**THE UNIVERSITY OF TEXAS AT AUSTIN**
**ELECTRONIC SECURITY SYSTEM DESIGN, CONSTRUCTION AND COMMISSIONING GUIDE**

# PART 1 - GENERAL

## 1.1 NOTICE OF CONFIDENTIALITY

A. Security system work is critical to the security of The University of Texas at Austin. Plans, specifications and other documentary material and information about the security system are confidential information and shall remain secure and confidential. Confidential information shall not be deliberately or inadvertently disclosed to anyone other than the Contractor's personnel and subcontractors who require disclosure to perform their portion of the work. Track confidential information and ensure that copies are accounted for and properly destroyed when no longer needed to perform the work.

## 1.2 PURPOSE

A. Establish design criteria, define activities, identify stakeholders and assign responsibilities as they relate to the installation of electronic access control, and intrusion detection systems for the UT Austin campuses. These guidelines are intended for Project Management and Construction Services (PMCS) projects, Office of Facilities Planning and Construction (OFPC) projects, and the UT Security Installation & Repair shop.

## 1.3 OVERVIEW

A. The electronic safety and security systems for UT Austin’s buildings and facilities are managed and maintained by the Information Technology Services (ITS) Security Operations department. The primary function of these security systems is to protect the campus population and assets. The University of Texas Police Department (UTPD) will monitor and respond to all approved security alarms that are a part of this campus security system. The hardware and installation requirements listed in this guide must be in full compliance in order to obtain infrastructure maintenance support by ITS and alarm monitoring by UTPD.

B. Prior to commencing work in an existing building contact ITS Security Operations (512-471-6878) and UTPD (512-471-4441) to notify them of location, activities, and start/finish times of necessary work.

## 1.4 ELECTRONIC SECURITY SUPPORTED AT UT AUSTIN

A. Card Access Control. This system replaces the typical mechanical key controlled door lock with a door locking system that uses an access card as the access credential. This provides added features including:

1. Student/staff ID issued by the University's ID Center functions as the access card.
2. Tailored access privileges for each user.
3. Card user access privileges can be deleted or modified without retrieving the issued access card.
4. Automatic card deactivation when a student, visitor or employee role becomes inactive.
5. Individual University Departments control their facility access controlled doors via a web interface.
6. Cancellation of all access privileges in case of lost or stolen access card.
7. Monitor and document building access activities.
8. Locking or unlocking doors performed by automatic schedule or manually via software.

9. One access card can function at other compatible UT Austin facilities.

Each system includes: an electric door-locking mechanisms, card reader located adjacent the door, door status sensor, door prop alarm and a request to exit device. Typical system configuration is card or schedule controlled entry with free exiting. To access the controlled area, users must present their cards to the card reader located near the door. The door will unlock momentarily and relock. If the door is held open or propped, a local warning buzzer will sound to remind the user to close the door before an alarm message is transmitted to the UTPD. Card access can also be used to control elevator functions.

B. Emergency Delay Exit Door. The emergency delay exit door system operates as a fire code compliant (NFPA 101) emergency exit door but will not open until a 15 second delay period has expired after an exit attempt has been initiated. Local siren sounds immediately to alert local staff of attempt to exit and police receive message with location and specific alarm information. A local fire alarm triggers the immediate release of the door(s). Local controls or programmable time schedules can be used to override this security function. Typical installations include back or side code required exits to labs, exterior building emergency exit doors and stairwell doors. These systems may also be used with card readers in interior egress applications; however, these interior applications should be provided on a limited basis only to secure areas accessed through egress doors.

C. Intrusion Detection System. This system monitors offices, classrooms, etc. for unauthorized entrance or intruder. This system can consist of motion sensors, door status sensors, glass break sensors and one or more control keypads. The keypad is used to arm/disarm system by entering a numeric code on the keypad. Alarm signals are transmitted to UTPD with location and specific alarm information.

D. Article Protection System. This system is designed to monitor various computer equipment, projectors, lab equipment etc. for unauthorized removal. A small cable attaches to the monitored equipment. Removing or cutting the cable will generate a message to the UTPD with location and specific alarm information. System is armed by entering a numeric code on a local control keypad to allow for authorized equipment removal for repair or reconfiguration.

E. Duress Button. These buttons, also known as panic buttons, are installed in locations where potential personal safety or security threats exist. Depressing the button sends a silent priority alarm signal to UTPD with location and specific alarm information. The panic button is usually located in the knee space underneath a desk or service counter. Once activated the alarm must be manually reset by UTPD.

F. Police Help Call Station. The typical system is a distinct yellow box or pole with a red call button, “Police Help” signage and a blue locator lamp. Depressing the call button puts the individual in direct voice contact with a police dispatcher along with specific location information. These can be interior or exterior installations. Typical installations are parking lots or remote areas where personal safety is a concern.

## 1.5 REFERENCES

A. Americans with Disabilities Act (ADA)

B. Crime Prevention Through Environmental Design (CPTED)

C. NFPA 70: National Electric Code (NEC)

D. NFPA 101: Life Safety Code

E. NFPA 730: Guide for Premises Security

F. NFPA 731: Standard for the Installation of Electronic Premises Security

G. BICSI's Electronic Safety and Security Design Reference Manual (ESSDRM)

H. Underwriter's Laboratories (UL) Applicable Standards

I. NECA 1: Standard Practice of Good Workmanship in Electrical Contracting

J. Electronic Industries Alliance (EIA) Applicable Standards

K. Telecommunications Industry Association (TIA) Applicable Standards

L. Institute of Electrical and Electronics Engineers (IEEE) Applicable Standards

M. OFPC Security Planning and Design Guidelines

N. The University of Texas at Austin Security System Alarm Policy

O. The University of Texas at Austin Minimum Building Security Standard

P. The University of Texas at Austin Security Standard Installation Practices

Q. The University of Texas at Austin Video and CCTV Security Systems Policy

R. Family Educational Rights and Privacy Act (FERPA)

S. Texas Accessibility Standards (TAS)

1.6 EXISTING SECURITY SYSTEM DESCRIPTION

A. Software – UTC Picture Perfect

B. Access Control - UTC Micro/5

C. Intrusion Detection – UTC NetworX Series NX-8E

1.7 QUALITY ASSURANCE

A. Contractor Qualifications

1. Only approved security contractors may perform work on UT Austin campuses. Refer to [Appendix A] for the list of approved security contractors and instructions for becoming approved.

2. A single security systems integration contractor shall provide the work specified in this guide and have a minimum of five years experience in the fabrication, assembly and installation of systems of similar complexity as specified herein.

3. The security contractor shall work directly for the GC and not as a subcontractor under another trade.

4. The security contractor shall provide an installation that falls under the manufacturer's guidelines for warranty and is certified to work on Micro/5 and NetworX Series data gathering panels running on Picture Perfect software. These companies are referred to as "UTC Picture Perfect Certified Channel Partners".

5. The security contractor shall maintain a service facility and organization with staffing capable of providing comprehensive maintenance and service for the specified systems within a 100 mile radius of The University of Texas at Austin campus.

6. The security contractor shall have local in-house engineering and project management capabilities consistent with the requirements of the project. Provide a team managed by a project manager and field supervisor responsible for submittals, installation, scheduling, manpower, testing, record documents, etc. The field supervisor shall be on-site during all work activities to ensure quality, compliance with contract documents and coordination with other trades.

7. The contractor shall maintain a spare parts inventory necessary to resolve component failures of the system. Spare part inventory shall include the following:

    a. DGP boards

    b. Card readers

    c. Power supplies

    d. Door position switches

    e. Door management units

    f. Local door alarms

    g. Motion sensors

    h. Glass break sensors

    i. Telephone call stations

B. Documentation to include with Bid Proposal

1. Proof of security contractor licenses from the Texas Department of Public Safety's Private Security Bureau for both the firm and employees working on-site.

2. Proof of on-site personnel manufacturer certifications, training and licenses as required to purchase, install, modify, and service the specified systems.

3. Provide a list of three projects within the last five years that utilize the specified systems. For each project, provide a name, location, description, date of completion, contact name and contact phone number.

4. Maintain factory trained and certified technicians. Certified technicians shall install and terminate security riser closet equipment including DGPs, terminal cabinets, and power supplies and shall supervise installation, commissioning, and maintenance of the work. All installing personnel shall be licensed as required by local and/or state jurisdictions. The contractor shall maintain certification information for each technician at all times and shall provide certifications to the general contractor, security consultant and ITS for verification and record.

5. If the contractor has been involved with any litigation or criminal action with a client or government agency within the past five years, provide full details and status of each occurrence.

6. Specification Compliance

    a. Provide a specification compliance statement indicating compliance or deviation for each item in the specification. The statement shall be comprised of a list of all numbered paragraphs that appear in this Specification.

b. Indicate compliance of the proposed equipment and/or services by the word “Comply” following each paragraph number.

c. Indicate an exception to the requirement by the word “Exception” following the applicable paragraph number.

d. Should the proposed equipment and/or services not entirely comply with the requirements specified, but ultimately achieve the intent, the Bidder shall indicate the clarification to the requirement with the word “Clarification” followed by a full explanation of the extent of compliance for the applicable equipment and/or services proposed.

e. Instances where there is no indication of compliance or exception shall be considered non-compliant.

f. This compliance statement is critical for proposal evaluation. Failure to submit may result in the disqualification of the proposal.

1.8 SUBMITTALS

A. Produce submittal drawings using the latest version of AutoCAD. Printed drawings shall be at least half size drawing that are suitable to show in readable detail all elements of the project, including any text or symbols.

B. Provide submittals within 30 days of contract award.

C. Prior to installation the submittals must be reviewed and approved by the security consultant and ITS.

D. Submittals shall include:

1. Equipment schedules necessary to identify products that will be provided for the project. Schedules shall include description, manufacturer, model, and quantity for each product.

2. Manufacturers’ product data sheets for all components of the security system provided by the project. These product data sheets should provide descriptive literature, illustrations, installation instructions, information on compliance with applicable standards, dimensions, model number, electrical characteristics, support requirements, connection requirements and all applicable information to verify compliance with specifications. Where more than one part number is listed on a manufacturer’s data sheet, highlight the applicable information.

