SECTION 28 13 00 – ACCESS CONTROL

1.1 GENERAL

A. This Section defines the general design requirements for an Electronic Access Control System that shall be followed for all OFCC Technology construction projects.

B. Refer to Sections 8500, Technology Systems, 28 16 00 Intrusion Detection System, and 28 23 00 Video Surveillance System for additional information.

1.2 QUALITY ASSURANCE

A. National Fire Protection Association.

B. NFPA 730 – Guide for Premises Security

C. NFPA 731 – Standard for the Installation of Electronic Premises Security Systems

D. National Electric Code.

E. American with Disabilities Act.

F. Underwriter's Laboratory.

G. Latest ANSI TIA/EIA-568, 569, 606, 607 Standards and Eleventh Edition (or later).

H. BICSI Telecommunications Distribution Methods Manual (TDMM).

1.3 SYSTEM WARRANTY

A. The Access Control System and software shall be fully warranted for one (1) year from date of substantial completion by the contractor and manufacturer. If any defects are found within this warranty period, the defective system component shall be replaced at no extra cost to the Owner for parts or labor. Provide a statement of this warranty with the O&M manuals and to the Director of IT. Make available a service contract offering continuing factory authorized service of this system after the initial warranty period.

1.4 GENERAL

A. Base System - Furnish an Access Control System (ACS) to provide automated control and credential-based access to building perimeter and interior spaces. In addition, the ACS, where required by the Owner, shall have a complete suite for badge creation/printing and basic visitor management. Provide an Integrated Security Management (ISM) system that provides a simple and easy-to-use graphical user interface incorporating aspects of Electronic Access Control, Intrusion Alarm, Video Management, Visitor Management, Background Checks, and Intercom systems.

B. The ACS shall be configured as a distributed system with centralized server, and control panels located either in TR spaces or out at each controlled portal. Owner wide solutions may have fail over servers. The servers can be virtualized.

1. In the event of a communications failure between the host server and the remote controllers, the controllers shall continue to make local access control decisions and save all transactions in memory until communications are restored. At that time the controller shall upload all stored transactions to the Central Server.

C. When a Owner has more than one building, the Central Server shall be in one of the owner's buildings and the other buildings shall be attached to the Central Server via the Wide Area Network. All buildings in the owner shall interface to the Central Server and Control Consoles.

D. Provide a minimum of one (1) complete workstation with monitor/keyboard/mouse in each building, pre-loaded with all EACS software and clients.

E. Provide a minimum of one (1) complete workstation with monitor/keyboard/mouse/camera/printer in owner, pre-loaded with all required EACS software and clients.

F. Credential Readers supporting various technologies shall provide data from user credentials via a door control unit that includes the electrical interface to the reader as well as inputs for door sensors and relays for outputs.

G. The following doors shall have ACS at a minimum.

1. Main Entry and Secure Vestibule
2. Additional Public/Event Exterior Entrances
3. Staff Exterior Entrances
4. Kitchen Delivery Exterior Entrance
5. Loading Dock Exterior Pedestrian Door Entrance.
6. Communications Main Equipment Room

H. Avoid providing key locks and dogging hardware on doors which have ACS control.

1.5 DOOR CONTROL

A. The system shall include door control modules to accept inputs from door sensors, credential readers, and other door control inputs, and provide lock/unlock functionality to local controlled doors.

B. System shall utilize distributed Architecture which allows door access information to be stored locally for continuous operation in the event of loss of network connectivity to system server.

C. Panels to be located in the TR spaces or locally at each door and provided with IP connectivity.

D. Power for panels to be sourced from building generator with battery back-up for short duration operation.

E. Provide panels for elevator control.

F. Optional – Provide I/O panels and other hardware for connection to building paging systems, Building Energy Management System, and Building door intercom systems.

G. Door access is granted based upon door group, user group, individual user, and TOD schedules.

H. Controllers provide additional interface with automatic door openers, local door intercom door release, remote push button door release, and system wide threat level settings.

1.6 CREDENTIAL READERS

A. System to utilize multi-technology readers that can utilize proximity and smart cards. Options for keypads and biometrics as required by Owner.

B. Readers shall have the ability to perform standard lock/unlock operation as well as secondary specialized functions with double/triple taps, etc.

