

**STANDARD SPECIFICATION**  
**SECTION 16720S**  
**INFOGRAPHIC SYSTEMS ENTRY CONTROL**  
**AND ALARM MONITORING SYSTEM**

	<u>Page</u>
<b>PART 1 - GENERAL</b>	<b>2</b>
1.01 <u>SCOPE</u> .....	2
1.02 <u>QUALITY ASSURANCE</u> .....	2
1.03 <u>RELATED DRAWINGS</u> .....	2
<b>PART 2 - PRODUCTS</b>	<b>3</b>
2.01 <u>GENERAL</u> .....	3
2.02 <u>CONTROLLER</u> .....	3
2.03 <u>CARD READER/KEYPADS</u> .....	3
2.04 <u>BIOMETRIC DEVICES</u> .....	3
2.06 <u>INTRUSION ALARM INPUT MODULES</u> .....	3
2.06 <u>LOCKING DEVICES</u> .....	3
2.07 <u>LOCKING DEVICE POWER</u> .....	4
2.08 <u>REQUEST-TO-EXIT (REX) DEVICES</u> .....	4
2.10 <u>CABLE</u> .....	4
<b>PART 3 - EXECUTION</b>	<b>5</b>
3.01 <u>GENERAL</u> .....	5
3.02 <u>CONTROLLER</u> .....	5
3.03 <u>CARD READERS/KEYPADS</u> .....	5
3.05 <u>LOCKING DEVICES</u> .....	6
3.06 <u>REQUEST-TO-EXIT (REX) DEVICES</u> .....	7
3.08 <u>VAULT TYPE ROOM (VTR) INSTALLATION</u> .....	7
3.09 <u>FINAL ACCEPTANCE AND TRAINING</u> .....	8

**STANDARD SPECIFICATION**  
**SECTION 16720S**  
**INFOGRAPHIC SYSTEMS ENTRY CONTROL**  
**AND ALARM MONITORING SYSTEM**

**PART 1 - GENERAL**

**1.01 SCOPE**

The work covered by this section of the specifications consists of the material and the work required to install a InfoGraphics Entry Control and Intrusion Alarm Monitoring System to restrict and monitor access to selected areas (i.e., vault rooms, vault-type rooms, sensitive areas, etc.). And the monitoring of intrusion alarms (both balanced magnetic switch and volumetric sensors). This specification is currently a special specification for the MESA project.

**1.02 QUALITY ASSURANCE**

The latest issue of the following specifications and standards form a part of these specifications.

- A. National Electric Code (NEC) (NFPA 70).
- B. Underwriter's Laboratories, Inc. (UL).
- C. National Fire Protection Association Standards (NFPA 101)

**1.03 RELATED DRAWINGS**

- A. The electrical drawings will delineate the InfoGraphics Entry Control and Intrusion Alarm System by locations of the controller, keypads, locking device, intrusion detection devices (both balanced magnetic door switches and volumetric), conduit routing and size, cable size, and all wiring diagrams required for proper connection of field cable.
- B. Raceways shown on the drawings are not intended to show all bends, kicks, offsets, couplings, and supports.

## PART 2 - PRODUCTS

### 2.01 GENERAL

- A. All electrical materials shall be new and approved by the Underwriter's Laboratories, Inc. for the application, except as otherwise specified herein.
- B. Materials and equipment shall be the standard product of manufacturers regularly engaged in the production of such material and shall be the manufacturer's current and standard design.

### 2.02 CONTROLLER

- A. The controller shall be manufactured by InfoGraphics Systems Corporation.
- B. The controller shall be a InfoGraphics Model ACU2 XL.

### 2.03 CARD READER/KEYPADS

- A. The card reader/ keypads shall be manufactured by InfoGraphics Systems Corporation.
- B. The InfoGraphics card reader/ keypad shall be Model No.RMS-2 unless drawings specify RMS 11 with separate RRE (typically for exterior applications).
- C. The card reader/keypad shall be mounted on a InfoGraphics keypad mounting plates as specified on the drawings.

### 2.04 BIOMETRIC DEVICES

Any biometric devices shall be as specified on the drawings.

### 2.06 INTRUSION ALARM INPUT MODULES

All intrusion alarm input modules shall be InfoGraphics Model RIM-0.

### 2.06 LOCKING DEVICES

- A. Electric strikes, electro-mechanical bored-in locks, electromagnetic locks, and other locking devices shall operate on 24VDC, unless specified otherwise on the drawings.
- B. Locking devices shall operate in the fail-secure mode, whereby the locking device unlocks when the solenoid is energized and automatically locks when the solenoid is de-energized. Electromagnetic locks shall operate in the fail-safe mode, whereby the magnetic will release the door upon loss of power.
- C. Electric Strikes shall conform to ANSI A156.5 (BHMA Standard 501) Grade 1.