3. Floor plans necessary to identify specific device locations, cable routes and quantities, cable types, riser locations, and references to installation details and diagrams.

4. Floor plans should also indicate electronic door hardware type and voltage for each door when these devices are controlled by the security system. This can be accomplished with symbols or keyed notes.

5. Device termination details necessary to ensure consistent installation by all personnel and subcontractors.

6. Data gathering panel (DGP) termination details and schedules necessary to ensure that installation personnel and subcontractors properly connect devices to the DGP, power supplies, transition equipment, and other head end equipment.

7. Complete installation drawings including system block and functional diagrams of all systems and subsystems. Terminal point to point wiring diagrams for each type of device including correct terminal or connector pin designations.

8. Power supply points listing with devices and maximum loads to prevent overloading.

9. Riser diagram showing routes between floors or other areas that are not easily identified on the floor plans.

10. Detailed elevation drawings showing DGP and associated panel layouts.

11. Completed programming forms provided by ITS Security Operations. These completed forms are necessary for ITS Security Operations to program the security system.

E. At the conclusion of approved Pre-functional Testing the contractor shall provide preliminary as-built drawings which will be an updated and fully reviewed version of the submittal (O&M's not required at this time). Preliminary as builts must incorporate all changes to the project including security system design modifications, architectural changes and updated room numbering. This must be submitted to ITS Security Operations at least 15 days prior to Functional Testing.

F. At the conclusion of the project the contractor shall provide as-built drawings which will be an updated and fully reviewed version of the submittals. As builts must incorporate all changes to the project including security system design modifications, architectural changes and updated room numbering and be submitted to ITS Security Operations.

1.9 OPERATION AND MAINTENANCE MANUAL

A. Submit two hard copies and one electronic copy of the security O&M Manual to ITS Security Operations at the conclusion of the project. The security O&M Manual must conform to the following:

1. Ring binder with project title and contractor's name on cover and spine.

2. Name, address, and phone number of nearest representative of each project contractor and sub-contractor.

3. Table of contents

4. Tabbed sections including:

a. Theory of operation, design philosophy, specific functions

b. System block diagram

c. List of system associated mechanical locking keys with key codes and tamper resistant hardware types.

d. Equipment list, including a brief description, model, and the total number of each item used in the project.

e. Rack and wall elevation layouts

f. Manufacturers' data sheet and O&M manual for associated equipment.

g. Maintenance requirements for equipment, inspections and preventative maintenance schedules.

h. Loose leaf pocket containing: as-built drawings for each floor. Each drawing shall show: cable type and identifier, actual cable routing pathway, device number and device input/output number.

1.10 CONSTRUCTION SCHEDULE

A. The completion of the security system is heavily dependent on work by other trades. To ensure coordination with these other trades the security contractor will be responsible for providing a detailed construction schedule. See the example schedule and Gantt chart located at the following link to gain an understanding of the level of detail required. [http://www.utexas.edu/cio/policies/campus-security/files/UT%20Construction%20Schedule%20P6.pdf]

B. The schedule shall include all relevant security activities, estimated completion dates, duration of each activities and predecessor activities by other trades that impact security activities. For a list of critical activities that are dependent on other trades see [Appendix B].

C. 30 days after award of contract the security contractor shall provide a preliminary schedule for all security work with the level of detail shown in the sample schedule referred to in paragraph A above. Schedule shall conform to requirements listed in paragraph B above. Throughout the installation the security contractor shall provide updates at least once every two weeks. This schedule will allow the GC and owner to verify progress and identify any issues early on that will impact the overall construction schedule.

1.11 WARRANTY

A. The contractor shall warranty the completed work to be free of defects in workmanship and materials for a period of one year from the date of system acceptance by ITS and UTPD.

B. If the workmanship or materials is found to be defective or not in accordance with the contract documents during the warranty period, the contractor shall correct it promptly with factory certified technicians at no cost to the owner. All labor and materials shall be provided by the contractor

C. The contractor shall provide the owner and ITS Security Operations with a 7 days per week 24 hours per day phone number that will respond to warranty service calls. A technician is required to be on-site within 8 hours of placing the warranty service call and the repair shall be completed within 24 hours of site arrival.

D. The contractor shall provide loaner equipment for any device that cannot be repaired in the field. Loaner equipment must be functionally and technically equivalent to the replaced item.

E. Immediately following a warranty service request, the contractor shall provide written notice to ITS Security Operations (seccontrol@its.utexas.edu) to confirm that a factory certified technician is being dispatched to the site with a schedule for repair. Include the technician's name and contact information.

F. After warranty service work is completed, the contractor shall provide written notice to ITS security operations (seccontrol@its.utexas.edu) to provide details on the service work completed, cause of trouble and any other outstanding issues with a timeline on correcting them.

G. ITS security operations reserves the right to expand or add to the system during the warranty period using firms other than the contractor for such expansion without affecting the contractor's responsibilities, provided that the expansion is done by a firm which is an authorized dealer or agent for the equipment or system being expanded. Contractor shall not be responsible for maintenance of equipment installed by other firms.

PART 2 - PRODUCTS

2.1 GENERAL

A. All products and materials must be new and approved in the pre-installation submittals.

B. Exterior devices shall be sealed and protected against weather conditions including heat, cold, moisture, dust, and sand.

## 2.2 BUILDING ACCESS CONTROL SYSTEM (BACS)

A. System Description

1. Provide UTC Micro/5 PXNplus panels, HID SE series card readers, and alarm input and output devices connected to the campus GE Picture Perfect security management system.

2. Provide power to locks and connect the locks to a DGP auxiliary relay to provide for card reader or BACS control of doors as programmed by ITS security operations.

3. Card Reader Controlled Doors

a. Card reader controlled doors shall include:

1) Card reader.

2) Double pole double throw (DPDT) magnetic door position switch for each door leaf.

3) 24 VDC electric locking mechanism with integral request to exit (REX) switch.

4) All card reader doors will be keyed to a UTPD key.

b. Typical Configuration

1) Wire normally closed REX switch output to the REX input of the associated 2SRP.

2) The Door shall automatically relock the lock after the door closes after a valid card read access.

4. Card Reader Controlled Doors with Automatic Door Operators

a. Configure doors with automatic door operators as follows:

1) Free Exit Side Push Plate

a) The push plate shall function at all times.

b) When pressed, the door operator push plate shall:

(1) Signal the interface controller to unlock the door and provide a normally closed REX signal to the DGP.

(2) Signal the door operator to open the door.

2) Card Reader Unlock Mode

a) The door shall be unlocked.

b) The card reader controlled side door operator push plate shall be enabled.

c) When pressed, the door operator push plate shall signal the door operator to open the door.

3) Card Reader Locked Mode

a) The door shall be locked.

b) The card reader controlled side door operator push plate shall be disabled.

c) Upon a valid card read, the DGP shall provide a signal to the interface controller to:

(1) Unlock the door.

(2) Enable the card reader controlled side door operator push plate.

5. Access Controlled Doors without a Card Reader

a. Emergency exit only doors

1) Emergency exit only doors shall include:

a) Double pole double throw (DPDT) magnetic door position switch for each door leaf.

b) Door Management Unit (DMU)

c) Sign stating “DOOR IS ALARMED CONTACT UTPD PRIOR TO OPENING”

d) Access control doors without a card reader will not have exterior trim. If a key is required, it must be a UTPD key only.

2) Anytime this door is opened the DMU will sound immediately and an alarm will be sent to UTPD.

b. Exit doors with request to exit switches

1) Exit doors with request to exit switches shall include:

a) Double pole double throw (DPDT) magnetic door position switch for each door leaf.

b) Door Management Unit (DMU)

c) Request to exit switch integral to door hardware

2) Anytime this door is opened without a request to exit signal, the DMU will sound immediately and an alarm will be sent to UTPD.

3) DMU activation if the door is held open longer than an adjustable time after a valid access. Coordinate exact times for each door with ITS Security Operations.

6. Card Reader Controlled Elevators

a. Provide card reader in elevator car panel and associated digital output relay control of elevator floor select buttons. Individual digital output relays are needed for each floor select button in each elevator equipped with a card reader. Provide cabling from access control panel to elevator demarc panel. Provide individual control for each floor select button for each elevator door.

b. When an elevator is in the card reader control mode, the floor select buttons shall be disabled. The passenger shall be required to hold their access card up to a card reader

mounted in the elevator return panel. Upon a valid card read, the BACS shall enable the floor select buttons the passenger is authorized to access. The passenger must then push the desired select button. Once the passenger has pushed the button, the elevator control system will illuminate the button and send the elevator to the selected floor and open the selected door.

c. When the elevator is in normal mode, floor select buttons shall be enabled.

d. If elevator DGP fails the elevator will enter secure mode.

e. Card readers shall be in override anytime the elevator is in fire service mode.

f. Elevator contractor to provide the following. Verify this information with UT Elevator Services and the elevator specifications:

1) Infrastructure for Card Reader in each elevator shall require six (6) 2-conductor 20 gauge stranded, low voltage cable with an overall braided shield and drain wire, and four (4) 18 gauge stranded wires. These items shall be run from the elevator controller to the elevator car top. Provide an excess loop of six (6) feet long on each end. The excess cable loop shall be neatly bundled and located in a 6" X 6" X 4" Deep "J " box on the elevator car top. Provide an 18" x 24" x 6" deep hinged lockable "J" Box in the Machine room as a Demarc for Card Reader wiring. Provide screw terminal strips for wiring connections. Clearly label both boxes "Elevator Card Reader Future Use".

2) Removable blank for Card Reader. The area where the future card reader will be installed in the Car Panel must be self-contained and isolated from the Elevator wiring within the car panel. The card reader must be installed using a cover panel to be removed and replaced from the finish side of the car panel using tamperproof screws. The height of this reader must be incompliance with all ADA and TAS requirements. Card reader shall be bypassed anytime the Elevator is in Fire Service Mode. See [Appendix C]

7. Card Reader Controlled Elevator Hall Call Buttons

a. Provide a card reader adjacent to the elevator hall call button. When the elevator is in card reader control mode, the hall call button shall be disabled. Upon a valid card read, the BACS shall enable the hall call button and the user shall be able to select the button for access.

b. When the elevator is in normal mode, hall call buttons shall be enabled.

c. Card readers shall be in override mode anytime the elevator is in fire service mode.

