased access control throughput.
12. A full product line of compatible products including single- and multi-technology readers, readers with integral keypads and LCD displays, long range readers, biometric readers, read/write readers, card programmers, and cards.
13. Global, off-the-shelf availability.
14. Built in compatibility across the product line without the need of special programming.
15. Product construction suitable for both indoor and outdoor applications.
16. Customizable behavior for indicator lights and audible tones.
17. Multi-technology contactless smart card reader shall comply with the following 13.56MHz-related standards to ensure product compatibility and predictability of performance:
    a. ISO 15693
    b. ISO 14443A
    c. ISO 14443B.
18. Contactless smart card reader shall be configurable to read 13.56 MHz data simultaneously from one to, at minimum, two of the following cards:
    a. HID iCLASS Access Control Sector/Application data
    b. ISO 15693 card serial number (CSN)
    c. ISO 14443A card serial number (CSN): including MIFARE & DESFire
    d. ISO 14443B card serial number (CSN)
    e. Sony FeliCa IDm – Transit version readers only
19. N/A - Contactless smart card reader shall be configurable to read data from any single compatible 125 kHz technology simultaneously with 13.56 MHz data. Compatible 125 kHz technologies include:
    a. HID 125 kHz Proximity access control application
    b. AWID 125 kHz Proximity access control application
    c. Indala 125 kHz Proximity access control application
20. Contactless smart card readers shall provide priority processing for reading multi-technology (13.56 MHz & 125 kHz) credentials. When reading a multi-technology credential, the reader shall provide a selectable priority of which technology to process and transmit data to the access control system.
21. The contactless smart card reader shall provide the ability to read card access data stored in the secure access control sector/application area of the ISO 15693 HID iCLASS card.
22. The contactless smart card reader shall be configurable to provide multiple hierarchical degrees of key compatibility for accessing the smart card access control data. Compatibility shall be provided for the following key structure options:
    a. Compatibility with the default iCLASS key structure to ensure convenient off the shelf compatibility with iCLASS cards and readers.
    b. Compatibility with higher security HID managed ELITE keys which provide a site-specific, unique, protected key structure.
    c. Compatibility with high security user-managed custom keys.
23. The contactless smart card reader shall be configurable to provide compatibility with all HID Prox formats, including Corporate 1000 and Long formats, or Indala Prox formats, including full support of any FlexPass® and FlexSecure® formats.
24. Contactless smart card reader shall be compatible with HID's iCLASS mutual authentication algorithm using 64-bit authentication keys. All RF data transmission between the card and reader shall encrypted using a secure algorithm to ensure that the communication between the card and reader can never be copied and repeated back to the reader (sniffing and replay).
25. Contactless smart card reader shall allow the reader firmware to be upgraded in the field without the need to remove the reader from the wall through the use of factory-provided Application Cards.

26. In areas requiring dual authentication as specified by Spectrum Physical Security Team, the contactless smart card reader shall provide a 12-position weatherproof keypad featuring a waterproof silicon boot, vandal-resistant metal keycaps, and backlit keypad numbering.
27. The weatherproof keypad shall provide a raised tactile mark on the “5” keycap for visually impaired users.
28. Kepad lighting shall be configurable as “Always On”, Always Off”, “Triggered by Card Read”, or “Triggered by Key Press”.
29. The contactless card reader keypad output shall provide a variety of keypad outputs to ensure compatibility with virtually any access control panel. Keypad output settings shall include:
    a. Buffer one key, no parity, 4 bit message
    b. Buffer one key, add compliment, 8 bit message (Dorado)
    c. Buffer six keys and add parity
    d. Buffer one key and add parity
    e. Buffer one to five keys (Standard 26 bit output)
    f. Buffer four keys and add parity
    g. Single Key buffering
    h. Local PIN Verify. (Requires User PIN code to be programmed into the iCLASS Credential by using the iCLASS Card Programmer (please consult factory for availability.)
30. Contactless smart card reader shall be suitable for global deployment by meeting worldwide radio and safety regulatory compliance including:
    a. UL294 (US)
    b. FCC Certification (US)
31. Contactless smart card reader shall be fully compliant with Restriction of Hazardous Substances directive (RoHS) restricting the use of specific hazardous materials found in electrical and electronic products. The substances banned under RoHS are lead (Pb), mercury (Hg), cadmium (Cd), hexavalent chromium (CrVI), polybrominated biphenyls (PBB) and polybrominated diphenyl ethers (PBDE).
32. Contactless smart card reader shall provide universal compatibility with most access control systems by outputting card data in compliance with the SIA AC-01 Wiegand standard.
33. Contactless smart card reader shall be available to provide Clock and Data output.
34. Contactless smart card reader shall allow for secure installation practices through mounting methods utilizing tamper resistant screws.
35. Contactless smart card reader shall provide the ability to transmit an alarm signal via and integrated optical tamper switch if an attempt is made to remove the reader from the wall. The tamper switch shall be programmable to provide a selectable action compatible with various tamper communication schemes provided by access control panel manufacturers. The selectable action shall include one of the following:
    a. The reader open collector line changes from a high state (5V) to a low state (Ground).
    b. During a tamper state, the “I’m Alive” message is inverted.
36. Contactless smart card reader shall provide ability of an on-line “I’m Alive” message so the reader’s functional health can be monitored at all times when paired with a compatible access control panel.
37. Contactless smart card reader shall provide the ability for mounting to standard electrical boxes through the use of universal international mounting holes.
38. Contactless smart card reader shall be provided with a full potted assembly.
39. The contactless smart card reader shall provide customizable reader behavior options either from the factory, or defined in the field through the use of pre-configured command cards. Reader behavior programming options shall include:
    a. LED & Audio configurations
    b. Disablement of reading specific card technologies (typically used after migration is complete to new technology).

