SECTION 281300
ACCESS CONTROL AND INTRUSION DETECTION
Revised 04/30/2013

General Note Regarding All Security Systems: The security systems contractor shall conform to all current University of Utah specifications and standards and coordinate all work with the General Contractor and/or the University Project Manager and the UCard Office. All bids for access control and intrusion detection systems should utilize the online “BidSync site unless bid as a subcontract to a general contractor (http://www.bidsync.com). Additions to existing access control and intrusion detection systems will be managed by the UCard only if the cost is below $10,000 and an iSTAR panel is not required. All installations in new or renovation projects will be managed by the general contractor and/or the University Project Manager.

PART 1 -GENERAL

The University of Utah has standardized on the Software House C*Cure Security Management Control System. This document is subject to regular review and change. The latest revision of this document will always be available by request from the University of Utah UCard Office. Failure to follow manufacturer guidelines or the substitution of non-approved equipment or materials may result in the rejection of the installation and may require remediation efforts. Final approval of any installation work regarding University of Utah access control and intrusion detection systems rests solely with the UCard Office.

1.1 RELATED DOCUMENTS

A. Drawings and general provisions of the Contract, including General and Supplementary Conditions and Division 1 Specification Sections, apply to this Section.
B. The contractor installing the security system must be qualified, trained and licensed according to the following Utah Administrative Code requirements.
C. The contractor installing the security system must apply for an individual building permit from the University’s office of the Building Official.
D. An itemized list of equipment, with code compliance review completed, must be submitted with bid. No change orders will be accepted except for change in scope of work or unforeseeable circumstances.

1.2 SUMMARY

A. The Access Control and Intrusion Detection system is the Software House C*Cure system which includes a microprocessor based and managed access control system, with options for intrusion detection, and personal protection (duress) security and specifies sensors, detection devices, signal equipment, system controls, and displays. Each system installed will utilize either the iSTAR Pro or iSTAR Edge Controllers, or designated dialer. *See section 2.1.

1.3 DEFINITIONS

A. Hard-Wired System: Alarm, supervisory, duress, and detection devices are directly connected, through individual dedicated conductors, to central control panels.
B. Wireless System: Duress alarm system components and devices shall communicate wirelessly between portable transmitters and installed receivers hard wired back to a central panel.
C. Zone: Initiating device connected to a single duress alarm device circuit for annunciation of alarms.
1.4 SYSTEM DESCRIPTION

A. The system shall tie into the existing C*Cure access control system currently installed on the University Campus.
B. The system shall have access controlled doors as well as perimeter doors and hatches monitored with door position switches.
C. The system shall interface with the fire alarm system and in the event of an alarm, and shall unlock all controlled doors designated for emergency egress.

1.5 FUNCTIONAL PERFORMANCE

A. Any card access component of this system shall be an extension of the existing campus-wide C*Cure access control system utilized by the University of Utah for all their facilities, with all existing functions available and be completely compatible with the then current version of the C*Cure system installed.
B. Duress alarm: Performed by indicated hard wired stationary duress alarm button locations and remote wireless receivers that are triggered by portable transmitters.
C. Alarm Annunciation: In addition to the audible signal sounds and visual text indication on the system keypad, video images from associated cameras in the area may, at the election of UCard, be called up immediately and automatically to an assigned workstation for viewing. No additional operations for video call up by the control officers shall be necessary. Provide all licensing as required for C*Cure system and video system to perform automatic video camera call up via event programming in C*Cure.
D. Battery backup for all components in security system shall be capable of operating for a minimum of 8 hours in the event of a power failure.
E. Security contractor shall interface ADA openers where security access control is installed to allow for proper ADA access/egress as per building code.

1.6 SUBMITTALS

A. General: Submit the following to the University Project Manager for review and approval by the campus code officials, according to Conditions of Contract and Division 1 Specification Sections. Final design must have code compliance review completed prior to final approval by UCard.
B. As Built Shop Drawings: Detail assemblies of standard components that are custom assembled for specific application on this Project.
   a. Functional Block Diagram: Show single-line interconnections between components including interconnections between components specified in this Section and those furnished under other Sections. Indicate methods used to achieve systems integration. Indicate control, signal, and data communication paths and identify programmable logic controllers, networks, and control interface devices and media to be used. Describe characteristics of network and other data communication lines.
   b. Site and Floor Plans: Indicate final outlet and device locations inside and outside the building.
   c. Device Address List: Coordinate with final system programming.
   d. System Wiring Diagrams: Include system diagrams unique to Project. Show connections for all devices, components, and auxiliary equipment. Include diagrams for equipment and for system with all terminals and interconnections identified.
   e. Details of AC power connections and indicate if supplied by emergency power circuit(s).
   f. Sensor detection patterns and adjustment ranges.
C. System operation description, including method of operation and supervision of each component and each type of circuit, and sequence of operations for all manually and automatically initiated system inputs. Description must cover this specific Project; manufacturer’s standard descriptions for generic systems are not acceptable.
D. As-built drawings to be submitted only to the University Project manager in CAD format for turn over to the campus UCard office.
E. Separate Qualification Data for Manufacturers and Installers: Demonstrate their capabilities and experience as specified in Quality Assurance Article. Include lists of completed projects with project names and addresses, names of Contracting Officer and Government representatives, plus other information specified.

