SECTION 281300

ACCESS CONTROL

PART 1 GENERAL

1.1 STIPULATIONS

A. The specifications sections “General Conditions of the Construction Contract”, “Special Conditions”, and “Division 1 - General Requirements” form a part of this Section by this reference thereto, and shall have the same force and effect as if printed herewith in full.

1.2 SUMMARY

A. This Section includes an extension of the existing Access Control System to add card readers where indicated.

B. The existing Access Control system is the Verint Nextiva SMC PSIM (Physical Security Information Management) system at the Capitol complex.

C. Related Requirements:

1. Section 087100 “Door Hardware” for hardware devices for connections to security system.

1.3 DEFINITIONS

A. Controller: An intelligent peripheral control unit that uses a computer for controlling its operation.

B. CPU: Central processing unit.

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

D. dpi: Dots per inch.

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

F. GFI: Ground fault interrupter.

G. 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.

H. I/O: Input/Output.

I. LAN: Local area network.

J. 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 a TIA 485-A communications loop. Where this term is presented with an initial capital letter, this definition applies.

K. PC: Personal computer. Applies to the central station, workstations, and file servers.

L. PCI Bus: Peripheral Component Interconnect. A peripheral bus providing a high-speed data path between the CPU and the peripheral devices such as a monitor, disk drive, or network.

M. PDF: Portable Document Format. The file format used by the Acrobat document-exchange-system software from Adobe.

N. RF: Radio frequency.

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

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

Q. 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.

R. UPS: Uninterruptible power supply.

S. USB: Universal serial bus.

T. WAN: Wide area network.

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

V. Windows: Operating system by Microsoft Corporation.

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

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

1.4 SUBMITTALS

A. Product Data: For each type of product indicated. Include rated capacities, operating characteristics, and 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. Qualification Data: For qualified Installer, submit all required training certifications.

C. Refer to Section 018113 “Sustainable Design Requirements” for requirements of sealants, primers, paints, adhesives, caulk, aerosols, and coatings.

1.5 QUALITY CONTROL

A. User and Administrative Account Control: Default administrator and user passwords shall not be used. Update and document all system administrator passwords prior to turning system over to the Department and Client Agency.

B. 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.

C. Source Limitations: Obtain central station, workstations, controllers, Identifier readers, and all software through one source from single manufacturer.

D. Electrical Components, Devices, and Accessories: Listed and labeled as defined in NFPA 70, by a qualified testing agency, and marked for intended location and application.

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

F. Comply with SIA DC-0, SIA DC-03 and SIA DC-07.

G. IBC 1708.5 Electrical equipment. Each manufacturer of designated seismic system components shall test or analyze the component and its mounting system or anchorage and submit a certificate of compliance for review and acceptance by the registered design professional in responsible charge of the design of the designated seismic system and for approval by the building official. The evidence of compliance shall be by actual test on a shake table, by three-dimensional shock tests, by an analytical method using dynamic characteristics and forces, by the use of experience data (i.e., historical data demonstrating acceptable seismic performance) or by more rigorous analysis providing for equivalent safety. The special inspector shall examine the designated seismic system and determine whether the anchorages and label conform with the evidence of compliance.

PART 2 PRODUCTS

2.1 MANUFACTURERS

A. Manufacturers: Subject to compliance with requirements, provide products by the following:

1. Open Options.

a. The above item has been approved by the Department as a Proprietary Item. No other item will be accepted. Article 9, Paragraph 9.6, Substitution of Materials, of the General Conditions to the Construction Contract does not apply to the above item.

2.2 CARD READERS, AND KEYPADS

A. Manufacturer: HID iClass series.

B. Card-Reader Power: Powered from its associated controller, including its standby power source, and shall not dissipate more than 5 W.

C. 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.

D. Enclosure: Suitable for surface, semi-flush, pedestal, or weatherproof 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.

E. Display: Digital visual indicator shall provide visible and audible status indications and user prompts. Indicate power on or off, whether user passage requests have been accepted or rejected, and whether the door is locked or unlocked.

F. Touch-Plate and Proximity Readers:

1. Active-detection proximity card readers shall provide power to compatible credential cards through magnetic induction, and shall receive and decode a unique identification code number transmitted from the credential card.
2. Passive-detection proximity card readers shall use a swept-frequency, RF field generator to read the resonant frequencies of tuned circuits laminated into compatible credential cards. The resonant frequencies read shall constitute a unique identification code number.
3. The card reader shall read proximity cards in a range from direct contact to at least 6 inches (150 mm) from the reader.

G. Communication Protocol: Compatible with local processor.

H. Touch-Plate and Contactless Card Reader: The reader shall have "flash" download capability to accommodate card format changes. The card reader shall have capability of transmitting data to security control panel and shall comply with ISO/IEC 7816.

I. Credential Card Modification: Entry-control cards shall be able to be modified by lamination direct print process during the enrollment process without reduction of readability. The design of the credential cards shall allow for the addition of at least one slot or hole to accommodate the attachment of a clip for affixing the credential card to the badge holder used at the site.

J. Card Size and Dimensional Stability: The Client Agency credential cards are 2-1/8 by 3-3/8 inches (54 by 86 mm). The credential card material is dimensionally stable so that an undamaged card with deformations resulting from normal use shall be readable by the card reader. Card readers shall be compatible with the Client Agency’s cards.

1. No new cards are required.

2.3 DOOR AND GATE HARDWARE INTERFACE

A. Exit Device with Alarm: Operation of the exit device shall generate an alarm and, where indicated in Section 087100 “Door Hardware” specification, annunciate a local alarm. Exit device and alarm contacts are specified in Section 087100 "Door Hardware."