#### D. Electro-Mechanical Bored-in Locks

1. Electro-mechanical bored-in locks shall be Sargent (Division of Kidde, Inc.), Model No. 8G71, 24VDC, 3W lock suitable for installing in hollow metal doors that are 1-3/4" thick.
2. Bored-in locks shall have the outside doorknob rigid at all times unless unlocked electrically or opened with a key.
3. The bored-in lock shall be keyed on the outside doorknob.
4. A Folger Adam Model No. 4-1/2EH Electric Hinge (non-load bearing) or approved equivalent shall be provided to replace the middle hinge on doors where bored-in locks are installed. The hinge shall have 5 #18 wire leads passing through the hinge to connect the locking device control wiring from the entry control system to the wiring inside the door going to the bored-in lock.

#### 2.07 LOCKING DEVICE POWER

The InfoGraphics ACU2 XL modules shall provide the power for the locking device. These Modules shall be equipped with gel cell battery back-up to provide a minimum of four (4) hours backup 24VDC power in the event normal operating power is lost.

#### 2.08 REQUEST-TO-EXIT (REX) DEVICES

The Contractor shall provide Detection Systems Model DS160 inside the secured area as required on the drawings.

#### 2.09 INTUSION ALARM HARDWARE

The alarm detection devices listed below, although not all inclusive, are commonly used in an IA system. No substitutes are allowed without the permission of the Electronic Security Department.

- Balanced magnetic switches: ADT (formerly Wells Fargo) (P/Ns SM-3, SM-4), Sentrol (P/N 2747A), (P/N 2707AD), (P/N 2757D).
- Passive infrared sensors: Aritech (P/Ns DR486, DR550, AP 633, AP669, DR851)
- Microwave space sensors: PROTECH (HITECH EX Series Explosion proof P/N HT 100EX, Passive Infrared/Microwave SDI-76 SDI-77, HT-50, HT-100)
- Tamper switch: Honeywell, Microswitch P/N 2AC6
- The Designer shall coordinate submittals with the Sandia/NM Electronic Security Department for the procurement of the Intrusion alarm sensors and related parts.

#### 2.10 CABLE

- A. The cable to the InfoGraphics card reader/keypads, shall be Belden 9369 or approved equivalent.

- B. The cable to the locking device shall consist of 1 twisted pair, 18 AWG, with an overall shield.
- C. The cable from the InfoGraphics controller to the REX devices shall be Southwest Model SW150410/G or approved equivalent.
- D. The cable from all intrusion detection sensors to the specified intrusion alarm input shall be a six-conductor #22 cable (Belden 9576 or approved equivalent).

PART 3 - EXECUTION

3.01 GENERAL

- A. All cable shall be installed in conduit, except where required to be routed in doorframes, inside doors for bored-in locks.
- B. No splices are allowed in the cable between any component in the entry control and intrusion alarm monitoring system, with the exception where necessary to connect to a locking device or associated hardware. Where required, splices shall be butt-spliced and covered with heat shrink tape. A tamper switch must protect all splices.

3.02 CONTROLLER

- A. Install the InfoGraphics controller in a convenient location inside the restricted-access room, unless indicated otherwise on the drawings. The controller shall be so mounted that the top of the cabinet does not exceed 6 feet, 6 inches above the finished floor.
- B. Connect the InfoGraphics controller to a dedicated 115 VAC, 15A circuit. Controller power wiring shall be #12 THHN installed in conduit. The conduit shall enter the controller at the bottom of the cabinet.
- C. Ground the controller cabinet to the building ground system with a #10 conductor color-coded green.
- D. The final switch settings and powering-up of the controller shall be completed by an authorized InfoGraphics representative or SNL Tech Security personnel

3.03 CARD READERS/KEYPADS

- A. The InfoGraphics card reader/keypad shall be installed on the appropriate InfoGraphics mounting box listed below, unless indicated otherwise on the drawings.

Mounting Box No.	Description
RMS-2	Standard Flush-Mounted Keypad
RMS-11	Heavy Duty Exterior Surface-Mounted Keypad

#### Installation of RMS-2:

- A. Mount card reader/keypads on the latch side of the door at a height of 40 inches from floor to keypad centerline, unless specified otherwise on drawings.
- B. Install a 3-stranded twisted pair Belden 9369 cable with an overall shield, color-coded Black, Red, from each RMS-2 to the InfoGraphics ACU2 XL.
- C. Provide a 12-inch cable service loop at each keypad to allow removal of the device for resetting switches or repair without disturbing field connections.
- D. All final switch settings at the keypad shall be completed by an authorized InfoGraphics representative or by Sandia Tech Security personnel.