F. Record of field tests of system performed with UCard representative during final inspection.

1.7 QUALITY ASSURANCE

A. Installer Qualifications: The system shall be installed by a contractor who has been regularly engaged in the installation of access control and security equipment for at least 5 years. The installer shall be a Software House sales and services representative of the C* Cure system submitted. UCard will provide the current list of Software House certified vendors who can implement the Software House C* Cure access control systems on campus. These are the only vendors that can be utilized for the implementation of access control systems. Provide, in writing, proof of compliance with system manufacturers service and installation certification programs. Installer must be capable of providing emergency maintenance and repairs for the overall system at the project site with 24 hours maximum response time. The installer shall have a local office staffed with factory trained technicians, fully capable of supervising installation, system start-up, providing training and servicing of both hardware and software for systems of similar complexity and function as the system described in this specification.

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

C. Listing and Labeling: Provide system and components that are listed and labeled for their indicated use and location on the Project.
   a. The Terms "Listed" and "Labeled": As defined in the "National Electrical Code," Article 100.
   b. Listing and Labeling Agency Qualifications: A "Nationally Recognized Testing Laboratory" (NRTL) as defined in OSHA Regulation 1910.7.
   c. Comply with UL Standard 609, 1023, and 1076.
   d. FM Compliance: Provide FM-approved card access system and components.
   e. FMG Compliance: FMG-approved and labeled intrusion detection devices and equipment.
   f. Single-Source Responsibility: Obtain system components from a single source (the prime system manufacturer) that assumes responsibility for system components and for their compatibility.

D. Testing: The campus UCard Office will perform final system testing. Contractor must provide notification to Project Manager that system is complete and ready. Project Manager will schedule the final testing with the UCard Office.

1.8 WARRANTY

A. Special Warranty: Manufacturer's standard form in which manufacturer and Installer agree to repair or replace components of access control and intrusion detection devices and equipment that fails in materials or workmanship within specified warranty period.
   1. Warranty Period: Two years from date of final walk-through and sign-off by UCard.

1.9 EXTRA MATERIALS

A. Furnish extra materials as required for this specific project.

PART 2 -PRODUCTS

2.1 MANUFACTURERS

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

<table>
<thead>
<tr>
<th>Description</th>
<th>Manufacturer</th>
<th>Part Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>iSTAR Control Panel, 8 slot,</td>
<td>Software House</td>
<td>iSTAR008W-64ANPS</td>
</tr>
<tr>
<td>Component</td>
<td>Supplier</td>
<td>Model</td>
</tr>
<tr>
<td>----------------------------------------</td>
<td>---------------------------</td>
<td>------------------------------</td>
</tr>
<tr>
<td>w/cables</td>
<td></td>
<td></td>
</tr>
<tr>
<td>iSTAR Control Panel, 16 slot, w/cables</td>
<td>Software House</td>
<td>iSTAR016W-64ANPS</td>
</tr>
<tr>
<td>Back-up Batteries</td>
<td>Any</td>
<td>Batteries 1270</td>
</tr>
<tr>
<td>Power Supply</td>
<td>Altronix ACMCB</td>
<td>Maxim 33D</td>
</tr>
<tr>
<td>Power Supply</td>
<td>Altronix Power</td>
<td>Maxim 33E</td>
</tr>
<tr>
<td>Power Supply</td>
<td>Altronix PD</td>
<td>PD8CB</td>
</tr>
<tr>
<td>Power Supply</td>
<td>Altronix</td>
<td>AL300ULX</td>
</tr>
<tr>
<td>PS Board</td>
<td>Software House</td>
<td>ACM8CB</td>
</tr>
<tr>
<td>Input Boards</td>
<td>Software House</td>
<td>AS0073</td>
</tr>
<tr>
<td>Output Boards</td>
<td>Software House</td>
<td>AS0074</td>
</tr>
<tr>
<td>Mounting Enclosures</td>
<td>Altronix or Software House</td>
<td>I/O Enclosures</td>
</tr>
<tr>
<td>Biometric Reader</td>
<td>L-1 or Bioscript</td>
<td>V-FLEX 4G WR (S) or V-SMART-A-H</td>
</tr>
<tr>
<td>Keypad Card Reader</td>
<td>Software House</td>
<td>RM2L-IC</td>
</tr>
<tr>
<td>I-Class R-30</td>
<td>HID</td>
<td>6110AKN0000</td>
</tr>
<tr>
<td>HID I-Class R-40</td>
<td>HID</td>
<td>6120AKN0000</td>
</tr>
<tr>
<td>HID I-Class RK-40</td>
<td>HID</td>
<td>6130AKN0000</td>
</tr>
<tr>
<td>HID I-Class R-10</td>
<td>HID</td>
<td>6100AKN0000</td>
</tr>
<tr>
<td>RM Board</td>
<td>Software House</td>
<td>RM4</td>
</tr>
<tr>
<td>Recessed Door Contact</td>
<td>S1078</td>
<td></td>
</tr>
<tr>
<td>Surface Door Contact</td>
<td>SR2505AL</td>
<td></td>
</tr>
<tr>
<td>REX MULTI-TECK</td>
<td>DS160</td>
<td></td>
</tr>
<tr>
<td>Push to Exit</td>
<td>Securitron</td>
<td>EEB2</td>
</tr>
<tr>
<td>DPDT Relay Push to Exit handicap</td>
<td>Securitron</td>
<td>DPDT</td>
</tr>
<tr>
<td>Door Strikes</td>
<td>Von Duprin</td>
<td>6211 FSE 24VDC US32D</td>
</tr>
<tr>
<td>Motion Detectors</td>
<td>DS9360</td>
<td></td>
</tr>
<tr>
<td>Glass Break Detectors</td>
<td>CK-FG1625</td>
<td>ISW-EN1247</td>
</tr>
<tr>
<td>Panic Buttons</td>
<td>Husk</td>
<td>Husk Panics</td>
</tr>
<tr>
<td>Resistors</td>
<td>Software House</td>
<td>GI 6644</td>
</tr>
<tr>
<td>Double Mags</td>
<td>Any</td>
<td>3002DSM2</td>
</tr>
<tr>
<td>LED Status Boxes</td>
<td>Any</td>
<td>LED</td>
</tr>
<tr>
<td>Door Mags</td>
<td>Any</td>
<td>M62-64</td>
</tr>
<tr>
<td>Dialer</td>
<td>Radionics</td>
<td>D7412GV3-C</td>
</tr>
<tr>
<td>Alpha Numeric Command Center Keypad</td>
<td></td>
<td>D1255W</td>
</tr>
<tr>
<td>E-Net Interface for G series</td>
<td>Inovonics</td>
<td>DX4020</td>
</tr>
<tr>
<td>Commercial Wireless Interface</td>
<td>ISW-D8125CW</td>
<td></td>
</tr>
<tr>
<td>Wireless Repeater</td>
<td>ISW-EN5040-T</td>
<td></td>
</tr>
<tr>
<td>Panic Wireless Panel</td>
<td>Inovonics</td>
<td>EN4232MR</td>
</tr>
<tr>
<td>Key Fob Panics</td>
<td>Inovonics</td>
<td>EN1223S</td>
</tr>
<tr>
<td>Pam Relay</td>
<td>Any</td>
<td>PAM-1</td>
</tr>
<tr>
<td>Rollup Door Contacts</td>
<td>Any</td>
<td>SR-2507AD</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ISW-EN1215WEOL</td>
</tr>
<tr>
<td>Inswing Mag</td>
<td>Any</td>
<td>3000TJ30LH-HSM</td>
</tr>
<tr>
<td>Key Override Switches</td>
<td>Any</td>
<td>MK2</td>
</tr>
<tr>
<td>Crash Bar w/mounting hardware</td>
<td>Von Duprin</td>
<td>98L X 996L X US26D</td>
</tr>
<tr>
<td>Crash Bar and FS</td>
<td>Von Duprin</td>
<td>CX 98L X 996L X US26D</td>
</tr>
<tr>
<td>ADA door RF receiver kit</td>
<td></td>
<td>8310-3860TW</td>
</tr>
<tr>
<td>Crash Bar Whip</td>
<td>Beacon Metal</td>
<td>18 inch door loop</td>
</tr>
<tr>
<td>Mag Locks</td>
<td></td>
<td>390 + DSM/MBS</td>
</tr>
<tr>
<td>Double Mag Locks</td>
<td></td>
<td>392 + DSM/MBS</td>
</tr>
</tbody>
</table>
**Door Contact**
Inovonics
FA210W

