SECTION 28 10 00

ELECTRONIC ACCESS CONTROL AND INTRUSION DETECTION

PART 1 – GENERAL

1.1 PURPOSE

A. This guideline is intended to provide useful information to the Professional Service Provider (PSP) to establish a basis of design. PSP is to apply the principles of this section such that the University of Texas at Arlington (UTA) may achieve a level of quality and consistency in the design and construction of their facilities. Deviations from these guidelines must be approved by UTA and may require justification through Life Cycle Cost (LCC) analysis and submitted to UTA for approval.

1.2 **LESSONS LEARNED AND DESIGN CONSIDERATIONS**

A. X

1.3 SUMMARY/OVERVIEW

A. This section provides specifications for the installation of Electronic Access Control (AC), Intrusion Detection (ID) and related components.

B. Related Sections

1. Section 08 71 00 – Door Hardware
2. Section 26 00 00 – Electrical (including related sub-sections)
3. Section 27 00 00 – Communications
4. Section 28 00 00 – Electronic Security
5. Section 28 05 00 – Racks and Enclosures
6. Section 28 23 00 – Video Surveillance
7. Section 28 26 00 – Emergency Intercommunications and Duress
8. Section 28 31 00 – Fire Alarm and Smoke Detection

1.4 REFERENCES

A. Section 28 00 00 – Electronic Security

1.5 SYSTEM COORDINATION

A. The Security Integrator shall completely coordinate all relevant work of other trades/systems including, but not limited to:

1. Door Hardware
2. Fire Alarm System
3. Elevator Control System
4. Electrical Systems(s)
5. Telecommunications System(s)

B. Electric Locking Mechanisms

1. The security integrator and door hardware contractor shall coordinate all door hardware, door and door frame design.
2. The security contractor shall verify all specified door hardware is appropriate for the security application and verify the sequence of operations for each access controlled opening.

C. Fire Alarm and Life Safety

1. The security integrator shall coordinate the access control system design with the life safety consultant to insure compliance with applicable codes and requirements.
2. This includes, but is not limited to:
   a. Fire alarm interface
   b. Fail safe/fail secure locking mechanisms
   c. Delayed egress

1.6 GENERAL SYSTEM DESCRIPTION

A. General Requirements

1. Furnish all labor, materials, tools, equipment, and services for a complete security system as indicated and

in accordance with provisions of the contract documents.
2. Although such work is not specifically indicated, furnish and install all supplementary or miscellaneous items, and devices incidental to or necessary for a sound, secure and complete installation.
3. Comply with the provisions of Division 1 for General Requirements.
   a. In the event of a conflict between the provisions of this Section and Division 1, the more stringent provisions shall apply.
4. All system devices and components included shall be compatible.

B. The facility shall be equipped with an AC/ID system that is an extension of the existing CBORD CS Gold system maintained by the UT Campus Card Operations.
1. All work required within the facility for extension of the AC/ID system to the existing system head end shall be furnished and installed by the project security contractor.
2. Contractor to coordinate with Owner to provide additional inputs to the system as required and ensure all interfaces and integration is completed prior to commissioning.

C. The AC/ID system will support the needs of the project in accordance with these specifications.
1. The AC/ID system shall have the capability for future expansion to support the security needs of the completed facility.

D. The AC/ID system shall be interfaced with the Fire Alarm system (by others) as required to comply with all building code requirements.

E. Emergency/UPS power will be utilized to power the AC/ID system's computer workstation (client) at the Security head end equipment location.

F. Emergency/APS power will be utilized to power the AC/ID system's Data Gathering Panels and control components as required throughout the facility.

1.7 ACCESS CONTROL SYSTEM

A. The AC system will consist of multi-technology card readers, wireless and wired card readers, door status switches, and request-to-exit sensors operating in conjunction with associated electric door hardware.
1. Card readers and adjunct devices shall be provided as shown on the drawings.
   a. Provide card readers, Access Control Panel, and alarm input and output devices connected to the security management system via Local Area Network (LAN).
   b. The security integrator shall coordinate network and IP address requirements with Owner to identify the Medium Access Control (MAC) address (Layer 2) of each provided device, the location to be installed, and the port configuration needed for communication.
   c. Furnish all labor, materials, tools, equipment, and services for a complete system as indicated and in accordance with provisions of the contract documents.
   d. Although such work is not specifically indicated, furnish and install all supplementary or miscellaneous items, and devices incidental to or necessary for a sound, secure and complete installation.

B. Card readers will have capability to use magnetic stripe technology, and work such that upon swipe of a valid access card, the unique card data shall be transmitted to an associated control panel where the data is compared to an authorized user database and access is approved or rejected accordingly. All card readers shall be compatible with the current access control system – CBORD CS Gold.
1. A valid authorization will activate operation of the electric lock and shunt the door status switch. The alarm shunt will not affect supervision of the detection circuit.
2. Coordinate with owner on card format and other pertinent details.