c. ISO 14443A CSN (E.g. MIFARE/DESFire) output configuration.
d. Wiegand output spacing and timing.
e. Keypad output and backlighting.

40. Contactless smart card reader shall provide the following programmable audio/visual indication:
    a. An audio beeper shall provide various tone sequences to signify: access granted, access denied, power up, and diagnostics.
    b. A high-intensity light bar shall provide clear visual status (red/green/amber).
41. The contactless smart card reader shall have the ability to provide consistent optimal read range by implementing an auto-tune function that adjusts for manufacturing tolerances to enhance consistency of performance from reader to reader. Contactless smart card reader shall provide the following typical contactless read ranges:
    a. 3.5” – 4.25” (9.0 – 11.0 cm) using HID iCLASS card
    b. 1.0” – 1.5” (2.5 – 4.0 cm) using ISO 15693 HID iCLASS Key or Tag
    c. 2.5” – 3.5” (6.5 – 9.0 cm) using HID Prox ISO card
    d. 3.5” – 4.0” (9.0 – 10.0 cm) using HID Prox Clamshell card
    e. 1.25” – 1.75” (3.2 – 4.5 cm) using HID Prox Key or Tag
    f. 1.5” – 2.0” (4.0 – 5.0 cm) using Indala Prox ISO card
    g. 1.75” – 2.25” (4.5 – 5.5 cm) using Indala Prox Clamshell card
    h. 1.0” – 1.25” (2.5 – 3.2 cm) using Indala Prox Key or Tag
    i. 1.25” – 2.0” (4.4 – 6.4 cm) using MIFARE/DESFire card (CSN)

F. Wall Mounted Contactless iCLASS R40 6120BK Smart Card Reader
1. Contactless smart card reader shall be designed for low current operation to enable migration from most legacy proximity applications without the need to replace existing access control panels and/or power supplies. Contactless smart card power requirements shall be:
    a. Operating voltage: 5 – 16 VDC, reverse voltage protected. Linear power supply recommended.
    b. Current requirements: 85 mA AVG, 169 mA PEAK @ 12 VDC
2. Contactless smart card reader shall meet the following physical specifications:
    a. Dimensions: 3.3” x 4.8” x 1.05” (8.4 cm x 12.2 cm x 2.7 cm)
    b. Weight: 9.1 oz (258 g)
    c. Material: UL94 Polycarbonate
    d. Plastics: Consist of two-piece design with mounting plate and combined keypad reader housing/reader body (totaling two-pieces). Keypad reader housing snaps onto mounting plate and is secured with a screw.
    e. Color: Black or Charcoal Gray as approved by the project architect.
3. Contactless smart card reader shall meet the following environmental specifications:
    a. Operating temperature: -31 to 150 degrees F (-35 to 65 degrees C)
    b. Operating humidity: 5% to 95% relative humidity non-condensing
    c. Weatherized design suitable to withstand harsh environments
4. Certified rating of IP55
    a. Contactless smart card reader cabling requirements shall be:
        1) Cable distance: (Wiegand or Clock & Data): 500 feet (150m)
        2) Cable type: 5-conductor #22 AWG
        3) Standard reader termination: 18” (0.5m) cable pigtail
5. The Contactless smart card reader shall provide a lifetime warranty against defects in materials and workmanship.
6. Contactless smart card reader shall be Genuine HID iCLASS SE R40 or SE RK40.