**Door Receiver**
Inovonics
FA416R

**Door Programmer**
Inovonics
FA116

**Motion Detectors**
Inovonics
ISW-EN1262

**Smoke Detector**
Inovonics
ISW-EN1242

**Composite Cable**
Belkin
CSC 112115

**12 input Grounding Bar**
Any
PK12GTA

*Additional wire and cable part numbers found in section 2.11

* UCard will obtain/maintain the “white sheets” of all products utilized within the C*Cure system.

**2.2 ACCESS CONTROL AND INTRUSION DETECTION SYSTEM EQUIPMENT, GENERAL**

The contractor shall follow the best practices for equipment installation. If cabling is required within the contractors Scope of Work, the contractor shall install cabling to minimize EMF interference and inductive noise within the installed cable locations. These best practices include but are not limited to:

A. Surge Protection: Comply with minimum requirements of UL Standard 1449, "Transient Voltage Surge Suppressors," for each component using solid-state devices and having a line voltage power source connection or an exterior underground signal connection.

B. Provide at the locations identified, a complete and C*Cure System including but not limited to the following equipment:
   a. iSTAR Pro or iSTAR Edge controller
      i. iSTAR Pro controllers can be purchased and installed as either an 8 door package or a 16 door package. The Altronix Power Supply AL300ULX can be used for powering 2 iSTAR Pro controllers when they are installed in the same room.

<table>
<thead>
<tr>
<th>16 READER FRONT END PACKAGE</th>
</tr>
</thead>
<tbody>
<tr>
<td>QTY</td>
</tr>
<tr>
<td>-----</td>
</tr>
<tr>
<td>1</td>
</tr>
<tr>
<td>1</td>
</tr>
<tr>
<td>2</td>
</tr>
<tr>
<td>1</td>
</tr>
<tr>
<td>1</td>
</tr>
<tr>
<td>2</td>
</tr>
<tr>
<td>Up to 16</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>8 READER FRONT END PACKAGE</th>
</tr>
</thead>
<tbody>
<tr>
<td>QTY</td>
</tr>
<tr>
<td>-----</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>---</td>
</tr>
<tr>
<td>1</td>
</tr>
<tr>
<td>2</td>
</tr>
<tr>
<td>2</td>
</tr>
<tr>
<td>1</td>
</tr>
<tr>
<td>1</td>
</tr>
<tr>
<td>Up to 8</td>
</tr>
</tbody>
</table>

b. I-Class Card Readers
c. Relay output contacts
d. Motion Detectors
e. Request to Exit Devices
f. Door Contacts
g. All power supplies and/or transformers
h. All equipment, security devices, components, wire, cable, and mounting hardware as required to meet specification requirements and manufacturers documented installation procedures.