8. Special Function Card Reader

a. Connect special function card readers to DGP card reader inputs.

b. ITS Security Operations will program special function readers to provide functions as required.

B. Equipment Requirements

1. Access Control Panel

a. Provide UTC Micro/5 control panels with (NO EXCEPTIONS):

1) PXNplus CPU board with latest firmware level as approved by ITS Security Operations.

2) Primary communications with the BACS server via RJ45 Ethernet connector.

3) Daughter board plug-in dial-up modem for secondary communications with the BACS server via RJ11 connector on controllers with exterior doors.

4) 2SRP card reader interface boards.

5) 5 volt communication chips for the card reader interface boards.

6) 16 DOR relay output boards. Must be placed in slot 4 in the micro unless otherwise approved.

7) 20 DI input boards (minimum one 20 DI board per Micro). Must be placed in slot 5 in the micro unless otherwise approved.

8) Minimum of one spare card slot for future microcontroller expansion.

9) Minimum of 20 percent spare alarm input and output points.

10) A separate manufacturer-approved power supply for each DGP.

11) UTC M5 enclosure.

12) Micro enclosure tamper switch wired as a discrete input to the power/com board.

13) Micro AC fail wired as discrete input to the power/com board.

14) Inputs and outputs associated with the same device must reside on the same controller.

15) The following supervised alarm inputs will be monitored as discrete alarm inputs on the 20 DI board (XX = micro account number) in this order: Micro XX PS Battery Fail, Micro XX PS Tamper, Micro XX Lock PS AC Fail, Micro XX Lock PS Low Battery, Micro XX Lock PS Tamper, Micro XX Termination Tamper.

2. Termination Cabinet

a. Provide Base Electronics LVPC-201677 (NO EXCEPTIONS) terminal cabinets with 201678 (NO EXCEPTIONS) terminal blocks to terminate system cables as follows:

1) Provide one cabinet for each BACS control panel.

2) Fully equip the cabinet with six terminal blocks regardless of the number of cables terminated within the cabinet. Blocks must installed in the same order as the micro.

3) Terminate BACS field device cables (e.g. card readers, door position switches, other alarm input devices, motion sensors, duress buttons, etc.) to the left side of the terminal blocks.

4) Provide individual patch cables from the terminal cabinet to the DGP for all DGP inputs and outputs including spares. Large multi-conductor cables shall not be acceptable for patch cable connections. Patch cable overall conductor counts, conductor sizes, and insulator colors shall match incoming cables.

5) Terminate each DGP input/output, including spares, to the terminal blocks. Terminate wires from the DGP to the right side of the terminal blocks.

6) The intent is to minimize access to the DGP cabinet for troubleshooting and field modifications and maintain a neat and serviceable DGP.

3. Proximity Card Readers

a. Card Reader Applications

1) Wall Mount and Special Function: HID SE SERIES (NO EXCEPTIONS).

2) Mullion Mount: HID SE SERIES (NO EXCEPTIONS).

3) Card Reader/Keypad: HID SE SERIES (NO EXCEPTIONS).

b. LED Configuration

1) Red LED for locked state

2) Green LED for unlocked state and valid card read

c. Associated Power Supplies

1) Wall-mounted and Mullion mount card readers shall be powered from the 2SRP at 5 VDC.

2) Card Reader/Keypad shall be powered from a fused auxiliary power supply at 12 VDC.

4. Request to exit (REX)

a. Doors equipped with electrified locksets or crash bars shall have integrated REX switches.

b. REX motion sensors can only be installed with prior approval from ITS Security Operations.

5. Door Position Switches

a. Concealed Magnetic Door Position Switch: Provide Sentrol 1076D Series or approved equal door position switches.

b. Surface Mount Door and Hatch Position Switch: Provide Sentrol 2500 Series or approved equal surface mount door position switches.

c. Overhead Door Position Switch: Provide Sentrol 2300 Series or approved equal surface mount door position switches.

d. Provide armored cable from surface mount and overhead switches to the associated junction box to conceal and secure the wire.

6. Door Management Unit

a. Provide Designed Security, Inc. (DSI) ES4200-K0 configured for 24VDC (NO EXCEPTIONS).

b. Typically used on door without a card reader.

c. Configure DMU as follows. See [Appendix D]:

1) Connect one DPDT door position switch output to the DMU door status input.

2) When a door is equipped with an electrified lock connect the DMU voltage sense input in parallel with lock voltage after the DGP lock control relay output. 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) When a door is not equipped with an electrified lock connect the DMU reset/bypass input to DGP control point relay output to provide remote momentary reset and/or maintained bypass.

5) Connect DMU alarm output to DGP 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. Coordinate exact times for each door with ITS Security Operations.

8) DMU shall reset automatically after the door returns to a closed position.

7. Delayed Exit Device Controller

a. Provide Securitron Model XDT-24 (NO EXCEPTIONS). Locate the controller above the secured side of the door. Provide additional cabinet as required to provide a neat and serviceable installation. See [Appendix E]:

b. Signage requirement for exit only delayed egress door. Signs should be mounted above the crash bar and have a red background with white letters that are 1” tall with a 1/8” stroke width (NFPA 101 requirement). ITS and UT Fire Prevention Services shall approve sign language upon request prior to installation.

8. Tamper Switches

a. Sentrol 3010 series or approved equal plunger type normally open tamper switches to monitor the secure status of all DGP’s, power supplies, terminal cabinets, power distribution units, and other Security System cabinets and enclosures. Tamper switches will be in the closed state when depressed.

b. Fasten tamper switches within the cabinet to provide no access to the switch and fasteners when the cabinet is closed.

c. Provide independent monitoring of tamper conditions for each cabinet. Include the number of tamper switches in the total alarm input figures.

9. End of line (EOL) Resistor Terminations

a. Field (Device) End

1) Provide GRI 6644T Standard Series Parallel Resistor Packs with 2 – 1K 1/8 watt 5% carbon film with 2 blue and 2 black 12-inch leads.

2) Locate EOL Resistor Terminators at the end of the cable being supervised and within device housings when possible.

b. Panel End

1) Provide GRI 6644TStandard Series Parallel Resistor Packs with 2 – 1K 1/8 watt 5% carbon film with 2 blue and 2 black 12-inch leads.

2) Locate Resistors at the end of the cable within the panel housing.

10. Tamper Resistant Screws

a. Provide Torx® fasteners with pins tamper resistant screws for the following applications:

1) Junction boxes located above doors.

2) Junction boxes located below ceiling height and/or within reach of hatch ladders.

3) Device cover plates.

4) Surface mounted door position switches and armored cable.

5) Duress buttons.

6) Card Readers

b. 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.).

11. Power Supplies

a. Provide Altronix / AL Series or approved equal UL Listed Class II power supplies for BACS equipment and electric locking devices.

b. Some electronic locking hardware require a 120VAC power supply at the door. In these instances the door hardware installation contractor shall be responsible for furnishing and installing the locking hardware manufacturer's recommended power supply. Verify with UTS Security Operations and security condultant to determine if a remote power supply is required.

c. Power supplies shall provide the following:

1) A switch and on/off indicator within the power supply cabinet.

2) Four hours of sealed gel battery backup to provide continuous operation during power failure. Provide batteries as required to provide specified battery backup time for a fully loaded power supply, regardless of the connected load.

3) Each battery shall be permanently labeled with the date of manufacturer and date of installation (month & year). The date of installation is the month & year that the battery was placed in the power supply and began charging.

4) A battery charger to maintain the battery.

5) Low battery and power fail contacts to monitor the status of the input power and the battery. Connect each power supply low battery and power fail alarm as a separate alarm input into DGP.

6) Key lockable wall mount metal enclosure with tamper switch. Coordinate keying requirements with ITS Security Operations.

d. Additional DGP Power Supply Requirements

1) The DGP power supply provide power only to DGP's and shall not provide power for locks or any other low voltage device.

e. Additional Electric Locking Mechanism Power Supply Requirements

1) 24 VDC output.

2) Provide (1) lock power supply per DGP.

3) Fail secure electric locking mechanisms shall remain locked during power failure and fire alarm conditions.

4) Connect fail safe locking devices in accordance with applicable life safety codes to unlock automatically under the following conditions:

a) Loss of power to the power supply.

b) Failure of the power supply.

c) Fire alarm activation if required by UT Austin Fire Prevention Services.

5) Provide power distribution boards with independently fused output relays and fire alarm control panel interface.

f. Additional Device Power Supply Requirements

1) Provide device power supplies for other security system devices requiring power (e.g. card readers, local alarms, motion sensors, etc.)

2) Provide power distribution boards with independently fused outputs.

C. System Interfaces

1. Electric Locking Mechanisms

a. The security consultant and door hardware consultant shall coordinate all door hardware, door and door frame design. The door hardware consultant shall be responsible for specifying all access control door hardware based on security consultant input and ensure consistency with project hardware. The security consultant shall verify all specified door hardware is appropriate for the security application. In addition, the security consultant must specify the sequence of operations for each access controlled opening and define termination requirements for the security contractor.

b. UT preferred electronic lock manufacturers:

1) Electrified Exit Device

a) Sargent (Assa Abloy)

b) Von Duprin (Ingersoll Rand)

c) Corbin-Russwin (Assa Abloy)

2) Mortise Locks

a) Sargent (Assa Abloy)

b) Corbin-Russwin (Assa Abloy)

c) Schlage (Ingersoll Rand)

3) Magnetic Locks

a) Locknetics (Ingersoll Rand)

b) Rutherford Controls (RCI)

4) Cylindrical Locks are prohibited

2. Elevator Control System

a. The security consultant must verify the elevator security requirements with ITS Security Operations and coordinate with the elevator consultant to ensure the appropriate system interfaces are in place.

3. Fire Alarm and Life Safety

a. The security consultant must coordinate the access control system design with the life safety consultant to insure compliance with applicable codes and requirements. This includes, but is not limited to, the fire alarm interface, fail safe/secure locking mechanisms, and delayed egress.