G. Mullion Mounted Contactless Smart Card Reader
1. Contactless smart card reader shall be designed for low current operation to enable migration from most legacy proximity applications without the need to replace existing access control panels and/or power supplies. Contactless smart card power requirements shall be:

a. Operating voltage: 5 – 16 VDC, reverse voltage protected. Linear power supply recommended.
b. Current requirements: 55 mA AVG, 114 mA PEAK @ 12 VDC

2. Contactless smart card reader shall meet the following physical specifications:
   a. Weight: 5.9 oz (166 g)
   b. Material: UL94 Polycarbonate
   c. Plastics: Consist of a mounting plate and combined front bezel/reader body (totaling two-pieces). Reader body snaps onto mounting plate and secured with a screw.
   d. Color: Black or Charcoal Gray as approved by the project architect.
3. Contactless smart card reader shall meet the following environmental specifications:
   a. Operating temperature: -31 to 150 degrees F (-35 to 65 degrees C)
   b. Operating humidity: 5% to 95% relative humidity non-condensing
   c. Weatherized design suitable to withstand harsh environments
4. Certified rating of IP55
5. Contactless smart card reader cabling requirements shall be:
   a. Cable distance: (Wiegand or Clock & Data): 500 feet (150m)
   b. Cable type: 5-conductor #22 AWG
   c. Standard reader termination: 18” (0.5m) cable pigtail
6. The Contactless smart card reader shall provide a lifetime warranty against defects in materials and workmanship.
7. Contactless smart card reader shall be Genuine HID Global iCLASS Model SE R10 or SE R15.

2.10 DOOR AND GATE HARDWARE INTERFACE

A. Exit Device with Alarm: Operation of the exit device shall generate an alarm. Exit device and alarm contacts are specified in Division 08 Section "Door Hardware."

B. Exit Alarm: Operation of a monitored door shall generate an alarm. Exit devices and alarm contacts are specified in Division 08 Section "Door Hardware."

C. Electric Door Strikes: Use end-of-line resistors to provide power line supervision. Signal switches shall transmit data to Controller to indicate when the bolt is not engaged and the strike mechanism is unlocked, and shall report a forced entry. Power and signal shall be from the Controller. Electric strikes are specified in Division 08 "Door Hardware."

D. Electromagnetic Locks: End-of-line resistors shall provide power line supervision. Lock status sensing signal shall positively indicate door is secure. Power and signal shall be from the Controller. Electromagnetic locks are specified in Division 08 Section "Door Hardware."

E. Vehicle Gate Operator: Interface electrical operation of gate with controls of this Section. Vehicle gate operators shall be connected, monitored, and controlled, by the security access Controllers. Vehicle gate and accessories are specified in Division 32 Section "Chain Link Fences and Gates."

2.11 RS-232 ASCII INTERFACE SPECIFICATIONS

A. ASCII interface shall allow RS-232 connections to be made between the control station operating as the host PC and any equipment that will accept RS-232 ASCII command strings, such as CCTV switchers, intercoms, and paging systems.
   1. Each alarm input in system shall allow for individual programming to output up to four unique ASCII character strings through two different COM ports on the host PC.
   2. Each input shall have the ability to be defined to transmit a unique ASCII string for alarm and one for restore through one COM port, and a unique ASCII string for a nonalarm abnormal condition and one for a normal condition through the same or different COM port.
   3. The predefined ASCII character strings shall have the ability to be up to 420 characters long with full use of all the ASCII control characters, such as return or line feed. The character strings shall be defined in database of system and then assigned to the appropriate inputs.

4. The COM ports of the host PC used to interface with external equipment shall be defined in the setup portion of the software. The COM port's baud rate, word length, stop bits, and parity shall be definable in the software to match that of the external equipment.

B. Pager System Interface: Alarms shall be able to activate a pager system with customized message for each input alarm.
   1. RS-232 output shall be capable of connection to a pager interface that can be used to call a paging system or service and send a signal to a portable pager. System shall allow an individual alphanumeric message per alarm input to be sent to the paging system. This interface shall support both numeric and alphanumeric pagers.

C. Alarm System Interface:
   1. RS-232 output shall be capable of transmitting alarms from other monitoring and alarm systems to central-station automation software.
   2. Alternatively, alarms that are received by this access control system are to be transferred to alarm automation system as if they were sent through a digital alarm receiver.
      a. System shall be able to transmit an individual message from any alarm input to a burglar alarm automation monitoring system.
      b. System shall be able to append to each message a predefined set of character strings as a prefix and suffix.

2.12 CABLES

A. Available Manufacturers:
   1. Anixter, Inc.
   2. Belden Inc.; Electronics Division.
   3. Berk-Tek; a Nexans Company.
   4. BIW Cable Systems; a Draka USA Company.
   5. Champlain Cable Corporation.
   6. Chromatic Technologies; a Draka USA Company.
   7. Coleman Cable.
   8. General Cable Technologies Corporation.
   9. KRONE Incorporated.
   10. Mohawk/CDT; a division of Cable Design Technologies.
   11. West Penn Wire/CDT; a division of Cable Design Technologies.

