16722 SECURITY AND ACCESS CONTROL SYSTEMS

PART 1: GENERAL

1.01 SYSTEM DESCRIPTION

A. Head-End Database Server (HDS)

1. The Head-End Database Server (HDS) warehouses the total University client information. This server supports Best Access Systems’ BASIS Software System and uses an Oracle database platform.

2. The Head-End Database Server (HDS) stores all alarms, trouble conditions, asset management information, administrative information, video management information, etc. delivered from the intelligent system controllers (ICSs) on campus across the TCP/IP connections. The historic alarms are kept for a period of two months and then they are deleted.

3. Existing non-BASIS supporting security and access systems tie into the Campus Police Workstation via Cornell’s Central Station manufactured by Digitize, Inc. These existing non-BASIS supporting systems report to the Digitize Central Station over dedicated copper communication pairs in the respective building. A digital dialer located in or at the building’s security access system transmits the information. The Digitize Central Station security output is gathered and transmitted over a TCP/IP connection to the HDS to ensure integrity of alarms and trouble conditions.

B. Campus Police Workstation (CPW)

1. A Campus Police Workstation (CPW) supporting the campus security systems resides at Barton Hall. This terminal supports Best Access Systems’ BASIS Software System. The CPW monitors only certain critical alarms and trouble conditions from intelligent system controllers (ISCs) located in Cornell University’s buildings. This system does not monitor routine transactions. Arrangements should be made with the Cornell Police to enable monitoring of the critical alarms.

2. New installations of BASIS supportive ISCs shall be tied into the CPW via the Head-End Database Server (HDS) through a dedicated secure TCP/IP network connection. Only designated IP addresses will be allowed to access the HDS.

3. Existing non-BASIS supported security and access systems tie into the CPW via the Head-End Database Server (HDS) through a dedicated TCP/IP network connection from Cornell’s Central Station manufactured by Digitize, Inc.
C. Client Workstations

1. Client Workstations (CWs) can be located in the building or remotely. These terminals support the Best Access Systems’ BASIS Software System. The CWs selectively monitor alarms, trouble conditions, asset management information, administrative information, video management information, etc. delivered from the HDS. They can also be used to modify administrative information such as grant access levels to cardholders, define time zones, and generate reports.

2. Client Workstations (CW) shall be tied into the HDS across the network via a dedicated TCP/IP connection. Only designated IP addresses will be allowed to access the HDS.

3. The project is responsible to pay the costs associated with providing the dedicated TCP/IP connection to the CW location in the building.

D. System Operation and Performance

1. System operation and performance shall include, but not be limited to, the following features:
   a. Alarm initiation.
   b. Trouble initiation.
   c. Activation of alarm notification.
   d. Activation of trouble notification.
   e. Activation of fire safety functions.
   f. Total supervision, monitoring of abnormal conditions in the system.
   g. Monitoring generator status such as “failure to start” and “run,” where the security and access control panel is powered by a generator. Disregard this requirement if the building’s energy management system or fire alarm control panel monitors the generator status.
   h. Activation of off-premise signals that are sent to the HDS via the Digitize Central Station (existing non-BASIS supported systems) or Ethernet (BASIS supported systems).

2. Activation of the fire alarm system shall cause, but not be limited to, electric door strikes located on egress doors to lose power and allow egress.
3. Activation of any security device producing an alarm or trouble shall cause, but not be limited to:
   a. Transmission of the alarm or trouble signal to the Building ISC(s) and the Client Workstation(s) (CW).
   b. Transmission of the selected alarm or trouble signal to the Cornell Police Workstation (CPW), and the Head-End Database Server (HDS).
   c. Indication of the alarm or trouble condition at the computer monitor display at the CW, CPW, and HDS shall include the alarm or trouble description, time/date, building controller, device, input/output, priority code.

4. Activation of any card access device shall cause, but not be limited to:
   a. Transmission of the data signal to the Building ISC(s), the CW and HDS.
   b. Indication of the data signal including the alarm or trouble description, time/date, building controller, device, input/output, card, and priority code by the computer monitor display at the CW, CPW, and HDS.

5. Items 3 and 4 above define normal operations. In the event of a communication failure between an ISC and the HDS, these signals will be stored and forwarded to the HDS when the communication is restored. The HDS will report the communication failure as a trouble signal to the CPW while communication is interrupted.