C. Readers located in elevator cab where required to restrict access.

1.7 DOOR HARDWARE

A. Controlled doors to be provided with electronic locks consisting of electric strike, electric latch, electrified panic, electrified trim, integrated locksets (reader built into hardware) or electromagnetic lock. Electronic door hardware to be provided with low voltage power from either local power supplies or centralized power supplies in the TR spaces.

B. Door locks to be operated on building generator and/or battery power for a fully functioning opening in the event of the loss of normal building power.

C. Access controlled doors to be provided with request to exit alarm shunt devices (hardware based or local PIR motion detector) to prevent forced-door alarms upon valid egress.

D. Access controlled doors to be provided with door position switches.

1. All exterior doors have door position switches and have the door status monitored through the ACS.

E. Optional – Access controlled doors to include latch position/lock monitoring hardware.

F. Wireless door locking hardware should be considered, recommend real time monitoring with full alarm functionality and battery life monitor.

G. Consider integrated locksets with direct network connection and Power of Ether (PoE) lock power on a single CAT 6 drop.

H. Infrastructure at each controlled door including wall boxes, door frame connections, conduit and low voltage power and control cabling.

1.8 BADGE/CREDENTIAL CREATION

A. Equipment to create and print single or double sided, color credential cards including PC workstation with color camera and color 2-sided badge printer. Provide quantity of stations as required by Owner's program and use requirements.

1.9 VISITOR MANAGEMENT

A. Provide visitor management software module along with workstation and color camera and printer to enroll visitors and create and print out visitor badges,

B. Optional – Provide enhanced features including license reader and on-line sex offender database look-up.

1.10 SOFTWARE

A. Graphical Maps

1. System to provide graphical maps with building floor plans which include real-time, m interactive icons for all controlled points. Maps to allow quick access to perform basic lock/unlock/status functions at individual doors.

B. Reports

1. System to provide both pre-configured and custom configurable system wide reports on all levels of activity throughout the system.

C. Alarm Log

1. System to provide a real time alarm/event log which displays system events in real time with provisions for acknowledging events, silencing alarms, searching for events, etc.

D. User Management

1. System to provide interface for creation and management of individual users including totally customizable user information fields.

E. Door Management

1. System to provide interface for creating and managing individual doors and control points along with groups, rules-based privileges, threat levels, time of day schedules,

F. System Management

1. System to provide real time monitoring and status of all connected hardware and servers.

G. CCTV Integration – Provide direct network or serial based communications with CCTV system to tie alarm events to video surveillance system, to provide access to live video through the EACS interface and icons on the graphical map,

H. Intrusion Alarm Integration - Provide direct network or serial based communications with Intrusion Alarm system to activate functions on the alarm system based upon card reader input, and to incorporate alarm points in the live view and graphical map interfaces.

I. Building Paging Integration – Provide interface to broadcast pre-recorded messages based upon ACS activity such as change in threat level, lock-down, etc.

1.11 OPTIONAL

A. Building Management Integration – Provide interface and programming to trigger building systems such as A/C, lighting, etc. by ACS events such as first card reader in.

B. Door Intercom Integration – Provide interface with door intercom system to allow remote unlock of doors through intercom master stations.

1.12 SPECIAL OPERATIONS

A. Provide secure vestibule operation at main entry with outer entrance doors, inner vestibule doors, and Office Entry Door each controlled as a separate point.

B. Provide panic duress capability in the Main Office, Principal/Vice Principal Office, Counselor's Office, and other areas identified by the Owner.

1.13 TRAINING

A. Provide training to the owner's personnel. Training session(s) shall cover the following topics at a minimum:

1. System Equipment Connectivity
2. Device Configurations
3. Operation, maintenance, and upgrade procedures.

B. Training to be arranged with Owner personnel and as required based upon a new system or a system expansion.

C. Training occurs in maximum of 2-hour increments per personnel or groups or personnel.

D. Consider requiring Contractor to provide manufacturer training vouchers for a portion of the training, which are valid during the warranty period.

E. Training shall be by a certified manufacturer instructor.

F. The training schedule shall be coordinated with Owner personnel and their needs.

G. Training plan, timeline, and agenda shall be provided to Owner IT personnel and signed off by Owner and Contractor.

H. Warranty certificate and agreement shall be provided to Owner IT personnel at the initial training session.

I. Provide a digital video copy of the training sessions.

END OF SECTION