C. Door status switches and electromagnetic lock bond sensors at card reader controlled locations serve to indicate the open/closed status of the associated door and shall establish the basis for reporting a door-propped or unauthorized entry condition.
1. Security contractor is responsible for coordinating the contact configuration (SPDT) (DPDT) and rating for door status switches and electromagnetic lock bond sensors, and for connection of switches with the AC.

D. Unless noted otherwise, the Door Contractor shall be responsible for providing all flush mounted door status switches and electromagnetic bond sensors as indicated on drawings.

E. Electrified door hardware for card reader controlled doors will include electrified locksets, electric exit devices, and electric power transfer as shown on the drawings.
1. All electrified door hardware shall be provided under the work of Division 08 unless otherwise noted.
2. Unless noted or specified otherwise, the Security contractor will provide all security cables and, low voltage power supplies for operation of electrified door hardware associated with card reader controlled

doors.

3. The Division 08 contractor will provide lock wiring between power transfer/power transfer hinge and lock.

F. Request-to-exit (REX) devices at designated card reader controlled doors shall cause the associated door status switch alarms to be shunted.
   1. The alarm shunt shall not affect the supervision of the alarm detection circuit.
   2. All electrified Locksets and Exit Devices connected to the access control system shall have an integral REX switch.
      a. Security contractor shall connect to REX switch (by Division 08).
         1) Coordinate with Division 08 to ensure proper REX switch configuration.
         2) Security contractor shall wire a REX output to the Access Control Panel REX input. The configuration shall be non-resettable and activate for two seconds.
         3) Security contractor shall wire a REX output in series with the lock power circuit to disconnect lock power.
      b. Provide a Passive Infrared (PIR) REX motion sensor as a primary REX device. **These are not allowed unless approved by the University. They are applicable to magnetic locks which are not allowed on campus without approval from Campus Card Operations, Office of Facilities Management, and Environmental Health & Safety.**
         1) Security contractor shall wire a PIR REX output to the Access Control Panel REX input. The configuration on this motion shall be non-resettable and activate for two seconds.
         2) Security contractor shall wire a PIR REX output in series with the lock power circuit to disconnect lock power when motion is sensed.
         3) The PIR REX shall be located to avoid detection more than three feet from the door and at the door bottom sweep. Deter under door spoofing attacks by pointing the sensor away from the door threshold. Position the sensor to detect motion at the door handle or door push plate.
      c. Provide a UL listed DPDT REX push button as a secondary REX device at doors without hardware integrated REX switch (by Division 08). **These are not allowed unless approved by the University. They are applicable to magnetic locks which are not allowed on campus without approval from Campus Card Operations, Office of Facilities Management, and Environmental Health & Safety.**
         1) Security contractor shall wire the REX switch as described for the above motion sensor, to disconnect lock power and activate the Access Control Panel REX input.
         2) Locate within 6’-0” of the door push-plate/handle. Coordinate accessibility requirements with the Architect.

G. Card Reader Controlled Automatic Sliding ‘Storefront’ Doors
   1. Interface the Access Control System to the Automatic Sliding ‘Storefront’ Doors to activate/deactivate locking solenoid**, which must be included in door installation,** and to enable and disable the outside motion detector (by Division 08 Contractor).
   2. The egress motion detector shall always unlock and open the sliding door and send a signal to the system to shunt the notification of an intrusion alarm.

H. Card Reader Controlled Elevators
   1. The system shall provide for card reader control of Elevator Floor select buttons within the elevator cab.
   2. When the elevator controls are in Card Access mode, a programmed card shall enable the floor select buttons allowing the user to select the appropriate floor select button for access which he or she has access to. If a card is not presented at the card reader after a button has been pushed, the doors will open, allowing the person to exit the cab. This will also prevent the person from riding the elevator if the cab is called from another floor.
   3. The contractor shall provide a relay for every floor in every cab.
      a. Example: 3 floors and 2 cabs = 6 relays.
   4. The system shall allow button selection for 5 seconds per valid card read.
   5. When the elevator is in free access, the floor select buttons shall operate normally.

I. Door Management Unit (DMU) – Local Annunciator
   1. Designated door will be equipped with a DMU to sound a local alert when doors are propped open beyond a field programmable time delay.
      a. The DMU audible alert will be a recording or tone prompting people in the area to close the door.
      b. The DMU shall report a door propped alarm to the AC/ID after a field programmable delay.
      c. The delay will be sufficient for people in the area to correct the security violation or as directed by

the Owner.