1.02 POWER REQUIREMENTS

   A. Provide 110VAC power system requirements for a fully operational security and card access system.

   B. Provide 12VDC power for Best Access System boards, and 24VDC power for other peripherals.

1.03 COMMUNICATIONS SYSTEMS

   A. Provide communication system requirements for a fully operational security and card access system.

1.04 CABLE AND RACEWAY SYSTEMS

   A. Installations shall be performed to the current code requirements.
B. Cables shall be routed in raceway systems. Plenum cable is not acceptable.

C. Raceway systems shall be installed in a concealed manner; they shall be brought in above an accessible ceiling and fished inside the walls. Surface raceway systems are permitted where ceilings are inaccessible and walls cannot be fished.

D. Cabling shall be run in such a fashion so as to be kept at least 18" away from electric or data lines. In the event that a cable must cross over the path of an AC line, the cable must cross the path at a 90-degree angle to the AC line, thus keeping EMF interference to a minimum. Cabling must be kept at least 18" away from fluorescent lighting ballasts.

E. Cornell University’s Department of Planning, Design and Construction must approve any deviations in wire, raceway systems, or hardware prior to the signing of the contract that includes the said system, and prior to the commencement of any installations.

F. Cornell University Police must approve any deviations in hardware prior to the signing of the contract that includes the said system, and prior to the commencement of any installations.

G. Raceways shall be run from the field device to the head-end termination point in a professional manner, utilizing conduit, beam clamps, wire ties or other devices where necessary. In areas where the raceways are to be run above the drop ceiling, conduits shall be routed together where possible. Routing shall be in a workmanlike manner, with raceways mounted so as not to interfere with the servicing of other building infrastructure systems in the future. Electrical work shall conform to the latest local codes and the National Electric Code (NEC).

1.05 CONTRACTOR REQUIREMENTS

A. The Contractor providing the security and access system shall be certified NICET Level II, and per Article 6d of the New York State General Business Law.

1.06 IDENTIFICATION

A. Provide lettered identification plates on the following equipment, components, and accessories (Note: Lettered identification plates shall be approved by Cornell University’s Planning, Design and Construction Department prior to installation):

1. Building Intelligent System Controllers (ISCs);
2. Control Modules;
3. Interface Modules;
B. Provide Lettered “Dyno 100” labels on system devices.
   1. The label shall indicate the address and must be located on the device or adjacent to the device if this is not practical.
   2. Cabling and devices terminating at the control equipment shall be appropriately labeled with the proper device number or device description. Terminal blocks that are active shall be labeled with their appropriate landing site on the terminal board.

C. Identification Plates and Labels shall be as follows:
   1. ISCs shall be labeled ISC–U, where U is a value from 1-9.
   2. DRIs shall be labeled DRI–UVWX, where U indicates its respective ISC numeral; and V is the ISC’s respective buss, a value from 1 to 4; where WX are values from 01 to 32.
   3. Devices shall be labeled UVWXYZ, where U indicates its respective ISC numeral; and V is the ISC’s respective buss, a value from 1 to 4; WX indicates its respective panel, values from 01 to 32; Y indicates the input or output terminals, a value of 1 for input and 0 for output; and Z indicates its respective input or output terminal, a value from 1 to 4.
   4. Examples:
      a) ISC-2 is the second Intelligent System Controller in the building.
      b) DRI-2305 is the fifth Dual Reader Interface served from the third buss of the second Intelligent System Controller in the building.
      c) Device #230503 is the device on the third output of the fifth panel served from the third buss of the second Intelligent System Controller in the building.

1.07 MISCELLANEOUS REQUIREMENTS

A. Equipment shall be mounted in a manner consistent with the ability to work around such equipment, and to perform the normal duties required in that area without coming into contact with the control equipment. Control equipment shall be mounted at a convenient height for future servicing.

B. Power transformers shall be mounted in such a way that shall prevent their disengaging, either by vibration, gravity, or an individual unplugging them.

C. Equipment enclosures shall have locking mechanisms that are left locked. Two keys shall be provided. One key shall be supplied to the Building’s Coordinator, and the other key must be supplied to Cornell Campus Police.
1.08 APPROVALS

A. Cornell University Department of Planning, Design and Construction’s (PDC) Sr. Electrical Engineer, and the Cornell Police shall approve security systems designs. Coordinate the approval process with the Department of Planning, Design and Construction’s Project Manager on capital projects and the Sr. Electrical Engineer on non-capital projects.

1.09 TESTING AND ACCEPTANCE

A. A final test of the respective security and card access equipment and hardware shall be performed prior to considering the installation to be “complete.” Cornell’s Sr. Electrical Engineer and Campus Police shall be notified two weeks prior to the completion of the installation of a tentative testing date. On that date, a full system test will be performed according to these guidelines.