C. A concerted effort should be made to not include magnetic door locks within alarm and access systems at the University. Magnetic door locks will require a key override. Magnetic door locks will require a push-to-exit button which temporarily cuts local power to magnetic lock. All electric strikes and all exterior doors must be wired to fail-to-secure.

2.3 ELECTRICAL POWER

A. Normal System Power Supply: 120 V 60 Hz from locked disconnect device. System components are supplied with power through separate power supplies. Provide all required power supplies and associated transformers as specified by the manufacturer and required for the installation.

a. The iSTAR Pro is provided without an uninterruptible power supply. The Advanced Power System (apS) is rated at 100-240 VAC, 50/60 Hz, 2.3A max@100VAC, 1.1A@240 VAC, and will provide
nominal 12 VDC output at 3.5 Amps in excess of four hours when using the supplied, single 18AH battery. An additional 18 AH battery shall be installed to provide 8 hours of battery-backed power.

B. Power Source Transfer: When normal power is interrupted, system is automatically switched to backup supply without degradation of critical system function or loss of signals or status data. Whenever possible, the system should be tied to the building’s emergency power.

2.4 CARD ACCESS SYSTEM HARDWARE, GENERAL

A. Manufacturers:
   a. *See section 2.1

B. Types, features, accessories, and mounting conditions of individual devices are as indicated.

C. Battery Back-up: The access control panel (iSTAR Pro and/or iSTAR Edge controller) shall be provided and wired with back-up battery power for a minimum of eight hours operation upon loss of AC power.

D. Suppression: The access control panel shall have provisions for relay suppressor kits for each relay used, to protect the access control panel from collapsing electrical fields.

E. Card Readers: Card readers shall be HID Prox-Pro and HID Mini-Prox readers matching the readers currently installed on campus for door control. The access control panel shall support card readers using Wiegand, Proximity and Biometrics technologies.

2.5 DOOR AND WINDOW SWITCHES

A. Manufacturers:
   a. *See section 2.1.

B. Description: Balanced-magnetic switch, complying with UL 634, installed on frame with integral overcurrent device to limit current to 80 percent of switch capacity. Bias magnet and minimum of [two] [three] encapsulated reed switches shall resist compromise from introduction of foreign magnetic fields. Position switches on doors shall be magnetic reed switch type and shall be per manufacturers recommendations for the type of door installed on. Provide concealed door frame types

C. Flush-Mounted Switches: Unobtrusive and flush with surface of door and window frame.

D. Overhead Door Switch: Balanced-magnetic type, listed for outdoor locations, and having door-mounting magnet and floor-mounting switch unit.

E. Remote Test: Simulate movement of actuating magnet from central-station control unit.

2.6 EXIT REQUEST DEVICES

A. Manufacturers:
   a. See section 2.1.

B. Comply with UL Standard 639, and the following general requirements:
   a. Passive Infrared (PIR) Devices: Detect request to exit by monitoring infrared energy emitted within the door exit zone. Units are sensitive to the infrared wavelengths emitted by the human body and are insensitive to general area thermal variations.

C. On door types (see drawing schedules) that do not show motion detectors being used, the request to exit function will be handled by the switched exit hardware devices. It shall be the responsibility of the security contractor to coordinate with the hardware contractor in wiring of power transfer hinges and switched exit devices. The only doors that do not require any exit request are doors with a reader on both sides.

2.7 POWER SUPPLIES.

A. Manufacturers:
   a. *See section 2.1.

B. Provide power supplies as per manufacturers written recommendations with total number of powered devices for each power supply restricted to only consuming 75 percent of the power supplies rated amperage. Provide separate power supplies for system controllers (As per manufacturer), card readers (12VDC, 5 A), and locks
2.8 ACOUSTIC-TYPE, GLASS-BREAK SENSORS (Typically not used, motion detectors are preferred)

A. Manufacturers:
   a. *See section 2.1.

B. Device Performance: Detect unique, airborne acoustic energy spectrum caused by breaking glass.
   a. Sensor Element: Microprocessor-based, digital device to detect breakage of plate, laminate, tempered, and wired glass while rejecting common causes of false alarms. Detection pattern shall be at least a 20-foot (6-m) range.
   b. Hookup Cable: Factory installed, not less than 72 inches (1830 mm).
   c. Activation Indicator: LED that lights on sensor housing when responding to vibrations, remaining on until manually reset at sensor controller or at central-station control unit.
   d. Controller: Integral with sensor housing or in a separate assembly, locally adjustable by control under housing cover.
   e. Glass-Break Simulator: A device to induce frequencies into protected glass pane that simulate breaking glass without causing damage to glass.

2.9 PHOTOELECTRIC SENSORS

A. Manufacturers:
   a. *See section 2.1.

B. Device Performance: Detect an interruption of a pulsed, infrared, light beam that links transmitter and receiver.
   a. Sensitivity: Detect standard-intruder movement within sensor's detection patterns at any speed of less than 7.5 fps (2.3 m/s) though the beam. Allow installation of multiple sensors within same protected zone that will not interfere with each other.
   b. Activation Indicator: LED indicator shall not be visible during normal operation. Indicator shall light when sensor detects a standard intruder. Locate test enabling switch under sensor housing cover.
   c. Remote Test: When initiated by central-station control unit, start a test sequence for each detector element that simulates standard-intruder movement within sensor's detection patterns, causing an alarm.

2.10 MICROWAVE-PIR DUAL-TECHNOLOGY MOTION SENSORS

A. Manufacturers:
   a. *See section 2.1.

B. Description: Single unit combining a sensor that detects changes in microwave signals and a PIR sensor that detects changes in ambient level of infrared emissions caused by standard-intruder movement within detection pattern.