B. Comply with Division 28 Section "Conductors and Cables for Electronic Safety and Security."

C. Access Control Hybrid Cable: Components have their own jacket, and are then cabled together under a common yellow jacket. 18 - 4/C SHLD, 22 - 3/PR SHLD, 22 - 2/C SHLD & 22 - 4/C SHLD. Solid or Stranded bare copper
   1. Color coded Polymer or PVC insulation
   2. 100% aluminum/polyester foil shield
   3. Tinned copper drain wire
   4. PVC or Polymer alloy PVC jacket
   5. NEC article 800
   6. UL listed CMR/CMP by item

D. PVC-Jacketed, RS-232 Cable: Paired, 2 pairs, No. 22 AWG, stranded (7x30) tinned copper conductors, polypropylene insulation, and individual aluminum foil-polyester tape shielded pairs with 100 percent shield coverage; PVC jacket. Pairs are cabled on common axis with No. 24 AWG, stranded (7x32) tinned copper drain wire.
   1. NFPA 70, Type CM.
   2. Flame Resistance: UL 1581 Vertical Tray.

E. Plenum-Type, RS-232 Cable: Paired, 2 pairs, No. 22 AWG, stranded (7x30) tinned copper conductors, plastic insulation, and individual aluminum foil-polyester tape shielded pairs with 100 percent shield coverage; plastic jacket. Pairs are cabled on common axis with No. 24 AWG, stranded (7x32) tinned copper drain wire.
   1. NFPA 70, Type CMP.
   2. Flame Resistance: NFPA 262 Flame Test.

F. RS-485 communications require 2 twisted pairs, with a distance limitation of 4000 feet (1220 m).

G. PVC-Jacketed, RS-485 Cable: Paired, 2 pairs, twisted, No. 22 AWG, stranded (7x30) tinned copper conductors, PVC insulation, unshielded, PVC jacket, and NFPA 70, Type CMG.

H. Plenum-Type, RS-485 Cable: Paired, 2 pairs, No. 22 AWG, stranded (7x30) tinned copper conductors, fluorinated-ethylene-propylene insulation, unshielded, and fluorinated-ethylene-propylene jacket.
   1. NFPA 70, Type CMP.
   2. Flame Resistance: NFPA 262 Flame Test.

I. Multiconductor, PVC Readers and Wiegand Keypads Cables: No. 22 AWG, paired and twisted multiple conductors, stranded (7x30) tinned copper conductors, semirigid PVC insulation, overall aluminum foil-polyester tape shield with 100 percent shield coverage, plus tinned copper braid shield with 65 percent shield coverage, and PVC jacket.
   1. NFPA 70, Type CMG.
   2. Flame Resistance: UL 1581 Vertical Tray.
   3. For TIA/EIA-RS-232 applications.

J. Paired PVC Readers and Wiegand Keypads Cables: Paired, 3 pairs, twisted, No. 22 AWG, stranded (7x30) tinned copper conductors, polypropylene insulation, individual aluminum foil-polyester tape shielded pairs each with No. 22 AWG, stranded tinned copper drain wire, 100 percent shield coverage, and PVC jacket.
   1. NFPA 70, Type CM.
   2. Flame Resistance: UL 1581 Vertical Tray.

K. Paired PVC Readers and Wiegand Keypads Cable: Paired, 3 pairs, twisted, No. 20 AWG, stranded (7x28) tinned copper conductors, polyethylene (polyolefin) insulation, individual aluminum foil-polyester tape shielded pairs each with No. 22 AWG, stranded (19x34) tinned copper drain wire, 100 percent shield coverage, and PVC jacket.
   1. NFPA 70, Type CM.
   2. Flame Resistance: UL 1581 Vertical Tray.

L. Plenum-Type, Paired, Readers and Wiegand Keypads Cable: Paired, 3 pairs, No. 22 AWG, stranded (7x30) tinned copper conductors, plastic insulation, individual aluminum foil-polypropylene tape shielded pairs each with No. 22 AWG, stranded tinned copper drain wire, 100 percent shield coverage, and fluorinated-ethylene-propylene jacket.
   1. NFPA 70, Type CMP.
   2. Flame Resistance: NFPA 262 Flame Test.

M. Plenum-Type, Multiconductor, Readers and Wiegand Keypads Cable: 6 conductors, No. 20 AWG, stranded (7x28) tinned copper conductors, fluorinated-ethylene-propylene insulation, overall aluminum foil-polyester tape shield with 100 percent shield coverage plus tinned copper braid shield with 85 percent shield coverage, and fluorinated-ethylene-propylene jacket.
   1. NFPA 70, Type CMP.
   2. Flame Resistance: NFPA 262 Flame Test.

N. Paired Lock Cable: 1 pair, twisted, No. 16 AWG, stranded (19x29) tinned copper conductors, PVC insulation, unshielded, and PVC jacket.
   1. NFPA 70, Type CMG.
   2. Flame Resistance: UL 1581 Vertical Tray.

O. Plenum-Type, Paired Lock Cable: 1 pair, twisted, No. 16 AWG, stranded (19x29) tinned copper conductors, PVC insulation, unshielded, and PVC jacket.
   1. NFPA 70, Type CMP.
   2. Flame Resistance: NFPA 262 Flame Test.