B. The Campus Police will give a pass or fail to the system after the test has been completed. When a portion of the system fails during the test, that portion, or the entire test will be tested again. The extent of the retest shall be up to the discretion of Cornell’s Sr. Electrical Engineer and Campus Police.

1.10 PROGRAMMING

A. Cornell’s Planning, Design and Construction Department shall accomplish the initial setup programming prior to the installation. A completed “Installation Checklist” for the facility shall be delivered and accepted by Cornell University’s Sr. Electrical Engineer prior to the installation of the system and the actual system programming.

B. Cornell University’s building coordinator, for the building implementing the security and access measures, shall supply Cornell University’s Sr. Electrical Engineer with the information pertaining to the population residing within, and the traffic patterns and times of operation therein.

1.11 WARRANTY

A. A warranty shall be provided for labor/workmanship and on hardware included in the installation, for a period of one (1) full year from the date of completion.
PART 2: PRODUCTS

2.01 CONDUIT, WIRE AND BOXES

A. Communication conductors shall be shielded twisted pairs; #22 AWG (minimum) stranded copper between the ISC and each downstream device. Manufactured by Belden, model #6541FE or equivalent.

B. Low-voltage power conductors shall be unshielded twisted pairs; #18 AWG (minimum) stranded copper between the power supplies and each downstream device. Manufactured by Belden, model #6342FE, or equivalent.

C. Card reader conductors shall be a minimum of 22 AWG/8-conductor, shielded, between card reader and reader interface. Belden model #6563FE or equivalent.

D. Egress device conductors shall be a minimum of 22 AWG/4-conductor between egress device and reader interface module. Belden model #6541FE or equivalent.

E. Door position switch conductors shall be a minimum of 22 AWG/4-conductor between egress device and reader interface module. Belden model #6541FE or equivalent.

F. Electric locking hardware conductors shall be a minimum of 18 AWG/2-pair, twisted, shielded between head-end power supplies and each downstream device. Belden model #6342FE or equivalent.

G. Security and Card Access circuits and wiring shall be installed in a separate and independent conduit system from other system circuits.

H. System wiring, circuits, and conductors shall be color coded and identified by number at termination points (i.e., control panels, remote annunciators, etc.) and splice points (i.e., junction boxes, splice boxes, etc.).

I. Junction and splice boxes containing card access system wiring, circuits, and conductors shall have black covers and marked “SECURITY” in ¾" (three-quarter inch) white letters.

J. End-of-line resistors in shall be installed at the location of the door contact or other sensor, not at the ISC.
2.02 DOOR HARDWARE

A. New door installations, opening hardware must conform with the 1991 Americans with Disabilities Act; either lever set, flip paddle, panic paddle or crash bar hardware is acceptable. Hinges must be on the secured side of the door (inside the protected area).

B. Existing door hardware may remain. Existing hinges located on the unsecured side of a door must be pinned with tamperproof screws or cotter pins.

2.03 ELECTRONIC LOCKING HARDWARE

A. Electronic hardware in the building shall use one standard voltage. Applications should operate on 12VDC and 24VDC voltage. Deviations from this voltage are unacceptable without prior written consent by the University’s Sr. Electrical Engineer. Existing electronic hardware that is not feasible to replace is an acceptable reason to deviate from this voltage. In applications where the teeth of the locking mechanism can be accessed from the outside of the door, a strike plate, or astragal, must be installed over the locking mechanism to prevent retraction of the teeth, allowing release of the door to an open condition.

B. Electronic locking hardware must be installed in a fail-secure configuration. Hardware installed on stairwell doors, perimeter doors, or doors exiting a space and emptying into an exit corridor or a common area must release to an unlocked position on any fire alarm activation.

C. Fail-Safe operation will be permitted only in instances where dictated by local fire or building codes.

D. For electric strike configurations, the strike must be installed in a flush-mounted configuration, properly adjusted to allow the anti-tamper mechanism on the lever set to be engaged. Surface-mount configuration will be allowed where warranted by the door configuration (i.e. concrete filled jamb) or by the hardware configuration (i.e. mechanical crash-bar).

2.04 INTELLIGENT SYSTEM CONTROLLERS (ISCs)

A. General

1. The project is responsible to pay the costs associated with providing the dedicated TCP/IP network connection to each ISC location.