J. Tamper Switches. **These are not widespread on campus since most of the equipment is located in the HUB room.**
   1. Provide closed circuit tamper switches to monitor the secure status of all security enclosures, power supplies, terminal cabinets, power distribution units, and other Security System cabinets and enclosures.
   2. Fasten tamper switches within the cabinet to provide no access to the switch and fasteners when the cabinet is closed.
   3. Provide independent supervised monitoring of tamper conditions for each cabinet.
      a. Include the number of tamper switches in the total alarm input figures.

1.8 SUBMITTALS
A. Follow provisions of Section 28 00 00 for additional requirements.
B. Field Test Reports
   1. Upon completion and testing of the installed system, test reports shall be submitted in booklet form and electronic media showing all field tests performed on, and adjustments made to each/any component and all field tests performed to prove compliance with the specified performance criteria.
   2. Indicate and interpret test results in written form and verbally to owner for compliance with performance requirements at a pre-scheduled meeting.
C. Battery calculations to show the expected loads and backup duration for power supplies and UPS devices for all active AC/ID equipment.
D. Security Contractor is responsible to prepare and submit as required to the AHJ any and all information to obtain an Electronic Locking Mechanisms permit.

1.9 QUALITY ASSURANCE
A. Follow provisions of Section 28 00 00.
B. Spare Parts:
   1. Provide two (2) spare components for every model and configuration of electronic components and devices used on the project as spare parts inventory.
      a. The security integrator will turn over the new and unused components and devices to the owner at project closeout.

1.10 DELIVERY, STORAGE AND HANDLING
A. Follow provisions of Section 28 00 00.

1.11 PROJECT/SITE CONDITIONS
A. Follow provisions of Section 28 00 00.

1.12 WARRANTY
A. Follow provisions of Section 28 00 00.
B. All devices and components shall comply with applicable U.L. standards.

PART 2 – PRODUCTS

2.1 ACCEPTABLE SYSTEM MANUFACTURERS
A. AC System Platform Software
   1. CBORD
      a. CS Gold

2.2 ACCEPTABLE ACCESS CONTROL MANUFACTURERS
A. Access Control Data Gathering Panels
   1. CBORD compatible
   2. Owner Approved Equivalent
B. Card Readers <CR>
   1. Allegion Aptiq MTMSK15 (with Keypad)
   2. Allegion SMR5 or CBORD MR-5
   3. Owner Approved Equivalent.
C. Wireless Card Readers <WR> **UTA has a strong preference for wired card readers; however, wireless**

card readers are permitted when wired card readers are not pragmatic.
    a. Allegion AD-400 with 40:Privacy lock; and
        1) PIM400-485 Panel Interface Module (required)
D. Door Position Switches (By Division 08, unless noted otherwise)
    1. Concealed Magnetic Door Position Switch
        a. Sentrol 1076D
        b. Detection Systems, Inc
        c. Securitron DPS-W-BK series
        d. Owner Approved Equivalent.
    2. Surface Mount Door and Hatch Position Switch
        a. Sentrol 2500
        b. Owner Approved Equivalent.
    3. Overhead Door Position Switch
        a. Sentrol 2200 (floor)
        b. Sentrol 2300 (side)
        c. Owner Approved Equivalent.
E. Door Management Units <DMU>:
    1. Designed Security, Inc. (DSI) ES4200-K1-T1 (with keyswitch)
    2. Owner Approved Equivalent.
F. Local Audible Alarm
    1. Schlage Model 800A
    2. Owner Approved Equivalent.
G. Tamper Switches
    1. Sentrol 3010
    2. Owner Approved Equivalent.
H. Electric Locking Mechanism Power Supply
    1. Altronix
    2. Alarm-Saf
    3. LifeSafety Power
    4. Owner Approved Equivalent.
I. Electric Locking Mechanisms (By Division 08)
    1. Refer to Division 08 Hardware Specification
    2. Owner Approved Equivalent
J. Electric Power Transfer (By Division 08)
    1. Refer to Division 08 Hardware Specification
    2. Owner Approved Equivalent
K. Uninterruptible Power Supply <UPS>
    1. APC Smart-UPS
    2. Minute-Man II UPS
    3. Owner Approved Equivalent.
L. Wire & Cable (By Division 27)
    1. Refer to Specification 27 15 00.
    2. Owner Approved Equivalent.

PART 3 – EXECUTION

3.1 GENERAL REQUIREMENTS

A. Power Supplies. **All power supplies must be installed in HUB room where CBORD Squadron building controllers are located. UTA does not allow them above the door or in exposed (public) areas.**
    1. Power supply requirements
        a. A switch and on/off indicator within the power supply cabinet.
        b. Four hours of sealed gel battery backup to provide continuous operation during power failure.
            1) Provide batteries as required to provide specified battery backup time for a fully loaded power supply, regardless of the connected load.
        c. A battery charger to maintain the battery.
        d. Low battery and power fail contacts to monitor the status of the input power and the battery.
            1) Connect each power supply low battery and power fail alarm as a separate alarm input into

Access Control Panel.

e. Key lockable wall mount metal enclosure with tamper switch.