P. Paired Lock Cable: 1 pair, twisted, No. 18 AWG, stranded (19x30) tinned copper conductors, PVC insulation, unshielded, and PVC jacket.
   1. NFPA 70, Type CMG.
   2. Flame Resistance: UL 1581 Vertical Tray.

Q. Plenum-Type, Paired Lock Cable: 1 pair, twisted, No. 18 AWG, stranded (19x30) tinned copper conductors, fluorinated-ethylene-propylene insulation, unshielded, and plastic jacket.
   1. NFPA 70, Type CMP.
   2. Flame Resistance: NFPA 262 Flame Test.

R. Paired Input Cable: 1 pair, twisted, No. 22 AWG, stranded (7x30) tinned copper conductors, polypropylene insulation, overall aluminum foil-polyester tape shield with No. 22 AWG, stranded (7x30) tinned copper drain wire, 100 percent shield coverage, and PVC jacket.
   1. NFPA 70, Type CMR.
   2. Flame Resistance: UL 1666 Riser Flame Test.

S. Plenum-Type, Paired Input Cable: 1 pair, twisted, No. 22 AWG, stranded (7x30) tinned copper conductors, fluorinated-ethylene-propylene insulation, aluminum foil-polyester tape shield (foil side out), with No. 22 AWG drain wire, 100 percent shield coverage, and plastic jacket.
   1. NFPA 70, Type CMP.
   2. Flame Resistance: NFPA 262 Flame Test.

T. Paired AC Transformer Cable: 1 pair, twisted, No. 18 AWG, stranded (7x26) tinned copper conductors, PVC insulation, unshielded, and PVC jacket.
   1. NFPA 70, Type CMG.

U. Plenum-Type, Paired AC Transformer Cable: 1 pair, twisted, No. 18 AWG, stranded (19x30) tinned copper conductors, fluorinated-ethylene-propylene insulation, unshielded, and plastic jacket.
   1. NFPA 70, Type CMP.
   2. Flame Resistance: NFPA 262 Flame Test.

V. Elevator Travel Cable: Steel center core, with shielded, twisted pairs, No. 20 AWG conductor size.
   1. Steel Center Core Support: Preformed, flexible, low-torsion, zinc-coated, steel wire rope; insulated with 60 deg C flame-resistant PVC and covered with a nylon or cotton braid.
   2. Shielded Pairs: Insulated copper conductors; color-coded, insulated with 60 deg C flame-resistant PVC; each pair shielded with bare copper braid for 85 percent coverage.
   3. Jute Filler: Electrical grade, dry.
   4. Binder: Helically wound synthetic fiber.
   5. Braid: Rayon or cotton braid applied with 95 percent coverage.
   6. Jacket: 60 deg C PVC specifically compounded for flexibility and abrasion resistance. UL VW-1 and CSA FT1 flame rated.

W. LAN Cabling: Comply with Division 28 Section "Conductors and Cables for Electronic Safety and Security."
   1. NFPA 262.

2.13 CONTROL PANEL POWER SUPPLIES

A. The Security Contractor shall be responsible for the provision and connection of power supplies. The power supplies shall be located in the security riser closets as shown on the drawings.

B. Electric locking devices shall be designed for continuous duty silent operation and shall be fail secure and/or fail safe. Refer to the door hardware schedule for exact requirements.

C. Power supplies shall be field installed as required to support operation of electric locking devices at all card reader controlled doors. The final connection of 120VAC power shall be provided by the Electrical Contractor.

D. Power supply capacities shall be sufficient to support 120% of the current requirements for associated electric locking devices.

E. Power supplies shall be mounted within a metal enclosure designed for wall mounting. Enclosures shall include a hinged, key lockable door and a door tamper switch.

F. Power supplies shall be adequately sized to accommodate up to eight (8) doors from the associated power supply. Each door shall be individually fused.

G. Power supplies used shall be designed to send a signal to the ACMS in the event of a power loss or low battery condition.

2.14 ELECTRIFIED HARDWARE POWER SUPPLIES

A. The Security Contractor shall coordinate the provision and connection of power supplies and associated circuitry as required for operation of electrified hardware. The power supplies shall be located in the security riser closets as shown on the drawings.

B. Electric locking devices shall be designed for continuous duty silent operation and shall be fail secure and/or fail safe. Refer to the door hardware schedule for exact requirements.

C. Power supplies shall be field installed as required to support operation of electric locking devices at all card reader controlled doors. The final connection of 120VAC power shall be provided by the Electrical Contractor.

D. Power supply capacities shall be sufficient to support 120% of the current requirements for associated electric locking devices.

E. Power supplies shall be mounted within a metal enclosure designed for wall mounting. Enclosures shall include a hinged, key lockable door and a door tamper switch.

F. Power supplies shall be adequately sized to accommodate up to eight (8) doors from the associated power supply. Each door shall be individually fused.

G. Power supplies used shall be designed to send a signal to the ACMS in the event of a power loss or low battery condition.