## 2.3 INTRUSION DETECTION SYSTEM

A. System Description

1. Provide UTC NetworX Series NX-8E panels and alarm devices for intrusion detection and article protection connected to the campus UTC Picture Perfect security management system.

2. Provide NX-148E keypads conveniently located near areas being protected so that maintenance personnel and UTPD can arm and disarm. Coordinate locations with UTPD and end user.

3. Coordinate interface and programming requirements with ITS Security Operations.

B. Equipment Requirements

1. Intrusion Detection Panel

a. Provide UTC NetworX Series NX-8E panel with (NO EXCEPTIONS):

1) NX-590E network module to provide primary communication to the servers via RJ45 network connection.

2) Secondary communication via dial-up modem is required is panel has panic buttons or is monitoring an exterior door.

3) Provide additional NX-148E keypad located next to each NX-8E panel to provide a maintenance and troubleshooting interface.

4) NX-590E, NX-216E, NX-507E, NX-148E and NX-320E modules as required. Use the NX-003C enclosure when NX-216E modules are required

5) A shielded 20/4 conductor wire shall be installed between all UTC NetworX panels located in the building.

6) Consult with ITS Security Operations regarding intrusion design and installation.

2. Article Protection

   a. Provide Cat5e network cable from the NX-8E control panel to the article location.

   b. Terminate the blue wire pair to a zone alarm input at the control panel.

   c. At the devices end terminate an RJ11 connector to the end of the Cat5e cable.

   d. Provide surface mount RJ11 “biscuit” block with a 3.3k resistor terminated across the red and green at each device interface location.

   e. Pass the cable through permanently affixed security plate/loops and connect to the termination block.

   f. Provide NX-148E keypads conveniently located near the articles being protected so that maintenance personnel can arm and disarm. Coordinate location with UTPD and end user.

   g. Terminate cable conductors to the termination block above the accessible ceiling. Provide 50 feet spare cable to allow ITS Security Operations to relocate termination as required to the final device location. Coil, bundle, and label the cable and terminal block.

   h. Neatly wrap unterminated wire pairs around the cable for potential future connection.

   i. Consult with ITS Security Operations regarding article protection design and installation in the building.

3. Motion Detector

   a. Provide dual technology (microwave and infrared) to prevent false alarms. Specific model depends on application and mounting requirements.

   b. One motion detector per zone, do not wire in series.

4. Glass break Detector

   a. Contractor will need to provide compatible glass break tester for device being installed.

   b. One glass break detector per zone, do not wire in series.

5. Duress Buttons

   a. USP model HUB-2B (NO EXCEPTIONS)

   b. These buttons, also known as panic buttons, are installed in locations where potential personal safety or security threats exist. Depressing the button sends a silent priority alarm signal to UTPD with location and specific alarm information. The panic button is usually located in the knee space underneath a desk or service counter.

   c. Duress button locations must be reviewed and approved by UTPD.

   d. One duress button per zone, do not wire in series.

e. 30 feet service loop in ceiling when mounting on non-fixed furniture.

f. Consult with ITS Security Operations regarding duress button design and installation in the building.

6. Police Help Buttons

a. System Description

1) These are the red mushroom buttons commonly seen in parking garages. Pressing the button will notify UTPD that assistance is needed and provides them with location information.

2) One police help button per zone, do not wire in series.

3) Signs should be mounted next to button and read: “POLICE HELP”. These should also include the associated zone number. Coordinate sign requirements with ITS Security Operations.

b. Equipment

1) Square D model 9001KR25R with 9001K93RM metal mushroom button.

## 2.4 POLICE HELP CALL STATIONS

A. System Description

1. The police help call station shall consist of security telephone call stations connected to analog telephone lines with blue locator lights and appropriate signage.

2. Provide one outside plant rated Cat5e cable from each telephone to the nearest telecom patch panel or 110 blocks.

3. Provide 120VAC power for associated lighting.

4. Terminate telecom cables following the existing telecom cabling labeling convention.

5. Coordinate extension numbers, telephone numbers, and other programming requirements with ITS.

B. Equipment

1. Stanchion Security Telephone Call Stations

a. Provide Talk-A-Phone ETP-MT Emergency Phone Tower with constantly lit blue light and ETP-400C telephone. Button on phone should say “To Call”.

b. Provide safety yellow tower (#02SF) with blue lettering (#A7822R) as coordinated with ITS.

c. Provide manufacturer recommended foundation.

2. Wall Mount Security Telephone Call Stations

a. Provide Talk-A-Phone ETP-401C telephone. Button on phone should say “To Call”.

b. Provide constantly lit blue light above wall mounted police help phone. Talk-A-Phone ETP-EL or equivalent.

## 2.5 WIRE AND CABLE

A. Description

1. Provide wire and cable infrastructure for all security system components.

B. Minimum Requirements

1. Conductors and cable shall be UL approved for its intended application and shall meet all national, state, and local code requirements for its application.

2. Conductors and cable shall meet individual security system manufacturer specifications.

3. Provide shielded conductors and cable as required by the manufacturer or as required to provide for interference-free signals.

4. Color coding shall be accomplished by using solidly colored insulation. Grounding conductors, where insulated, shall be colored solid green or identified with green color as required by NEC.

5. Increase conductor sizes on cables as required to be consistent with circuit current ratings, length of wire runs, and manufacturers' recommendations.

6. Composite cables are not an acceptable alternative.

7. Due to wire run distance, electronic locks may require a larger gauge wire or remote power supply to work properly. Contractor will be responsible for determining distance, power supply, and wire gauge requirement. Confirm requirements with ITS Security Operations.

8. Patch Cables

   a. Provide pre-manufactured patch cables (cable, connectors, boots, etc.) as required to connect security systems to voice and data communication outlets.

   b. Patch cables shall be certified for their specific use to meet or exceed applicable industry specifications (e.g. EIA/TIA, ETL, UL, CSA, etc.).

   c. Provide cable lengths as necessary to neatly route cables through cable management systems and other cable organization systems.

   d. Provide connectors as required for proper termination. Provide boots for connectors where applicable to prevent snagging.

   e. Provide Cat5e patch cables as required for the connections of security equipment. Confirm Cat5e cabling specifications and requirements with ITS.

   f. Provide cable jacket colors as follows:

      1) Blue for data cables.

      2) White for voice cables.

      3) White for security cables except for direct burial cables.

C. Minimum Conductor and Cable Types and Sizes.

1. Security contractor to verify maximum distances and size wire accordingly

2. Low Voltage Power Cable

    a. 18 AWG (4 conductors minimum per locking device), stranded, insulated, and jacketed.

3. Card Reader Cable

    a. 18 AWG (6 conductors minimum), stranded, shielded, insulated, and jacketed.

4. Keypad Cable

    a. 20 AWG (4 conductors minimum), stranded, insulated, and jacketed.

5. Alarm Point Monitoring Cable

    a. 20 AWG (4 conductors minimum per input or alarm point), stranded, insulated, shielded and jacketed.

6. Siren, Speaker, and Control Point Cable

    a. 18 AWG, (4 conductor minimum )stranded, insulated, and jacketed.

PART 3 - EXECUTION

3.1 COORDINATION

A. Security contractor shall be required to coordinate installation activities with the following divisions or groups:

1. Door hardware, doors and door frames by contractor.

2. Electrical power and pathways by contractor.

3. Telecom voice and data cabling and outlets by contractor.

4. Fire alarm interface by contractor.

5. Elevator demarc panel, traveling cables and elevator car card reader enclosure by contractor.

6. IP and phone number assignment by ITS.

7. Security system programming by ITS security operations.

B. Meetings

1. Coordination meetings shall include the following in addition to regular project meetings coordinated by the general contractor. Contractor shall store meeting minutes, meeting agenda, sign-in sheet and handouts in the Commissioning and Closeout Manual.

2. Project Kickoff Meeting

    a. The intent of this meeting is to:

        1) Introduce the ITS representative, security consultant and construction teams.

        2) Identify communication channels and process.

        3) Establish expectations.

4) Review the project scope and requirements.

5) Establish schedule for provision and review of submittals.

6) Answer questions and resolve any issues.

3. Pre-Installation Meeting

a. The intent of this meeting is to:

1) Review the construction schedule.

2) Coordinate requirements and schedules of other trades related to the security system.

3) Review issues and/or problems as necessary.

4. Meetings with Other Trades

a. The intent of these meetings are to coordinate requirements with other trades as required to:

1) Review the details for each interface.

2) Ensure that each trade understands requirements for the interface with the security system.

3) Verify interface responsibilities and close any necessary gaps in scope of work.

4) Resolve issues as required.

b. The initial coordination meeting shall involve all trades related to the security system. Additional meetings will be scheduled as necessary for additional coordination.

c. The general contractor will be responsible for scheduling coordination meetings.

## 3.2 INSTALLATION

A. General

1. Coordinate equipment installation requirements with other trades prior to installation.

2. After installation, protect equipment to prevent damage during the construction period. Close openings in conduits and boxes to prevent the entrance of foreign materials.

3. Make equipment connections in accordance with the approved submittal drawings and manufacturer specifications.

4. Seal exterior devices to protect against weather conditions including heat, cold, moisture, dust, and sand.

B. Equipment

1. Field-verify specific equipment locations to provide the best fit and function. Verify locations with the Architect as necessary.

2. Install equipment in accordance with manufacturer specifications.

3. Install equipment to allow adequate clearance for testing and maintenance.

4. Locate end of line resistors within the device housing.

5. Provide tamper resistant screws and fasteners for equipment located in accessible and/or public areas.

6. Remove dirt, packaging, wiring scraps, and other debris from equipment, boxes, cabinets and work areas at the end of each work day.

7. Wherever possible, remove contractor and manufacturer equipment logos from security field devices.

8. Final approved program sheet submitted to ITS will be placed in a clear plastic sleeve mounted on the inside door of the controller for future reference.

9. Accessibility Coordination

    a. When mounting card readers or other devices that require accessibility coordinate with the architect and other trades to ensure ADA requirements are being met.

    b. Doors with both a card reader and automatic door operator push plate should have both of these devices placed next to each other.

    c. On the pull side of a single door, place the card reader on the latch side of the opening. On the pull side of double doors, place the card reader on the right side which is generally the path of travel.

    d. Card readers should generally be mounted 48” from an inside corner and 42” above finished floor.

    e. On the pull side of a door, card readers should be mounted 48” from the door jamb so that a wheelchair would be clear of the swing of the door.