C. Device Performance: An alarm is transmitted when either sensor detects a standard intruder within a period of three to eight seconds from when the other sensor detects a standard intruder.
   b. PIR Sensor Sensitivity: Adjustable pattern coverage to detect a change in temperature of 2 deg F (1 deg C) or less, and standard-intruder movement within sensor's detection patterns at any speed between 0.3 to 7.5 fps (0.09 to 2.3 m/s) across 2 adjacent segments of detector's field of view.
   c. Microwave Sensor Sensitivity: Adjustable, able to detect standard-intruder movement within sensor's detection pattern at any speed between 0.3 to 7.5 fps (0.09 to 2.3 m/s). Sensor sensitivity adjustments shall be accessible only when sensor housing is removed, and sensors shall comply with 47 CFR 15.
   d. Activation Indicator: LED indicator shall not be visible during normal operation. Indicator shall light when sensor detects a standard intruder. Locate test enabling switch under sensor housing cover.
   e. Remote Test: When initiated by central-station control unit, start a test sequence for each detector element that simulates standard-intruder movement within sensor's detection patterns, causing an alarm.

2.11 WIRE AND CABLE
A. General: Provide both TPS (Twisted pair Shielded) and TP (Twisted Pair) as indicated in the drawings, with the appropriate number of pairs. Provide Cat 5e UTP for emergency telephone signal wiring.

B. Comply with Division 26 Section "Wires and Cables" except as indicated.

C. Cable for Low-Voltage Control and Signal Circuits: Shielded twisted-pair cable with drain. Comply with Division 26 Section "Wires and Cables."

D. Additional Cable and wiring:
   a. HID Card Reader-Weigand-Composite cable part number CSC #702790
      i. 1-22/6 conductor overall shield (Reader)
      ii. 1-18/4 conductor (Lock Power)
      iii. 1-22/2 conductor (Door Contact)
      iv. 1-22/4 conductor (Request to Exit)
   b. RM Style Card Reader-RS485-CSC #112102
      i. 1-18/2 pair individually shielded
   c. Inside Card Reader on IN/OUT Door-Weigand-CSC #110253
      i. 1-22/6 conductor overall shield
   d. Alarm Door Contact-CSC #110105
      i. 1-22/2 conductor
   e. Alarm Motion Detector-CSC #110205
      i. 1-22/4 conductor
   f. Duress/Panic Button-CSC #110105
      i. 1-22/2 conductor
   g. RM input/output Modules-RS485-CSC #112102
      i. 1-18/2 pair individually shielded

2.12 RACEWAY

A. Comply with Division 26 Section "Raceways."

2.13 POWER REQUIREMENTS

To ensure adequate power, installer must calculate the total power requirements of the iSTAR Pro controller and related hardware. If the maximum power consumption exceeds the output of the iSTAR Pro power supply, an additional power supply must be connected to the system.

PART 3 -EXECUTION

3.1 INSTALLATION

Failure to follow these guidelines may result in rejection of contractor equipment installation and require remediation before installation acceptance. Clarification of planned installation procedures and methodology must be reviewed with UCard prior to contractor installation. These practices are specified but not limited to:

A. General:
   a. Install system according to NFPA 70, applicable codes, and manufacturer's printed instructions.
   b. Install system according to manufacturer’s instructions and best practices.

B. Wiring method:
   a. Install all wiring in raceways
   b. ¾ inch minimum conduit is required
   c. Multiple home runs may be contained in a single conduit of appropriate size
   d. Conceal raceways except in unfinished indoor spaces
   e. Conduit fill shall not exceed 40%.

C. Wiring within panels and enclosures
   a. Wiring shall be neat and workmanlike
   b. Cables shall be individually labeled
c. Cable management using spools, guides, supports and other devices shall be used
d. Cable shielding and grounding SHALL be utilized in panels and enclosures
e. Shield grounding SHALL be at the panel and NOT at the device (to avoid ground loops)
f. Cable routing within the enclosure or panel shall be neat and workmanlike
g. Number of terminated conductors shall be in accordance with manufacturers recommendations and/or requirements
h. Un-terminated conductors shall be electrically isolated and secured within the enclosure or panel
i. Appropriate splices, taps or terminations shall be in an approved junction box
j. External device power supplies shall be installed in UCard approved locations.

D. Installer Examination:
   a. Installers must examine areas and conditions under which access control systems are to be installed, and notify Contractor in writing of conditions detrimental to proper completion of work. Do not proceed with the work until the unsatisfactory conditions have been corrected in a manner acceptable to Installer.

E. Adjusting and Cleaning:
   a. Touch-up scratched and marred surfaces to match original finishes; remove dirt and construction debris.

F. Examples of typical door piping for card reader doors are below. PDF File is available as a separate document on the ucard web page. [www.ucard.utah.edu](http://www.ucard.utah.edu)
3.2 NAMING AND PROGRAMMING CONVENTION

*Prior to programming, installers must consult with UCard for appropriate building numbers, names and abbreviations.

A. Convention:
   a. Use the official University of Utah campus building numbers, and the University designated room numbers.
   b. Descriptive abbreviations should be used as most C*Cure program display boxes are limited in size.

B. iSTARs:
   a. Building Number: iSTAR Number L# Door# Room Description
      i. Ex.; 0003:03 L1 0166 Northwest Comm Rm
             0079:02 L2 2000D L2 Data Closet
             0525:19 L4 East Comm Rm by Elevator
   b. A more complete description of the iSTAR’s location, access requirements (card access, key number, how to find the room where the iSTAR is located, etc.) should be entered in the description section of the configuration identification screen.
      i. Ex.; Located on level one, room 1001, (or across from elevator) using key RT2674 or access
card.
c. Programming
   i. Leave time zone box blank.
   ii. Tamper, AC power fail and Low Battery inputs should all be defined and properly working.
   iii. An event should be defined for controller communication failure.