2. There shall be only one Intelligent System Controller (ISC) per building complex. Multiple ISCs are unacceptable without prior written consent by the University’s Sr. Electrical Engineer. Acceptable reasons to use more than one ISC include the use of more than 64 card readers and situations where devices would be more than 4,000 ft. from a single ISC.
3. The integrated system including equipment, components, and accessories shall be UL listed for the purpose for which the equipment, components, and accessories are used.

B. Enclosures

1. Enclosures shall be of the 22 ga. heavy-gauge, galvanized steel, dead-front construction with keyed, lockable panel cover type.

2. Enclosures, panel covers, and trim rings shall be of surface, semi-flush, or flush-mounted design type, black in color, and assembled with tamper-proof screws. Panel shall be surface-mounted when installed in non-public spaces such as mechanical rooms, electrical rooms, and closets. Panel shall be flush mounted when installed in public spaces such as lobbies and corridors and should have tamper switches on the enclosure wired to the cabinet tamper inputs on the controller board.

3. Manufacturer: Best Access #BAS-CTX.

C. Intelligent System Controller Modules:

1. Host communications shall be 38.4Kbps direct wire TCP/IP, flash memory for real-time updates, with 1MB onboard memory expandable to 4MB. The TCP/IP is over Ethernet at 10mbps – the 38.4 is only for internal communications between the ISC and the Lantronix daughter-board.

2. Supports up to eight different card formats, with issue code support for both Wiegand and magnetic formats.

3. Will support maximum 64 readers or 32 downstream devices, and maximum 32,000 access levels, 255 Holidays with grouping, 255 time-zones, each with 6 time intervals.


5. Integral Lithium battery back up, with two dedicated inputs for tamper and power failure status.


2.05 INPUT CONTROL MODULES

A. General:

1. Locate its respective power source as close as physically possible, while maintaining proper service clearances.
2. Two inputs are for cabinet tamper and power fault monitoring. Normally, the contacts are closed. Short the inputs if not used.

3. Alarm inputs shall be supervised with end-of-line resistors that are 1000 ohm, 1% tolerance.

4. The Input Control Modules are intended for low voltage, class 2 circuits only.

B. Cabinet

1. Refer to ISC requirements for Input Control Module cabinet requirements.

C. Input Control Module:

1. Line supervision, with 12VDC power supply.

2. RS-485, 4-wire communications.

3. 16 programmable supervised input contacts (use end-of-line resistors).

4. Two form-C 5A, 30VDC contacts for load switching.

5. Two dedicated inputs for tamper and power failure status.


2.06 OUTPUT CONTROL MODULES

A. General:

1. Locate its respective power source as close as physically possible, while maintaining proper service clearances.

2. Two inputs are for cabinet tamper and power fault monitoring. Normally, the contacts are closed. Short the inputs if not used.

3. Alarm inputs shall be supervised with end-of-line resistors that are 1000 ohm, 1% tolerance.

4. Contact protection shall be used to minimize premature failure of the contacts and to increase system reliability.

5. The Output Control Modules are intended for low voltage, class two circuits only.
B. Cabinet
   1. Refer to ISC requirements for Input Control Module cabinet requirements.

C. Output Control Module
   1. Line supervision with 12VDC power supply.
   2. RS-485, 4-wire communications.
   3. 16 form-C 5A, 30VDC contacts for load switching that support “on”, “off”, and “pulse” control.
   4. Two dedicated inputs for tamper and power failure status.
   5. Manufacturer: Best Access #BAS-1200.

2.07 SINGLE READER INTERFACES (SRIs)

A. General:
   1. Locate its respective power source as close as physically possible, while maintaining proper service clearances.
   2. Two supervised inputs are for exit request (normally open) and door contact (normally closed) monitoring.
   3. Alarm inputs shall be supervised with end-of-line resistors that are 1000 ohm, 1% tolerance.
   4. Two output relays support fail-safe and fail-secure operation. One relay shall be used for the strike and is capable of 5mA; the other relay may be used for auxiliary functions and is capable of 1mA.
   5. Provide end-of-line resistor at the end of the communications line. If the Single Reader Interface is at the end of the RS-485 line, the J4 termination jumper must be set.

B. Power:
   1. Provide a 12VDC, 125mA power input.
   2. 80mA is available from Single Interface Reader for reader TTL power.
   3. Circuit with 18AWG (minimum) twisted pair cable.
C. Upstream Communication:
   1. Port 1, using 2-wire RS-485 interface, is used to communicate with the Intelligent System Controller.
   2. RS-485 interface cable shall be a minimum 24 AWG twisted shielded pair.
   3. Cable drops to devices from the Single Interface Reader should be kept to a minimum. Drops should not exceed 10 feet.