10. All power transfer hinges or other devices that provide a wiring path from the door to the frame must be serviceable without having to remove the door.

## 3.3 CONDUIT, BOXES AND RACEWAYS

A. Conduit must be a minimum of ¾ inch (flex is not allowed). Junction boxes must be a minimum of 8x8x4, pull boxes, wire troughs, and wire ways dedicated to security will be provided by electrical contractor. Provide additional conduit necessary to complete the installation, but not provided.

B. Provide conduit between power sources provided under a separate section and security system low voltage power supplies.

C. Provide conduit from interface terminal cabinets to security pull boxes.

D. Carefully install conduit, properly and adequately support conduit as required to comply with the requirements specified herein and as required by the NEC, and provide a neat, workmanlike installation. Support horizontal conduit runs with clamps, pipe straps, special brackets, or heavy iron ties secured to building structure.

E. Lay out and install conduit runs to avoid proximity to hot pipes. In no case shall a conduit be run within three inches of such pipes, except where crossings are unavoidable, and then the conduit shall be kept at least two inches from the covering of the pipe crossed.

F. Provide fire stops where conduits penetrate fire rated walls and/or floors.

G. Provide tamper resistant screws or fasteners for junction boxes located in accessible and/or public areas.

3.4 WIRING TECHNIQUES

A. Wire installation is not specifically detailed in the Contract Documents. Determine conductor requirements for each device in accordance with the Contract Documents and manufacturer requirements.

B. Install cable in accordance with Security System manufacturer requirements and NEC.

C. Color code and terminate conductors consistently as follows:

1. Red for positive and black for negative DC power leads.

2. White for positive and green for negative alarm loop conductors.

D. Run wiring within conduit or exposed within walls, neatly above accessible ceilings, and in riser closets.

E. Arrange cables within access panels to allow for removal of the access panel and access to equipment within the panel. Arrangement shall also be in a neat and workmanlike manner. ITS Security Operations shall hold the final, authoritative opinion on what constitutes a neat and workmanlike manner. Failure to meet Security Operations' expectations in this matter shall result in Security Contractor to redress cabling/installation to Security Operations' satisfaction, at no additional cost to the project.

F. Neatly route cables parallel or perpendicular to building lines.

G. Provide J hooks and other cable support systems (spaced at regular intervals) within accessible ceiling spaces. Fasten cables to the cable support systems and provide strain relief to protect cables and ensure compliance with required cable bends.

H. Keep cable not run in conduit a minimum of 18" from high voltage (120 VAC and above) circuits (e.g. light fixtures, wire run parallel with conduit, transformers, electric panels, etc.).

I. Run cables at least six inches from the communications cable plant, intercom wires, input/output wires, and siren wires.

J. Route wire and cable as required to prevent interference and signal contamination of both Security System cable and cable associated with other systems. Coordinate the routing of wire and cable requiring isolation from power, radio frequency (RF), telephone, etc.

K. Provide sleeves and code compliant fire proofing techniques for all penetrations of fire rated partitions, masonry walls, and slabs, where the penetrations are made by or used for installation of Security Systems.

L. Separate high voltage (120 VAC and above) cables from low voltage cables within enclosures to comply with NEC requirements.

M. Fasten approved wire management hardware (bridle rings, j-hooks, etc.) to the building structure and/or cable tray at least every 10 feet where not in conduit. Do not lay or fasten cables to electrical conduits, light fixtures, piping, mechanical equipment, or ceiling grids.

N. Run wire and cable continuous from device location to the final point of termination. No mid-run cable splices will be allowed except where cables must transition from one type to another (e.g. underground cable to plenum cable). Provide the following where cable transitions are required:

1. Provide labeled terminal strips inside lockable cabinets at cable transition locations and document locations in the submittals.

2. Label terminal cabinets and document labels in record documentation.

3. Provide the same number of conductors and insulator colors for each cable type from the security device to the DGP location.

4. Where shielded cable is required, the shield must also be spliced.

O. Visually inspect wire and cable for faulty insulation prior to installation.

P. Provide bushings, grommets, and strain relief material where necessary to prevent abrasion of wire and excess tension on wire and cable.

Q. Component Connections

1. All security component connections from device to wire/cable shall be soldered and individually heatshrinked from jackect to jacket. Exposed conductors are not acceptable.

2. All security panel connections from wire/cable to terminal blocks shall be soldered, tinned, and heatshrinked from jacket to jacket. Exposed conductors are not accepatable.

3. Wire nuts and crimp type connectors shall not be an acceptable means of connecting wire and cable.

R. Neatly install and terminate wire and cable within DGP's, power distribution cabinets and other security enclosures. Pull cables tight, remove slack, and route in such a way as to allow direct, unimpeded access to the equipment within the enclosure. All wires within DGP and all panels must be tinned and heat shrink used to insulate the wires.

S. Bundle and tie wire and cable with Velcro hook & loop type or similar cable ties.

T. Provide heat-shrink to insulate wire connections. The use of electrical tape shall not be acceptable.

U. Cover exposed high voltage (120 VAC and above) power terminations within DGP's, power distribution cabinets and other security enclosures.

V. When electric locking mechanisms or power transfer hinges come with factory terminated connectors, the contractor shall consult with ITS Security Operations prior to removal. Under no circumstances will the contractor be allowed to cut these connectors off without consulting ITS Security Operations.

## 3.5 POWER REQUIREMENTS

A. 120 VAC emergency power dedicated to security will be provided by the electrical contractor.

B. Connect to AC power and provide UL listed power supplies and transformers to distribute low voltage power to the system components as required.

## 3.6 GROUNDING

A. Ground all equipment and cables in accordance with manufacturer requirements and instructions.

B. Ground cable shields and drain wires as follows:

1. From the field devices, terminate shield drain wires to the terminal cabinet ground bar.

2. Bond the terminal cabinet and micro cabinet ground bars to the DGP ground bar with a minimum 12 AWG solid conductor green grounding wire.

3. Do not terminate shields and drain wires between the terminal cabinet and DGP.

3.7 LABELED FRAMES AND DOORS

A. In no instance shall any UL labeled door or frame be drilled, cut, penetrated, or modified in any way.

B. The Contractor shall be responsible for replacing any labeled door or frame that is modified without written approval from the Architect.

3.8 LABELING

A. All labels shall be based on final UT door and room numbering scheme. ITS Security Operations shall be consulted on labeling prior to installation.

B. All cables need to labeled alike at both ends.

C. Permanently mark all terminals. Terminal and cable markings shall agree with markings shown on as-built drawing.

D. Label the top of each card reader with the door number shown on final security system program sheet that has been approved by ITS security operations.

E. Neatly coil and secure spare conductors in the ceiling, device back box or panel wire way. Neatly bundle and tag conductors.

F. Label equipment including, but not be limited to DGPs (label to denote DGP address), power supplies, and termination cabinets. Coordinate names, fonts, styles, and devices to be labeled with ITS security operations prior to labeling. Provide computer-generated labels; handwritten labels shall not be accepted.

G. Identify power circuits and breaker locations within each power supply cabinet. This shall include any remote power supplies.

H. Label Materials

1. Conductor and Cable Labeling

a. Provide T&B Shrink-Kon Type HVM or equal labels.

b. Labels shall be computer generated and fastened to conductors/cables with transparent heat shrink material. Hand-written labels shall not be accepted.

2. Equipment Labeling

a. Engraved plastic with contrasting letter colors.

b. Half-inch minimum size lettering

c. Fasten labels with permanent adhesive.

I. Label wires and cables as follows:

1. Mark all wire and cable in common at both ends.

2. Install markers to be readable from left to right or top to bottom. Locate labels near termination points.

3. Install labels when wire and cables are installed.

4. Labeling shall agree with record documentation.

J. Control Panels, Power Supplies and Termination Cabinets

1. All Micro/5 and NX-8E control panels will be assigned a unique account number by ITS security operations after the contractor submittals have been reviewed. Labels on each Micro/5 and NX-8E control panel shall read: “ACCT: XXXX”. XXXX represents a 4 digit account number.

2. Each termination cabinet associated with a Micro/5 shall have a label that reads: “MICRO XXXX TERMINATION”. XXXX represents a 4 digit account number.

3. Each power supply associated with a Micro/5 or NX-8E shall have a label that reads: “MICRO XXXX YYYY PS”. XXXX represents a 4 digit account number and YYYY represents the type of equipment being powered. For example “MICRO 1234 LOCK PS” represents the lock power supply for Micro #1234.

K. Micro/5 Cables
Accounts: 0001-2000
Micro account – 4 digits
Board – 1 digit
Address – 2 digits
Device – 2 characters
Input (DI) or output (DO) – 2 characters
Examples:
[account#]_[board#]_[address#]_[input or output type]
[device type] [room or door number]

0172_2_00_DI
CR 1.108

L. NX-8E Cables
Accounts: 3001-9999
Account – 4 digits
Zone – 3 digits
Device – 2 characters
Examples:
[account#]_[zone#]_[input or output type]
[device type] [room or door number]

6666_002_DI
MD 2.103

## 3.9 PROGRESS OBSERVATIONS

A. Security consultant and/or ITS will conduct progress observations during construction to verify construction progress and verify the construction schedule. Coordinate progress observation site visits with the Contractor. Provide Contractor with copies of progress observation reports and other applicable documentation for inclusion in the Commissioning and Closeout Manual.

B. Security consultant and/or ITS will conduct the following minimum progress observations:

1. Security Conduit Rough-in and Preliminary Wire and Cable Installation

   a. The intent of this observation is to verify that adequate and proper conduit rough-in is installed, verify that wire and cable are being properly installed and labeled, and identify and resolve issues regarding conduit and wire and cable installation.

2. Preliminary Wire Termination Progress

   a. The intent of this observation is to verify that the contractor will install and terminate equipment in accordance with specifications and ITS standards.

   b. Observations will occur upon initial installation of each type of equipment (e.g. Panels, Card readers, alarm devices, junction boxes, etc.).

   c. Observations must be complete prior to proceeding with the installation of remaining similar or like equipment.