2. Additional Access Control Panel Power Supply Requirements
   a. The Access Control Panel power supply provides power only to Access Control Panels and shall not provide power for locks or any other low voltage device.
3. Additional Electric Locking Mechanism Power Supply Requirements
   a. Fail secure electric locking mechanisms shall remain locked during power failure and fire alarm conditions.
   b. Connect fail safe locking devices in accordance with applicable life safety codes to unlock automatically under the following conditions:
      1) Loss of power to the power supply
      2) Failure of the power supply
      3) Fire alarm activation
   c. Provide power distribution boards with independently fused output relays and fire alarm control panel interface.
4. Additional Device Power Supply Requirements
   a. Provide device power supplies for other security system devices requiring power (e.g. card readers, local alarms, motion sensors, etc.)
   b. Provide power distribution boards with independently fused outputs.

B. Video Surveillance System Integration
1. Automatic Video Call-up
   a. All alarms shall call up all cameras in the area of alarm to the screen of the ACID alarm operator workstation to allow for operator assessment of the alarm.
2. Pre and Post Alarm Video
   a. The operator shall be able to view up to 10 seconds of video before the alarm and 30 seconds after the alarm for all cameras associated with the alarm.
   b. This feature is to be integrated with the operator alarm notification to assist in alarm assessment.
   c. This feature shall be displayed as an option on the alarm notification screen and will not require operator to make a manual video search.
3. Recording
   a. All cameras whose field of view that include images of the area affected by the alarm, shall be recorded when an alarm is detected for use in forensic analysis, including the pre and post alarm video.
4. Duress and Emergency Intercommunications Integration
   a. Calls from emergency intercoms/phones with cameras shall provide the above video call-up and the pre and post alarm video capabilities.

C. Tamper Resistant Screws
1. Provide appropriate screw heads for each application (e.g. countersunk heads for recessed cover plate screws, flat head screws for standard junction box covers, etc.).
2. The security integrator shall provide Torx® tamper resistant screws for:
   a. Junction boxes located above doors
   b. Junction boxes located below ceiling height and/or within reach of hatch ladders
   c. Security device cover plates
   d. Surface mounted door position switches and armored cable

3.2 ACCESS CONTROL SYSTEM CONFIGURATION

A. Request to Exit <REX>
1. All doors equipped with electrified locksets or electrified exit hardware shall have integrated REX switches.
2. REX motion sensors can only be installed with prior approval from UT Arlington Campus Card Operations, EH&S Fire Safety Director, and as required by door manufacturer.

B. Door Management Unit <DMU>: (*If required in design drawings*)
1. Connect one DPDT door position switch output to the DMU door status input.
2. Connect the DMU voltage sense input in parallel with lock voltage after Access Control Panel lock control relay output.
   a. The DMU shall shunt and allow access when lock is electrically activated to unlock.
3. Wire the integral REX switch output to the REX input of the DMU.

4. Connect DMU reset/bypass input to Access Control Panel control point relay output to provide remote momentary reset and/or maintained bypass.
5. Connect DMU alarm output to Access Control Panel alarm input for alarm monitoring.
6. Immediate local alarm activation if the door opens without a valid access input.
7. DMU activation if the door is held open longer than an adjustable time after a valid access.
   a. Coordinate exact times for each door with ITS Security Operations.
8. DMU shall reset automatically after the door returns to a closed position.

C. Door Position Switches <DP>:
1. Double pole double throw (DPDT) magnetic DP switches shall be mounted in door frame when possible.
2. A DP switch shall be provided for each door leaf of all electronic access controlled doors regardless of number of door leaves.
3. Surface mounted door and hatch position switches shall be mounted on secure side of opening.
4. Provide armored cable/cord from surface mount and overhead switches to the associated junction box to conceal and secure the wire.

3.3 FURTHER REQUIREMENTS

A. Refer to provisions of Section 28 00 00.
B. Furnish and coordinate installation of all special device back boxes and ACID field devices as shown on the security drawings and as specified in this section.
C. The exact installation locations of all equipment shall be coordinated and verified with the Contractor prior to installation.
1. Subcontractor shall notify the General Contractor if any location appears to be unsuitable.
D. Provide low voltage power supplies for electric locking devices and ACID devices and components as shown on the security drawings and specified in this Section.
E. Coordinate with the Telecommunications Subcontractor for data network connections, IP address requirements, and telephone circuits as required.
F. Prepare all systems for user operation.
1. The security system must be complete and ready to operate prior to Owner final acceptance of the system.
G. Coordinate with the Owner for all system programming requirements.
H. Perform database programming as required to support the card reader, alarm point, surveillance system integration, and control panel configuration as required.

END OF SECTION