B. 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 they shall report a forced entry. Power and signal shall be from the controller. Electric strikes are specified in Section 087100 "Door Hardware."

C. 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 Section 087100 "Door Hardware."

2.4 DOOR CONTACTS

A. Flush, Concealed:

1. Coordinate door and frame preparations with door and frame suppliers.
2. Switches shall be installed recessed in frame head approximately 4" from latching door edge.
3. Self-lock mounting.
4. Hermetically sealed reed switch, encapsulated in polyurethane.
5. Life Cycle: 100,000 full load, 10,000,000 dry circuit.
6. Sense Range: 0.5” nominal.

2.5 REQUEST TO EXIT DEVICES

A. Monitor request to exit devices and shunt Access Control System alarm signals from doors opened by authorized request to exit inputs. Request to exit devices may be integrated with electric locking hardware per Section 087100 “Door Hardware.”

B. Where not part of an integrated locking device, provide request to exit motion sensor above doorway on the secured side unless otherwise indicated.

2.6 CABLES

A. Manufacturers:

1. Belden Inc.; Electronics Division.
2. Berk-Tek; a Nexans Company.
3. General Cable Technologies Corporation.
4. Mohawk/CDT; a division of Cable Design Technologies.
5. West Penn Wire/CDT; a division of Cable Design Technologies.
6. Or approved equal complying with specified requirements.

B. General Cable Requirements: Comply with requirements in Section 280513 "Conductors and Cables for Electronic Safety and Security" and as recommended by system manufacturer for integration requirement.

C. Paired, PVC, Reader Cables:

1. Three 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.

2. NFPA 70, Type CMP plenum rated.

2.7 TRANSFORMERS

A. NFPA 70, Class II control transformers, NRTL listed. Transformers for security access-control system shall not be shared with any other system.

PART 3 EXECUTION

3.1 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.

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.

3.2 PREPARATION

A. Comply with recommendations in SIA CP-01.

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

3.3 CABLING

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

B. Wiring Method: Install wiring in raceway within wall. In accessible ceiling spaces where unenclosed wiring method may be used. Use NRTL-listed plenum cable. Conceal raceway and cables except in unfinished spaces.

C. 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 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.

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

3.4 CABLE APPLICATION

A. Comply with TIA 569-D, "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. TIA 232-F Cabling: Install at a maximum distance of 50 ft. (15 m).

D. TIA 485-A Cabling: Install at a maximum distance of 4000 ft. (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 ft. (75 m), and install No. 20 AWG wire if maximum distance is 500 ft. (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 250 ft. (75 m).

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

3.5 GROUNDING

A. Comply with Section 260526 "Grounding and Bonding for Electrical Systems."

B. Comply with IEEE 1100, "Recommended Practice for Power and Grounding 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.

3.6 INSTALLATION

A. Controllers: Shall be installed above the ceiling on the secured side of the doors.

B. Card Readers: Shall be installed as indicated on the detail drawings unless specifically indicated otherwise on the project drawings. The system supplier shall furnish manufacturers' backboxes. The electrical contractor shall provide all other required backboxes.

C. Electrified Door Hardware: Coordinate the installation requirements with the hardware supplier and install the power supplies. Provide connections to all required power supplies. Door openers, door locks, electric hinges, and pushbars shall be installed by the electrical contractor.

3.7 IDENTIFICATION

A. 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.

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

3.8 FIELD QUALITY CONTROL

A. Perform tests and inspections.

1. Manufacturer's Field Service: Engage a factory-authorized service representative to inspect components, assemblies, and equipment installations, including connections, and to assist in testing.

B. Tests and Inspections:

1. 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.
2. 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.

C. Devices and circuits will be considered defective if they do not pass tests and inspections.

D. Prepare test and inspection reports.

3.9 STARTUP SERVICE

A. Complete installation and startup checks according to approved procedures that were developed in "Preparation" Article and with manufacturer's written instructions.

3.10 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, "Server Burglar-Alarm Units," during periods when a qualified operator in the employ of Contractor is not present.

3.11 CYBERSECURITY RISK MITIGATION

A. Coordinate with Department and Client Agency IT personnel to restrict external network access to Internet connected system through virtual private network (VPN) connections only.

B. Security Event Log: Coordinate with the Department and Client Agency IT personnel to configure security event logging. Access to security logs shall be limited to users with proper authentication. Security logs shall be time stamped with Time and Date metadata for auditing and back-up.

C. Disable any protocols for remote connectivity, unless constantly required for day-to-day operations.

D. All external transport data shall be routed through encrypted channels with 2048-bit secure sockets layer (SSL).

E. Coordinate with Department and Client Agency IT personnel to implement a Web server-based human machine interface (HMI) that relies on IT technologies to secure access and restrict ports that can be opened on the firewall. Coordinate with Department and Client Agency IT personnel to restrict access to known IP addresses only.

F. Where building system networks are not physically separate from IT business networks, coordinate with Department and Client Agency IT personnel to segregate networked and Internet connected systems from the IT business network using virtual local area network (VLAN) IT technologies to restrict internal attacks/breakdowns.

G. Set unique, cryptographically strong passwords for administrator and user accounts. Default passwords must be changed before systems are connected to the Department and Client Agency IT personnel.

H. Collect only the data that is necessary for analytics and optimization.

I. References:

1. NIST Special Publication 800-14 – Generally Accepted Principles and Practices for Securing Information Technology Systems.
2. NIST Special Publication 800-54 Revisions 4 – Security and Privacy Controls for Federal Information Systems and Organizations.
3. Defense Security Service Office of the Designated Approving Authority – Master System Security Plan (MSSP) Template for Peer-to-Peer Networks (June 2011, Version 3.0).
4. IEC 62443: Industrial Network and System Security

END OF SECTION 281300