   C. Security contractor shall coordinate appropriate timing of each observation with the general contractor, security consultant and/or ITS as required to meet intended goals.

   D. The inspectors will issue reports for each observation to summarize findings and document clarifications noted during the observation.

## 3.10 COMMISSIONING

A. Commissioning of the security system shall comply with the requirements in section 01 91 00.

B. The following activities must take place to complete the installation of the security system. Documentation of activities, corrective action items and status, and activity completion verification shall be provided to the Contractor for inclusion in the Commissioning and Closeout Manual.

1. Pre-functional Tests (PFT)

   a. Utilize PFT checklists created by ITS.

   b. Test and document security device connections with a multi-meter to verify proper termination and operation.

2. Operational Field Testing with ITS

   a. Submit updated security system program sheets and completed PFT checklist to ITS.

   b. Operational Field Testing can be scheduled once the communications cabling contractor has completed the portion of the voice and data network which supports the new security system.

   c. The completed PFT form will initiate the IP address and phone number assignments for each security control panel.

d. ITS will review updated system programming forms and make changes as needed.

e. Conduct a complete security system test of each alarm point and signal and document results on checklist. While conducting this test, the contractor shall be in direct communication with security operations as they observe the signals on their screen. The intent of this test is to verify proper system operation and ensure accuracy of system programming prior to functional testing.

3. Functional Tests (FT)

a. Utilize FT checklists created by ITS.

b. Contractor shall provide two sets of preliminary as-built drawings to ITS and the security consultant at least 15 days before the FT process is scheduled to start.

c. Once PFT and operational field testing procedures have been documented and completed, the final FT walkthrough can begin. The contractor shall demonstrate to ITS and the security consultant during a full walkthrough inspection that the completed and integrated system complies with the contract documents, initial training is complete, and the system is fully operational.

4. Integrated System Test (IST)

a. Consult ITS Security Operations on IST

b. Test critical system interfaces such as fire alarm and elevators.

C. Substantial completion requirements:

1. All alarm points and devices shall be fully installed and operational.

2. Any punch list items as a result of the FT or IST will not interfere with the operation of the security system.

END

APPENDIX A

To perform work on campus a security contractor must meet the qualifications outlined section 1.6, “QUALITY ASSURANCE, Contractor Qualifications” of this document.

Companies desiring to be considered for performing security work at UT Austin should submit their qualifications meeting the requirements described in section 1.6, “QUALITY ASSURANCE, Contractor Qualifications” of this document. Please be advised that the review process takes 60 days from receipt of acceptable package to date of approval. This timeline will not be modified to accommodate circumstances.

Submit complete packages to:

The University of Texas at Austin
ITS - Campus Security Operations C3800
PO Box 7580
Austin, Texas 78713-7580

Below is a list of companies that have demonstrated that they meet these requirements.

| Company | Address | City | State |
|---|---|---|---|
| Diebold Security | 9701 Dessau Rd., Bldg 1, Ste 104 | Austin | TX |
| Entech Sales & Service | 10139 Metropolitan Dr | Austin | TX |
| Nathan Alterman Elec. | 14703 Jones Maltsberg | San Antonio | TX |

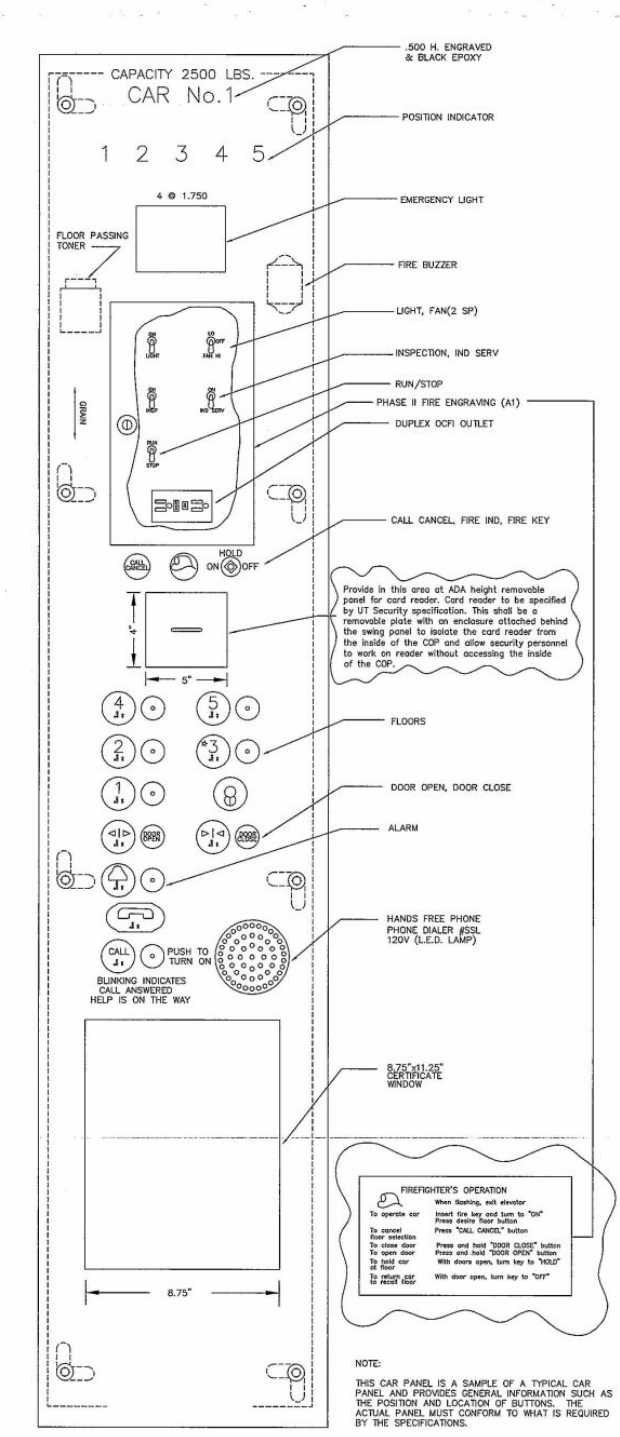
APPENDIX B

CRITICAL SECURITY MILESTONES BY CALENDAR DAYS PRIOR TO SUBSTANTIAL COMPLETION

| **Column A** | | | **Column E** |
|---|---|---|---|
| DURATION IN DAYS | **CRITICAL MILESTONES** | **PREREQUISITE START CONDITIONS** | DAYS before SUBSTANTIAL |
| | Wire and cable installation. | 1. Pathway, conduit and cable tray installation is complete. | 98 |
| | Access control, intrusion detection & CCTV system head end equipment installation. | 1. Equipment rooms are complete.<br>2. Plywood is on the wall for wall mounted enclosures.<br>3. Equipment rack is installed for DVR.<br>4. Power is available.<br>5. Ground bar is installed. | 70 |
| | Field device wiring & termination for access control. | 1. Door, frame and hardware are installed and functional. | 70 |
| | Wall mounted devices installation. | 1. Paint and finish work on walls is complete. | 63 |
| | Equipment Start Up | 1. MDF completed and ITS has installed OSP feeder cables.<br>2. Voice and data horizontal cabling must be installed, tested and labeled.<br>3. Riser cables for connecting network switches to the gateway must be installed, tested and labeled.<br>4. Network rooms that need switches for security must be complete with grounding, HVAC and locks on the door. ITS Networking will then install switch.<br>5. Pre-functional test requirements complete and approved by ITS.<br>6. Operational field testing completed with ITS. | 56 |
| | Functional Test | 1. Equipment start up requirements are complete including testing with ITS security operations. | 21 |
| | Integrated System Test | 1. Fire alarm system is complete and fire alarm relay interface to the lock power supplies is installed.<br>2. Elevator controls are functional and fully operational. | 7 |

INSTRUCTIONS:
Column A: Enter calendar days required to complete this activity
Column E: Enter calendar days prior to SC this prerequisite activity must be completed