C. iSTAR Clusters:
a. Naming: Building Number: iSTAR L#
   i. Ex.; 0003:03 L1 Cluster
         0079:02 L2 Cluster
         0525:19 L4 Cluster

D. Reader, Input & Output Device:
a. Naming: Building Number:iSTAR number, (IZ, PH, EX, etc) – if included in intrusion zone, pharmacy, exterior door, etc.: (input/output type) (DC, REX, DL, ML, GB, DUR, MOT) Room number, L#, which board it is controlled by (ACM, I8 or RM) and which port or relay it is wired to on the board to which it is attached.
   i. Ex.; 0851:01 1125 Lab Reception 1-R6 (reader 6 on ACM 1 of iSTAR 1)
         0043:01 (IZ):MOT Safe Rm 1-I7 (motion sensor within intrusion zone)
         0086:04 DC L1 DSL/TACC RM-4-I1 (door switch monitor on RM board number 4)
         0512:01 DC L1 E101 Conf Rm I8:1-I4 (door switch monitor on I8 board number1)

b. Programming:
   i. Input and output state changes should not be sent to the Monitoring Station and should only be sent to the Journal if it is part of an intrusion zone, panic button or other life safety or high level security feature; i.e. freezers.
   ii. Readers should have the continuously active box checked.
   iii. Reverse sense of input should only be used in exceptional situations and then only temporarily.
   iv. No unused inputs, outputs, readers, doors or any other element should be defined in the system.
   v. After complete installation, no input supervision errors, open loops, or line faults should be reporting in the Monitoring Station.

E. Door:
a. Naming: Building Number: iSTAR number (Door type) – IZ (intrusion zone), EX (exterior door), PH (pharmacy) University assigned room number (if known) Floor (if applicable): Description
   i. Ex.; 0019:03 0490 Atmos Comp/Vis
         0575:01 (EX) L1 North Entry
         0521:13 3C354 Vascular Surgery Back Dr

b. A more complete description of the door can be entered in the description section of the configuration identification screen.

F. Camera:
a. Naming: Building Number View Description (IP Address) Camera Model Number
   i. Ex.: 0086 Loading Dock (10.0.86.5) Axis P3346

*UCard is generally responsible for programming the following:

G. Event:
a. Naming: Building Number : iSTAR number, (type) – (intrusion zone, duress, etc) : Event Description
   i. Ex.; 0026:01 (DU) Rm 106 Duress Evt
         0032:01 Unlock Usher Rm Evt
         0179:01 (IZ): Arm Event Group Evt

b. A more detailed description should be entered if the cause of the event or required action to the event needs to be displayed on the General Activity Monitor screen.

H. Clearance:
a. Naming: Building Number – Partition name if other than default, Description, (type) – (IZ-intrusion zone, PH-pharmacy, etc.), time range (D-D 0000-0000)
   i. Ex.; 0093 Natatorium Men’s Pool Entry C1r
         0179 Ext Ent M-F 0800-1700 Clr
b. The type and/or location of the doors in the clearance should be clear.

I. Schedule:
   a. Naming: Building Number: iSTAR number (if applicable for event activation) – Description, time range (D-D 0000-0000)
      i. Ex.; 0053:01 Disability Center Unlock M-F 0800-1700 Scd
              0722:02 Shop Area Force Arm M-S 2200 Scd
              0086 Custodial Day M-F 0600-1500 Scd
      ii. Since there is no place for a detailed description, the time specification name should supply as much information in as an abbreviated form as possible.

   b. Programming:
      i. The time zone box must be left blank when defining a time specification.

I. Groups:
   a. Naming: Building Number: Floor (if applicable): Description
      i. Ex.; 0512 Ext Door Grp for door group
              0556 Patient ElevGrp for elevator group
              0865 EvtGrp for event group
              0064 InputGrp for input group
              0035 OutputGrp for output group
              Etc.
      ii. There is a description box that can be used to clarify particular group information if necessary.

3.3 GROUNDING

C* Cure system components and conductor and cable shields MUST be grounded at the panel or enclosure. There are two types of grounds within the C* Cure equipment; Electrical/powersupply ground and electronic or signal ground. Proper grounding of the electrical or power supplies eliminate shock hazards and provides safety for field technicians working on the C* Cure equipment. Proper electronic grounding vastly improves the quality of communications connectivity to the many types of devices interconnected with the C* Cure system. Proper electronic or signal grounding is important to minimize ground loops, common mode returns, noise pickup, cross talk, and other impairments within the C* Cure access control system.

**Ground requirements are as follows:**

A. Ensure that the iSTAR Pro controller is properly connected to an earth ground at the ground stud near the AC input wiring.
B. Ensure that the shield wires are grounded at one end of the cable to panel ground stud.
C. Do NOT ground the shield at the device end (no ground loops)
D. When disconnecting wiring, disconnect ground wires last (to provide maximum protection to the equipment and personnel).

3.4 FIELD QUALITY CONTROL
A. Manufacturer's Field Services: Provide services of a factory-authorized service representative to supervise the field assembly and connection of components and system pre-testing, testing, adjustment, and programming.

B. Inspection: Verify that units and controls are properly labeled and interconnecting wires and terminals are identified.