2.15 ELECTRIFIED PANIC HARDWARE POWER SUPPLIES

A. The Security Contractor shall coordinate the provision and connection of power supplies and associated circuitry as required for operation of field devices to include request to exit devices and glass break detectors. The power supplies shall be located in the security riser closet as shown on the drawings.

B. Power supply capacities shall be sufficient to support 120% of the current requirements for associated devices. Final connection of 120V power shall be provided by the Electrical Contractor.

C. Power supplies shall be mounted within a metal enclosure designed for wall mounting. Enclosures shall include a hinged, key lockable door and a door tamper switch.

D. Power supplies used shall be designed to send a signal to the ACMS in the event of a power loss or low battery condition.

2.16 EQUIPMENT TAMPER SWITCH

A. Tamper switches shall be designed to detect access to security equipment via the equipment cabinet door and shall consist of a spring loaded switch assembly such that movement of the door shall cause the switch contacts to transfer.

B. Tamper switches shall incorporate SPDT type micro switches and shall provide of mounting within the equipment cabinet such that the switch cannot be disconnected or disabled from the cabinet exterior.

C. Equipment tamper switches shall be installed on every power supply cabinet, access control cabinet, or elevator interface panel cabinet.

D. The Security Contractor shall provide all necessary connections to interface all equipment tamper switches as individual alarm points

2.17 FIBER OPTIC ACMS TRANSCEIVERS

A. The Security Contractor shall provide RS-485 compatible, fiber optic transceivers for distribution of the ACMS data.

B. Fiber optic transmitters shall be provided as shown on the ACMS block diagram and shall provide for transmission of data signals over the fiber optic cable specified.

C. Fiber optic transmitters shall be provided at a minimum for all the security closets to the security equipment room.

D. Fiber Optic Data Transmitters
   1. Fiber optic transmitters shall be provided as shown on the ACMS block diagram and shall provide for transmission of two way data signals over the fiber optic cable specified.
   2. Fiber optic transmitters shall be compatible with the HID iCLASS card readers specified.

E. Fiber Optic Transmitter Card Cage
   1. Fiber optic transmitter card cage shall be provided in the security equipment room and security closets as shown on the ACMS block diagram and shall provide for the compact installation of the fiber optic transmitters in the equipment rack.

2.18 CARD READER PEDESTALS

A. Pedestals shall be made of 2" X 4" rectangular steel tubing or 4” round steal tubing with an 8" X 12" base plate.

B. A steel base plate cover is provided to conceal the mounting hardware.

C. OVERALL HEIGHT: TBD, ADA Compliant

D. MATERIAL: 2" x 4" Rectangular steel tubing

E. FINISH: As determined by Architect.

PART 3 EXECUTION

3.01 EXAMINATION

A. Examine pathway elements intended for cables. Check raceways, cable trays, and other elements for compliance with space allocations, installation tolerances, hazards to cable installation, and other conditions affecting installation.
   1. If during examination of pathways, pentrations through rated enclosures are not firestopped, please notify EC, GC, and Owner.
   2. If new pathways are required that were not provided by the EC, all sections of this specification apply for conduit sizing, fire stopping, and other specific requirements outlined in these specifications.

B. Examine roughing-in for LAN and control cable conduit systems to PCs, Controllers, card readers, and other cable-connected devices to verify actual locations of conduit and back boxes before device installation.

C. Proceed with installation only after unsatisfactory conditions have been corrected.

3.02 PREPARATION

A. Comply with recommendations in SIA CP-01.

B. Comply with EIA/TIA-606, "Administration Standard for the Telecommunications Infrastructure of Commercial Buildings."

C. Obtain detailed Project planning forms from manufacturer of access-control system; develop custom forms to suit Project. Fill in all data available from Project plans and specifications and publish as Project planning documents for review and approval.
   1. Record setup data for control station and workstations.
   2. For each Location, record setup of Controller features and access requirements.
   3. Propose start and stop times for time zones and holidays, and match up access levels for doors.
   4. Set up groups, facility codes, linking, and list inputs and outputs for each Controller.
   5. Assign action message names and compose messages.
   6. Set up alarms. Establish interlocks between alarms, intruder detection, and video surveillance features.
   7. Prepare and install alarm graphic maps.
   8. Develop user-defined fields.
   9. Develop screen layout formats.
   10. Discuss badge layout options; design badges.
   11. Complete system diagnostics and operation verification.
   12. Prepare a specific plan for system testing, startup, and demonstration.

13. Develop acceptance test concept and, on approval, develop specifics of the test.
14. Develop cable and asset management system details; input data from construction documents. Include system schematics and Visio Technical Drawings.

D. In meetings with Architect and Owner, present Project planning documents and review, adjust, and prepare final setup documents. Use final documents to set up system software.

3.03 CABLING

A. Comply with NECA 1, "Good Workmanship in Electrical Contracting."

B. Install cables and wiring according to requirements in Division 28 Section "Conductors and Cables for Electronic Safety and Security."