#### Installation of RMS-11:

- A. Mount card reader/keypads on the latch side of the door at a height of 40 inches from floor to keypad centerline, unless specified otherwise on drawings.
- B. Install a 3-stranded twisted pair Belden 9369 cable with an overall shield, color-coded Black, Red, from each RRE to the InfoGraphics ACU2 XL.
- C. Install a 10-conductor cable (provided by InfoGraphics) from the RRE to the InfoGraphics RMS 11. All RMS-11 devices shall be within 25 feet of the associated RRE.
- D. Provide a 12-inch cable service loop at each keypad to allow removal of the device for resetting switches or repair without disturbing field connections.
- E. All final switch settings at the keypad shall be completed by an authorized InfoGraphics representative or by Sandia Tech Security personnel.

### 3.05 LOCKING DEVICES

- A. Install a 2 conductor, twisted, shielded 18 AWG cable from the locking device to the InfoGraphics controller. Locking device cable may be installed in the same raceway with card reader/keypad or REX device wiring.
- B. Install the locking device cable to the appropriate N.O. and N.C. terminals at the InfoGraphics controller for lock devices that have fail-secure operation.
- C. Install an InfoGraphics MOV (Metal Oxide Varistor) across the plus and minus lines going into the locking device to provide suppression of electrical noise.
- D. In doors where electro-mechanical bored-in locks are installed, replace the middle hinge on the door with an electric hinge (non-load bearing). Butt-splice wiring to the leads on the electric hinge and cover splice with heat shrink tape.

- E. Provide a 12-inch cable service loop at the locking device to allow removal of the device for cleaning or repair without disturbing field connections.

### 3.06 REQUEST-TO-EXIT (REX) DEVICES

- A. Install all REX devices inside the secured room.
- B. Mount REX sensor located at exit doors centered above the door mounted on the ceiling or the wall. For exact location contact Tech Security.

### 3.07 INTRUSION DETECTION DEVICES

All balanced magnetic switch (BMS) alarms shall be terminated at the associated RMS-2 "Door Contact" input. All volumetric sensor alarms shall be terminated into specified RIM intrusion alarm inputs.

Specify an ADT (formerly Wells Fargo) SM-4 balanced magnetic door switch and MB 4 spacer or a Sentrol balanced magnetic door switch 2707 AD for surface mounted and 2757D for a recessed at each exterior entrance door and vault perimeter door. Specify a Sentrol 2807T explosion-proof balanced magnetic door switch in hazardous locations. At each exterior roll-up door, exterior elevator door, or any other door that has a wide tolerance range in the closed position, install a Sentrol #2747A balanced magnetic switch on a #1961 L-mounting bracket.

Mount all volumetric sensors according as specified in drawings.

### 3.08 VAULT TYPE ROOM (VTR) INSTALLATION

When a request for a new vault or vault-type room is received, obtain the latest Sandia/NM Corporate Process Requirement document No: CPR400.39. An official version is located on the Sandia/NM Restricted Network (SRN). If the SRN is not accessible, contact Department 3111, Risk Management / Physical Security.

Consult with the Sandia/NM Electronic Security Department for the type and location of sensors to be installed in the vault room. Provide, if available, a layout of the room showing all furniture and heating and cooling equipment to assist the Sandia/NM Electronic Security Department personnel in the proper placement of infrared and microwave space alarm detection devices.

Provide a RIM cabinet in or near the vault room. It is recommended that the cabinet be installed outside the vault room for easy access by Entry Control and Intrusion Alarm System personnel. An existing RIM cabinet near the vault room may be used if the alarm capacity of the cabinet is not exceeded. To reduce the voltage drop, avoid excessive distance between the RIM cabinet and the vault room sensors.

Sensitive Compartmented Information Facilities (SCIFs) require a self-contained independent alarm system. Consult with personnel in the Electronic Security Department for the design guidelines of these special areas. For vault rooms that meet the NFPA definition of a vault, NFPA 232 shall be followed as well as security requirements. Contact Sandia/NM Facilities Fire Protection Engineering before applying the requirements of NFPA 232 unless this requirement is specified in the Design Criteria.

### 3.09 FINAL ACCEPTANCE AND TRAINING

#### A. Contractor Training and Qualifications

1. The Contractor shall be a licensed New Mexico electrical contractor.
2. The Installers employed by the Contractor shall have a minimum of 2 years experience installing InfoGraphics systems or shall have been certified by InfoGraphics as having been trained to install and test InfoGraphics systems.
3. The Installers to be used by the Contractor must possess a final Government-issued Q-clearance.
4. The Installers must have been trained by the Sandia/NM Electronic Security Department to use the specific methods of installation required by Sandia or must be prepared to spend time (over a period of 5 to 10 days) with the Sandia/NM Electronic Security Department learning these methods.

#### B. Final Acceptance

1. The Contractor shall obtain the services of Tech Security to approve final connections at the InfoGraphics controller, the card reader/keypad, intrusion detection devices, and the RIM-0, and to power up the system.
2. The Tech Security representative shall conduct operational tests in the presence of the Contractor, the Sandia Delegated Representative (SDR), and the system user.

END OF SECTION