C. Pre-testing: Align and adjust the system and perform pre-testing of all components, wiring, and functions to verify conformance with specified requirements. Correct deficiencies by replacing malfunctioning or damaged items with new items. Retest until satisfactory performance and conditions are achieved.

D. Testing: Provide at least 10 days' notice of acceptance test performance schedule.

E. Operational Tests: Perform operational system tests to verify conformance with specifications. Test all modes of system operation and intrusion detection. Methodically test for false alarms in each zone of space intrusion detection devices by simulating activities outside indicated detection patterns.

F. Installer Start-up Responsibility: The Installer shall initiate system operation. The Installer shall provide competent start-up personnel until the system is fully functional. Upon reoccurring technical problems, the Installer shall supply factory direct Manufacturer's support in the form of factory technical representation and/or diagnostic equipment until the resolution of those defined problems.

G. Final testing must be observed by a representative of the campus UCard Office. Complete security system must be approved and accepted by UCard.

END OF SECTION 281300
General Note Regarding All Video Systems: The Video systems contractor shall conform to all current University of Utah specifications and standards and coordinate all work with the General Contractor and/or the University Project Manager and UCard Office. Standards and specifications are subject to regular review and change as video/surveillance technology continues to evolve. The latest revision is available by request from the UCard office.

PART 1 -GENERAL

The University of Utah has standardized on OnSSI Ocularis as the primary video monitoring and recording software for surveillance and other video monitoring functions. The Software House C*Cure Access Control system integrates completely with the OnSSI video system. Currently installed video systems can be made compatible with the OnSSI system through interface devices. The video systems contractor must have a minimum of two local technicians certified in OnSSI video systems.

1.1 RELATED DOCUMENTS:

A. Drawings and general provisions of Contract, including General and Supplementary Conditions and Division-1 Specification sections, apply to work of this section.
B. Division-26 Basic Electrical Materials and Methods sections apply to work specified in this section.
C. An itemized list of equipment must be submitted with bid. No change orders will be accepted except for change in scope of work or unforeseeable circumstances.
D. The contractor or sub-contractor installing the video system must be qualified and trained to OnSSI standards and Axis certified.

1.2 SUMMARY:

A. Video management systems shall integrate with the Software House CCURE 9000 software. The IP video surveillance control and management system shall handle an unlimited number of cameras and alerts through a desktop-based or mobile video client.
B. Extent of video surveillance systems work is indicated by drawings and schedules. Video surveillance systems are comprised of, but not limited to cameras, camera enclosures, monitors, servers, switches, signal transmission lines, controls and accessories, and shall be viewable from desktop-based or mobile video clients.
C. Work of this section includes raceways, electrical boxes and fittings, wiring/cabling, and control/signal transmission media, as specified in applicable Division-26 Basic Electrical Materials and Methods sections, which are used in conjunction with installation of video surveillance systems.

1.3 SUBMITTALS:

A. Product Data: Submit to Project Manager for UCard Office review and approval, the manufacturer's data on video surveillance systems including components and accessories. **Final design must be approved by UCard prior to installation.**
B. Shop Drawings: Submit layout drawings of video surveillance systems showing scaled components and spatial relationship to associated equipment.
C. Wiring Diagrams: Submit wiring diagrams for video surveillance systems, including interconnecting signal/video units and electrical power connections to equipment and components. Show physical layout of signal and power cabling.
D. Description of system operation to include exact locations of cameras with field of view and lens sizes shown. Provide on floor/site plans in PDF or CAD format.

E. Design Considerations: Design specifications, camera models and camera placements shall be specifically defined and approved by UCard prior to bid process for surveillance systems. The following guidelines must be considered during the design phase:
   a. Target image – i.e. facial recognition at what distance from camera
   b. Potential obstructions in view
   c. Light levels and sensitivity
   d. Video compression and viewing/recording frame rates
   e. Network connectivity

1.4 QUALITY ASSURANCE:

A. Installer's Qualifications: Firms with at least 3 years of successful installation experience with projects utilizing IP video surveillance system work similar to that required for this project. Installers must have a demonstrated background, of at least 3 years, in advanced networking from Cisco Systems and Microsoft.

B. Codes and Standards:
   a. Electrical Code Compliance: Comply with applicable local code requirements of the authority having jurisdiction and NEC 800-Series articles as applicable to installation, and construction of video surveillance equipment and signal distribution systems.
   b. UL Compliance: Comply with applicable requirements of UL Standards 486A and B, 813, 983, 1409, 1410, 1412, 1414, 1416, 1417, and 1418 pertaining to video surveillance system products. Provide video surveillance systems and components that are UL-listed and labeled.
   d. EIA Compliance: Comply with applicable requirements of Electronic Industries Association Standards RS-170, 222, 232, 312, 330, 403, 412, 420, 439, and 455 pertaining to video surveillance equipment and accessories.
   e. FCC Compliance: Comply with Subpart J of PART 15, FCC Rules pertaining to computing devices including Class A, Class B, personal and peripheral types. Provide equipment which complies with technical standards for both radiated and power line conducted interference.

1.5 WARRANTY

A. Special Warranty: Manufacturers standard form in which manufacturer and Installer agree to repair or replace components of video surveillance devices and equipment that fails in materials or workmanship within specified warranty period which is two years from date of final walkthrough and sign-off by UCard.