APPENDIX C

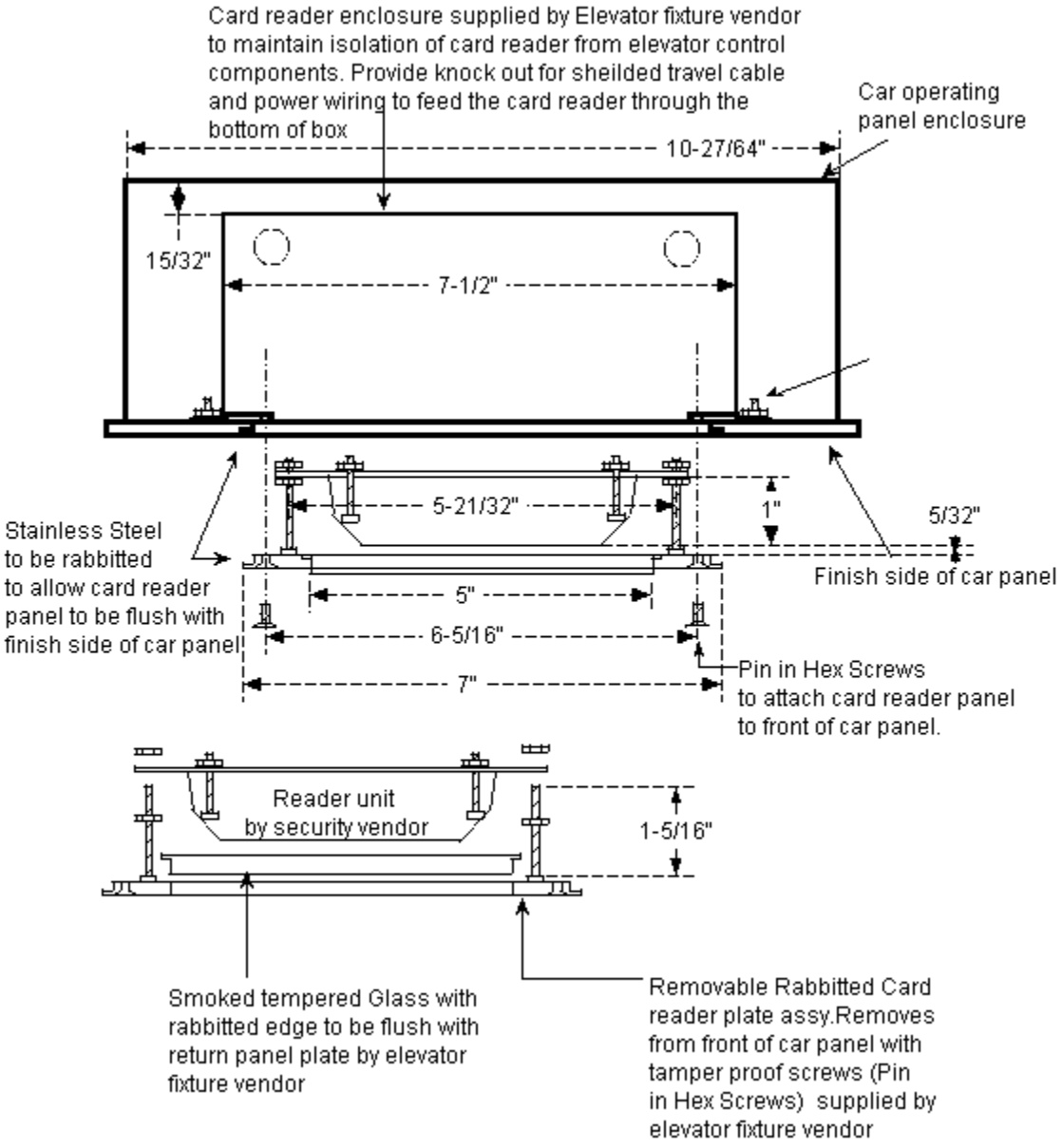



DETAIL: CAR PANEL

6

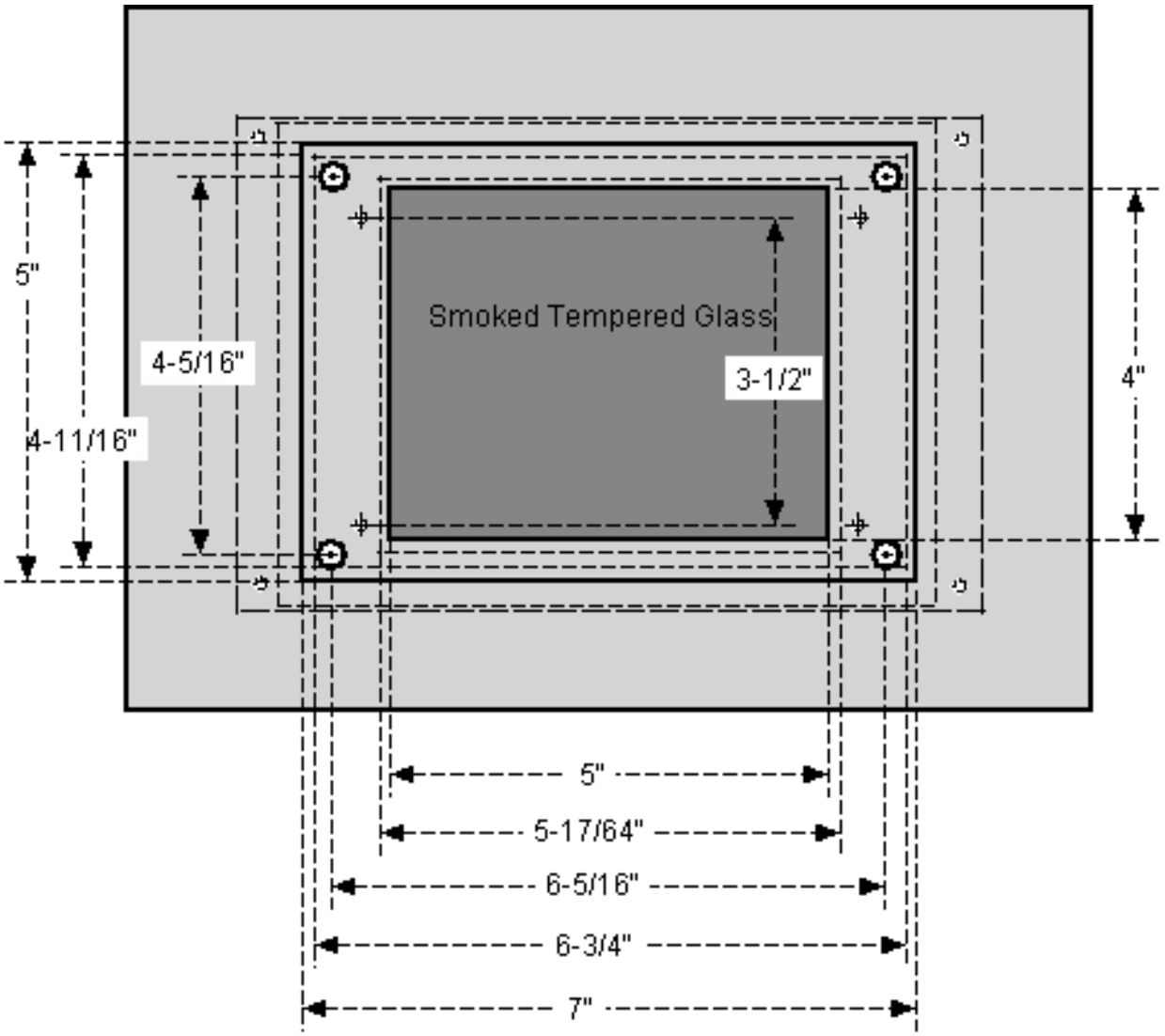
NO SCALE

Detail showing top view of Card reader inset in Car Panel



# Detail showing front view of Card reader inset in Car Panel

Front view of Car panel
with rabbitted removable panel
has all of the card reader components affixed .
Contained within an isolated enclosure within
the car operating panel enclosure. Card Reader
mounted on plate behind Glass (Glass required
to meet the A17.1 Code)



APPENDIX D

DSI 4200 Set Up

Power to be 24 VDC
For Card Reader W/RTE and for NON-Reader applications W/ RTE & Lock Refer to Figure #1.

Jumper settings:
1-IN (if resistors are used from DPS to DMU), OUT (other)
2-IN (failsafe maglocks), OUT (fail secure mortise)
3-OUT (N/C RTE INPUT)
4-IN (RTE or card reader), OUT (other)
5-IN
6-OUT
7-IN
8-IN
9-OUT
10-OUT
TIMERS
AUTO RESET-0 (RESETS WHEN DOOR CLOSES)
ALARM DELAY-8 (30 SEC)
SILENT TIME-7 (20 SEC)

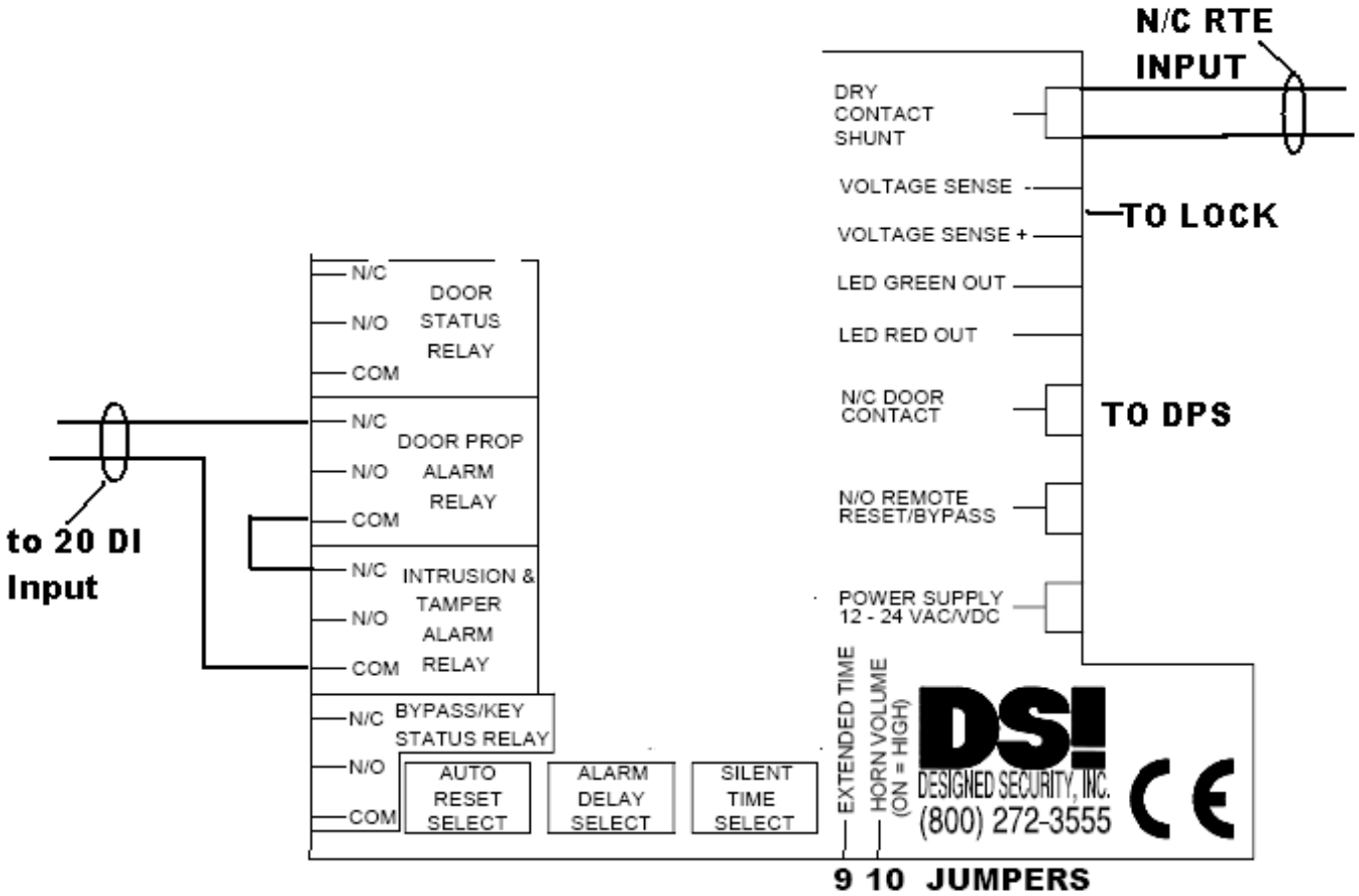



Figure # 1

DSI 4200 Set Up

For non-card reader applications W/O  RTE & lock refer to Figure #2:

Remove J4 (all others remain as listed above)
Jumper dry contact shunt (so as it remains N/C)
Provide power to voltage sense from power distribution module to allow for bypass. Set up as fail secure

****No door forced will be received.

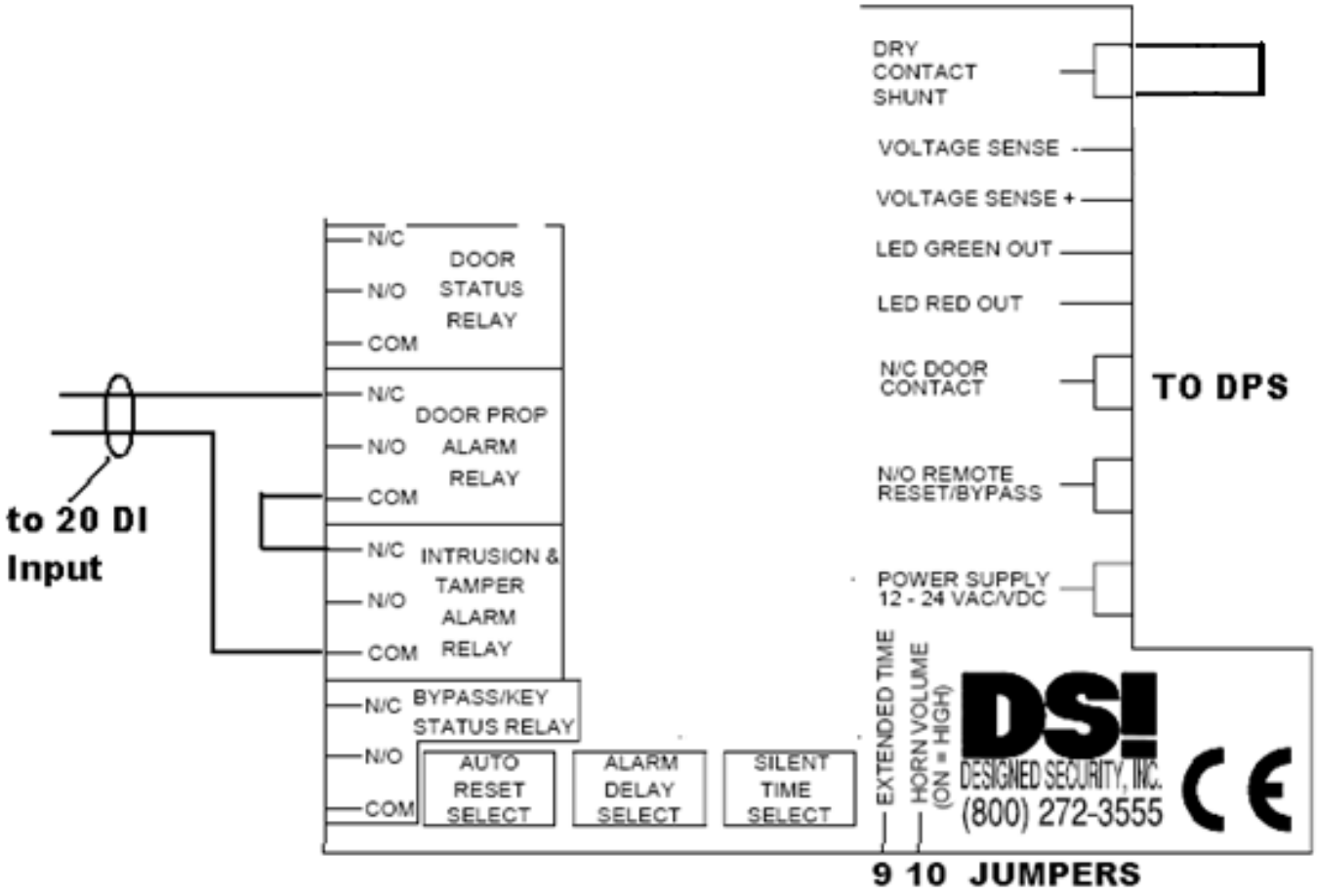
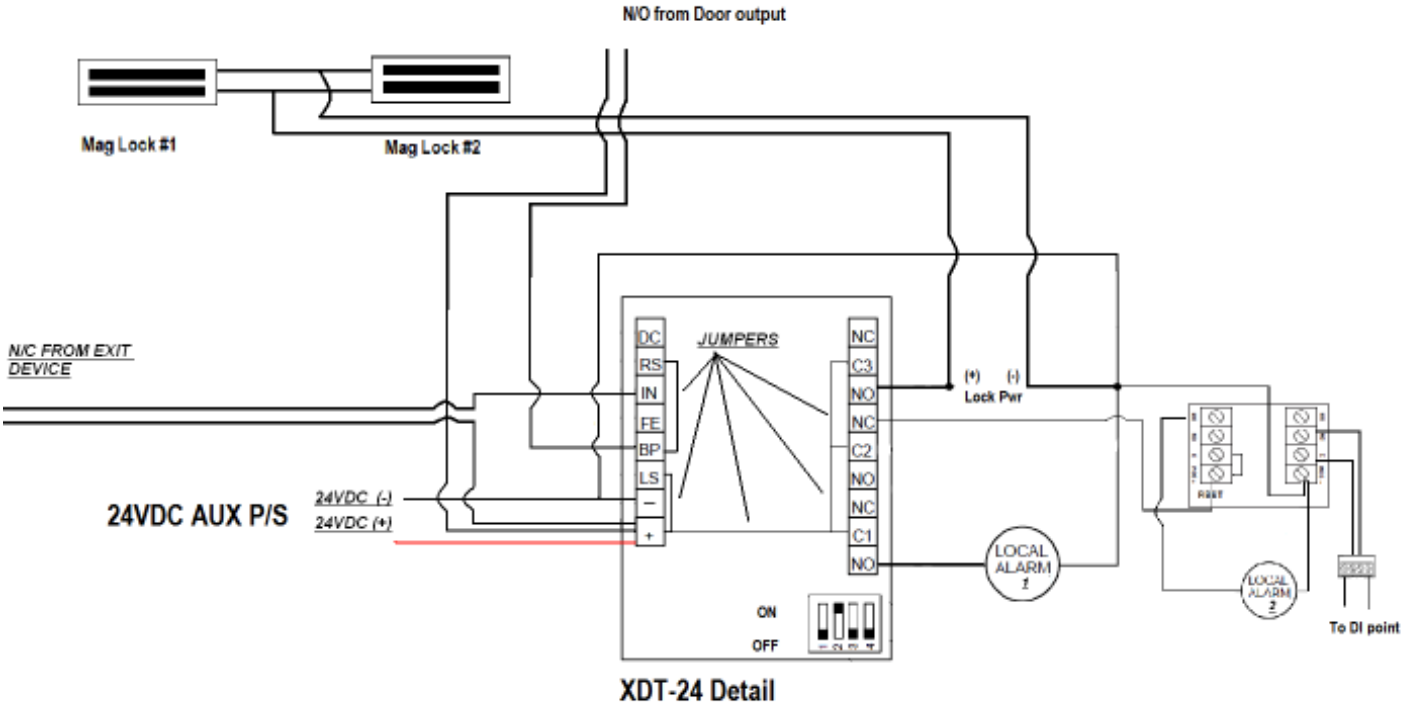



Figure # 2

APPENDIX E

Securitron Model XDT-24 delayed egress controller wiring diagram:



# Document Modification Schedule

| | | |
|---|---|---|
| Initial Publication | Oct. 19, 2009 | |
| Update #1 | Nov. 11, 2010 | |
| | 1.1 | Addition of Notice of Confidentiality |
| | 1.3, B | Addition of contact information prior to commencing work |
| | 2.2, B, 1, a, 15) | Updated alarm inputs |
| | 2.2, B, 3, b, 3) | Removed requirement for flashing red LED |
| | 2.2, B, 3, d | Addition of Associated Power Supplies |
| | 2.2, B, 10 | Addition of separate specifications for Field and Panel Resistors |
| | 2.2, B, 12, e, 2) | Addition to Electric Lock Power Supply Requirements |
| | 3.4, E | Addition to arrangement of cables within access panels |
| | 3.4, R | Addition of Card Reader connection directions |
| Update #2 | Jul. 26, 2011 | |
| | 3.2, B, 9 | Addition of serviceability requirement of door/frame. |
| | 3.4, W | Addition of connector requirement for electric locking mechanisms and power transfer hinges. |
| Update #3 | Aug. 8, 2011 | |
| | 2.2, C, 1, b, 1, c | Under electric exit devices Schlage was replaced with Corbin-Russwin. |
| | 2.2, C, 1, b, 2, b | Under mortise locks Von Duprin was replaced with Corbin-Russwin. |
| Update #4 | Jan. 18, 2012 | |
| | Appendix A | SMS was removed from the list pre-qualified security contractors. |
| Update #5 | Feb. 2, 2012 | |
| | 1.5 | Addition of Q. The University of Texas at Austin Video and CCTV Security Systems Policy to the References section. |
| Update #6 | May. 1, 2013 | |
| | Global | Removed all references to CCTV. |
| | Appendix D | Added DMU wire termination details |
| | Appendix E | Added XDT-24 delayed eqress wire termination details. |
| | 2.2, B, 3 | Changed card readers to HID SE series. |
| | 2.2, B, 7 | Changed delayed egress controller to XDT-24. |
| | Global | Changed all references from GE to UTC. |
| Update #7 | Jul. 15, 2014 | |
| | 2.2, B, 6, a | Clarified 24VDC for DMU |

| | | |
|---|---|---|
| | Appendix D | Clarified 24VDC for DMU |
| | Appendix A | Added Diebold Security to list of approved security contractors and also alphabetized the list. |