D. Manufacturer:
   1. Manufacturer: Best Access #BAS-1300.

2.08 DUAL READER INTERFACE MODULES (DRI's)

A. General:
   1. Locate its respective power source as close as physically possible, while maintaining proper service clearances.
   2. Eight supervised inputs, four per door. Inputs per door are for exit request (normally closed), door contact (normally open), and two auxiliary monitoring points (selectable through the software).
   3. Alarm inputs shall be each supervised with two end-of-line resistors that are 1000 ohm, 1% tolerance for a total of 2000 ohms.
   4. Six output relays support fail-safe and fail-secure operation. All six relays are capable of 5mA apiece. Relays per door are for the strike and two auxiliary relays.
   5. Provide end-of-line resistor at the end of the communications line. If the Dual Reader Interface is at the end of the RS-485 line, the J5 and J6 termination jumpers must be set.

B. Power:
   1. Provide a 12VDC, 450mA power input.
   2. 80mA is available from Dual Interface Reader for reader TTL power.
   3. Circuit with 18AWG (minimum) twisted pair cable.
C. Upstream Communication:

1. Port 1, use 2-wire RS-485 interface, is used to communicate with the Intelligent System Controller.

2. RS-485 interface cable shall be a minimum 24 AWG (minimum) twisted shielded pair.

3. Cable drops to devices from the Dual-Interface Reader should be kept to a minimum. Drops should not exceed 10 feet.

D. Manufacturer:

1. Manufacturer: Best Access #BAS-1320.

2.09 CARD READERS

A. The card readers shall be wall-mounted adjacent to the door, on the knob set/handle or opening side. The reader shall be mounted 44" from floor level to the top of the reader. The reader shall be placed in a vertical position, with the LED at the top of the reader.

B. For double door installations, the reader shall be wall-mounted or doorframe-mounted on the hinge side of the door that contains the knob set/handle hardware. The other door must have the capabilities to be locked in a closed position.

C. Key override hardware shall not be accessible from the non-secured side of the door, other than the integral opening hardware. Key override hardware on existing doors shall be removed from the non-secured side of the door.

2.10 BATTERY BACK-UP POWER SUPPLY

A. Battery Back-Up Power Supply

1. Batteries shall be of the sealed, lead-acid, or vented nickel-cadmium type.

2. Batteries shall be capable of providing operating and supervisory power for a minimum of fifty-five (55) amp/hours in buildings that are not provided with an emergency generator power supply, and four (4) amp/hours in buildings that are provided with an emergency power supply.

3. Batteries shall be capable of providing operating power to operate alarm signals for a minimum of an additional five (5) minutes after the above time period has elapsed (i.e., in addition to either fifty-five amp/hours in buildings not provided with emergency generators, or in addition to four amp/hours in buildings that are provided with emergency generators).
4. Batteries shall be mounted in a separate enclosure of similar type to the main control panel.

5. The Engineer of Record shall provide battery calculations to Cornell University’s Sr. Electrical Engineer during the submittal process and at the completion of the project.

2.11 INTRUSION DETECTION CONTACTS

A. On standard man doors, the contact shall be mounted in the top of the doorframe, 6" in from the opening edge of the door.

B. The electronic configuration for IDS contacts is normally closed and supervised.

2.12 EGRESS MOTION DETECTORS

A. Egress motion detectors shall be ceiling mounted whenever possible. When the detector must be wall or frame mounted above the door, it will be angled down as far as possible, to provide the proper coverage.

B. The coverage pattern shall reach from the detector to the level of the floor, and shall not protruding more than 12" out from the surface of the door, nor more than 6" past the doorframe on either side. Masking of the detector is acceptable to meet the coverage pattern.

C. Use of motion detection for egress is unacceptable in high traffic areas.

2.13 ACCEPTABLE MANUFACTURERS

A. The card access system shall be a complete operating system of one manufacturer.

B. The equipment, components, and accessories shall be as specified by Planning, Design and Construction. Requests for authorization to substitute, vary or change the specified equipment, components or accessories of the approved manufacturer may be submitted, in compliance with Cornell University’s Design and Construction Standards (see Section 01001 - General Requirements), to Planning, Design and Construction prior to the Contractor’s submission of the invitation-for-bid proposal.

C. Best Access shall be the manufacturer of new security and card access systems. Other manufacturers are unacceptable.