C. Wiring Method: Install wiring in raceway and cable tray except within consoles, cabinets, desks, and counters and except in accessible ceiling spaces and in gypsum board partitions where unenclosed wiring method may be used. Use NRTL-listed plenum cable in environmental air spaces, including plenum ceilings. Conceal raceway and cables except in unfinished spaces.

D. Open wiring is not permitted in exposed locations (electrical rooms, machine rooms, IT Closets). All wiring to be in conduit or cable tray per 26 0500 Basic Electrical Requirements

E. Install LAN cables using techniques, practices, and methods that are consistent with Category 5E rating of components and that ensure Category 5E performance of completed and linked signal paths, end to end.

F. Install cables without damaging conductors, shield, or jacket.

G. Boxes and enclosures containing security system components or cabling, and which are easily accessible to employees or to the public, shall be provided with a lock. Boxes above ceiling level in occupied areas of the building shall not be considered to be accessible. 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 tamperproof screws.

H. Install end-of-line resistors at the field device location and not at the Controller or panel location.

3.04 CABLE APPLICATION

A. Comply with EIA/TIA-569, "Commercial Building Standard for Telecommunications Pathways and Spaces."

B. Cable application requirements are minimum requirements and shall be exceeded if recommended or required by manufacturer of system hardware.

C. RS-232 Cabling: Install at a maximum distance of 50 feet (15 m).

D. RS-485 Cabling: Install at a maximum distance of 4000 feet (1220 m).

E. Card Readers and Keypads:
1. Install number of conductor pairs recommended by manufacturer for the functions specified.
2. Unless manufacturer recommends larger conductors, install No. 22 AWG wire if maximum distance from Controller to the reader is 250 feet (75 m), and install No. 20 AWG wire if maximum distance is 500 feet (150 m).
3. For greater distances, install "extender" or "repeater" modules recommended by manufacturer of the Controller.
4. Install minimum No. 18 AWG shielded cable to readers and keypads that draw 50 mA or more.

F. Install minimum No. 16 AWG cable from Controller to electrically powered locks. Do not exceed 500 feet (150 m).

G. Install minimum No. 18 AWG ac power wire from transformer to Controller, with a maximum distance of 25 feet (8 m).

3.05 GROUNDING

A. Comply with Division 26 Section "Grounding and Bonding for Electrical Systems."

B. Comply with IEEE 1100, "Power and Grounding Sensitive Electronic Equipment."

C. Ground cable shields, drain conductors, and equipment to eliminate shock hazard and to minimize ground loops, common-mode returns, noise pickup, cross talk, and other impairments.

D. Bond shields and drain conductors to ground at only one point in each circuit.

E. Signal Ground:
   1. Terminal: Locate in each equipment room and wiring closet; isolate from power system and equipment grounding.
   2. Bus: Mount on wall of main equipment room with standoff insulators.
   3. Backbone Cable: Extend from signal ground bus to signal ground terminal in each equipment room and wiring closet.

3.06 INSTALLATION

A. Push Buttons: Where multiple push buttons are housed within a single switch enclosure, they shall be stacked vertically with each push-button switch labeled with 1/4-inch- (6.4-mm-) high text and symbols as required. Push-button switches shall be connected to the Controller associated with the portal to which they are applied, and shall operate the appropriate electric strike, electric bolt, or other facility release device.

B. Install card, fob, and biometric readers.

3.07 IDENTIFICATION

A. In addition to requirements in this Article, comply with applicable requirements in Division 26 Section "Identification for Electrical Systems" and with TIA/EIA-606.

B. Using cable and asset management software specified in Part 2, develop Cable Administration Drawings for system identification, testing, and management. Use unique, alphanumeric designation for each cable, and label cable and jacks, connectors, and terminals to which it connects with same designation. Use logical and systematic designations for facility's architectural arrangement.

C. Label each terminal strip and screw terminal in each cabinet, rack, or panel.
   1. All wiring conductors connected to terminal strips shall be individually numbered, and each cable or wiring group being extended from a panel or cabinet to a building-mounted device shall be identified with the name and number of the particular device as shown.
   2. Each wire connected to building-mounted devices is not required to be numbered at the device if the color of the wire is consistent with the associated wire connected and numbered within the panel or cabinet.

D. At completion, cable and asset management software shall reflect as-built conditions.

3.08 SYSTEM SOFTWARE

A. Develop, install, and test software and databases for the complete and proper operation of systems involved. Assign software license to Owner.

3.09 SEQUENCE OF OPERATION

A. Main Entry Automatic Door
   1. All Hours Entry:
      a. The card reader is active.
      b. Pressing actuator button without credential presentation will not start the operator sequence to open door.
      c. Presenting a valid card and pressing actuator button will start the operator sequence to open door.

B. Loading Dock Overhead Door
   1. All Hours opening:
      a. The card reader is active.

b. Pressing door open button without credential presentation will not start the operator sequence to open door.
c. Presenting a valid card and pressing door opening button will start the operator sequence to open door, shunt the alarm and start a 15 minute timer.
d. After 13 minutes the card reader will beep to notify the staff member to either close the door or present their card again.
e. Presenting the card again resets the timer and allows the operation in item C or D above.
f. Not presenting the card before the 15 minutes are up sends alarm to central station ~~the third party central station~~.
g. A valid card read is not required to allow the door to be closed.

C. Main Gate
1. All Hours Entry:
a. At all hours the card reader is active.
b. Activating the pavement loop without credential presentation will not start the operator sequence to open the gate.
c. Presenting a valid card and activating the pavement loop will start the operator sequence to open the gate.
d. Presenting valid card and activating the pavement loop will shunt portion of beam detection directly in front of drive only.
2. All Hours Exit:
a. At all hours a card read is not required to exit the equipment yard.
b. Activating the pavement loop will start the operator sequence to open the gate.

D. Vehicle Yard Gate
1. All Hours Entry:
a. At all hours the card reader is active.
b. Activating the pavement loop without credential presentation will not start the operator sequence to open the gate.
c. Presenting a valid card and activating the pavement loop will start the operator sequence to open the gate.
2. All Hours Exit:
a. At all hours the card reader is active. Activating the pavement loop will start the operator sequence to open the gate without a card read.
1) A card read is required to shunt the alarm when exiting the equipment yard.
b. Activating the pavement loop without credential presentation will not start the operator sequence to open the gate.
c. Presenting a valid card and activating the pavement loop will start the operator sequence to open the gate.

E. Pedestrian Yard Gate
1. All Hours Entry:
a. At all hours the card reader is active.
b. Presenting a valid card will unlock the gate.
2. All Hours Exit:
a. A card read is not required to exit through the pedestrian yard gate.
1) A card read is required to shunt the alarm when exiting the equipment yard.

F. Interior Card in/Card out Doors
1. All Hours Entry:
a. At all hours the card reader is active.
b. Presenting a valid card will unlock the door.
2. All Hours Exit:
a. A card read is not required to exit through the door.
1) A card read is required to shunt the alarm when exiting the room.
2) Failure to read a valid card will result in a Forced Door alarm being sent to the Central Station

3.10 FIELD QUALITY CONTROL

A. Manufacturer's Field Service: Engage a factory-authorized service representative to inspect[, test, and adjust] field-assembled components and equipment installation, including connections[, and to assist in field testing]. Report results in writing.

B. Testing Agency: [Owner will engage] [Engage] a qualified testing and inspecting agency to perform field tests and inspections and prepare test reports:

C. Perform the following field tests and inspections and prepare test reports:
   1. LAN Cable Procedures: Inspect for physical damage and test each conductor signal path for continuity and shorts. Use Class 2, bidirectional, Category 5 tester. Test for faulty connectors, splices, and terminations. Test according to TIA/EIA-568-1, "Commercial Building Telecommunications Cabling Standards - Part 1 General Requirements." Link performance for UTP cables must comply with minimum criteria in TIA/EIA-568-B.
   2. Test each circuit and component of each system. Tests shall include, but are not limited to, measurements of power supply output under maximum load, signal loop resistance, and leakage to ground where applicable. System components with battery backup shall be operated on battery power for a period of not less than 10 percent of the calculated battery operating time. Provide special equipment and software if testing requires special or dedicated equipment.
   3. Operational Test: After installation of cables and connectors, demonstrate product capability and compliance with requirements. Test each signal path for end-to-end performance from each end of all pairs installed. Remove temporary connections when tests have been satisfactorily completed.

D. Remove and replace malfunctioning devices and circuits and retest as specified above.

3.11 STARTUP SERVICE

A. Engage a factory-authorized service representative to supervise and assist with startup service. Complete installation and startup checks according to approved procedures that were developed in " Preparation" Article and with manufacturer's written instructions.
   1. Enroll and prepare badges and access cards for Owner's operators, management, and security personnel.

3.12 PROTECTION

A. Maintain strict security during the installation of equipment and software. Rooms housing the control station, and workstations that have been powered up shall be locked and secured, with an activated burglar alarm and access-control system reporting to a Central Station complying with UL 1610, "Central-Station Burglar-Alarm Units," during periods when a qualified operator in the employ of Contractor is not present.

3.13 DEMONSTRATION

A. Engage a factory-authorized service representative to train Owner's maintenance personnel to adjust, operate, and maintain security access system. Refer to Division 01 Section "Demonstration and Training"

B. Develop separate training modules for the following:
   1. Computer system administration personnel to manage and repair the LAN and databases and to update and maintain software.
   2. Operators who prepare and input credentials to man the control station and workstations and to enroll personnel.
   3. Security personnel.
   4. Hardware maintenance personnel.
   5. Corporate management.

END OF SECTION 281300 28 1300