PART 2 -PRODUCTS

2.1 MANUFACTURERS:

A. Manufacturers: Subject to compliance with requirements, provide video surveillance system products of the following (for each type of product):
   a. Video Surveillance Wire/Cable: The primary cabling is Ethernet cabling, either Cat 5 or Cat 6. Cat 6 cable shall be used for any new or replacement cable installations. Additional cable may be required for the environmental controls of outdoor housings or additional power requirements for PTZ (Pan-Tilt-Zoom) cameras. However, as cameras have continued to evolve, the additional power required for these other camera functions, can often be met within the High-Power PoE (Power-Over-Ethernet) standard. Any deviation shall require approval from UCard prior to installation of substitute cabling.

<table>
<thead>
<tr>
<th>Signal</th>
<th>From</th>
<th>To</th>
<th>Belden #</th>
<th>Gauge</th>
<th>Pairs</th>
<th>Shielded</th>
<th>Max Length</th>
</tr>
</thead>
<tbody>
<tr>
<td>RJ45-Ethernet</td>
<td>Camera</td>
<td>Network</td>
<td>(See Ethernet)</td>
<td>Cat 5 or</td>
<td>4</td>
<td>N/A</td>
<td>Max 328 ft.</td>
</tr>
</tbody>
</table>
Ethernet extenders may be used in rare circumstances to provide reliable connectivity. Use of extenders must be approved by UCard during the design process.

b. Video Surveillance Equipment: The University of Utah has standardized on the Axis product line for video surveillance. Common Axis camera models used by the university are listed. Other camera models may be required for specific surveillance purposes, but must still contain the remote focus feature. However, any substitution or deviation from Axis camera products, or these specific Axis models, must be approved by UCard prior to installation.

<table>
<thead>
<tr>
<th>Axis Model Number</th>
<th>Device Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>P3346 (V or VE as required)</td>
<td>Fixed Dome</td>
<td>3MP; Multi-view; H.264 multi stream; audio; I/O ports; remote focus</td>
</tr>
<tr>
<td>P3354 (720p or 1MP)</td>
<td>Fixed Dome</td>
<td>1MP; H.264; remote focus</td>
</tr>
<tr>
<td>P3364 (V, or VE as required)</td>
<td>Fixed Dome</td>
<td>1MP, H.264; remote focus</td>
</tr>
<tr>
<td>P3364-LV</td>
<td>Fixed Dome</td>
<td>1MP, IR illumination, H.264; remote focus</td>
</tr>
<tr>
<td>P3367 (V, or VE as required)</td>
<td>Fixed Dome</td>
<td>5MP, Multi-view, H.264 multi stream; remote focus</td>
</tr>
<tr>
<td>P1344 (E as required)</td>
<td>Traditional Fixed</td>
<td>1MP; H.264; Multi-view; remote focus</td>
</tr>
<tr>
<td>P1346 (E as required)</td>
<td>Traditional Fixed</td>
<td>3MP; H.264; Multi-view; remote focus</td>
</tr>
<tr>
<td>P1347 (E as required)</td>
<td>Traditional Fixed</td>
<td>5MP; H.264; Multi-view; remote focus</td>
</tr>
<tr>
<td>Q1755-E</td>
<td>Traditional Fixed</td>
<td>2MP; 10x optical zoom;</td>
</tr>
<tr>
<td>P5534 (720p)</td>
<td>PTZ</td>
<td>High Resolution – (0.74 Lux Color, 0.04 Lux B/W)</td>
</tr>
<tr>
<td>P5534-E (720p)</td>
<td>PTZ</td>
<td>High Resolution – (0.74 Lux Color, 0.04 Lux B/W) Ruggedized Housing IP66</td>
</tr>
<tr>
<td>Q6034-E (720p)</td>
<td>PTZ (18X Zoom)</td>
<td>High Resolution – Outdoor – (0.74 Lux Color, 0.04 Lux B/W) Ruggedized Housing IP66</td>
</tr>
<tr>
<td>Q6035-E (1080p)</td>
<td>PTZ (20X Zoom)</td>
<td>High Resolution – Outdoor – (0.8 Lux Color, 0.04 Lux B/W) Ruggedized Housing IP66</td>
</tr>
<tr>
<td>Q1910-E (13mm)</td>
<td>Thermal with Housing</td>
<td>Fixed Focal Length - Indoor or Outdoor</td>
</tr>
<tr>
<td>Q1921-E (10, 19, 35 or 60mm)</td>
<td>Thermal with Housing</td>
<td>Fixed Focal Length - Indoor or Outdoor</td>
</tr>
</tbody>
</table>

Provide mounting hardware as required.

c. Legacy analog camera conversion: existing camera installations can be converted to the Ocularis OnSSI system with the addition of conversion hardware. While replacement of analog cameras with newer high-definition models is preferred, the following hardware must be used in situations where analog camera images are determined to be sufficient.

| Q7401 Single Channel | Analog Encoder | Converts Analog Camera to IP Network |
| Q7404 Four Channels | Analog Encoder | Converts Analog Cameras to IP Network |
| Q7406 Six Channels (blade) | Analog Encoder | Converts Analog Cameras to IP Network |
| M7010 Sixteen Channels | Analog Encoder | Converts Analog Cameras to IP Network – 15 Frames Per Second |
2.2 OnSSI Video Software and Hardware:

A. UCard maintains the centrally managed servers for the Ocularis Surveillance system as well as the appropriate server(s) for the cameras at various locations throughout the campus. Installations/conversions of fewer than 8 cameras will record to existing Ocularis servers. Installations/conversions of 9 or more cameras will require an additional recording server which will be supplied and maintained by UCard. Cost of these servers is covered within monthly camera fees already billed to the departments.

B. Video Monitoring Workstations require a minimum of:
   a. CPU : Intel core i7 (similar or better)
   b. RAM: 8GB
   d. Graphics Adapter: PCI-Express, 1GB RAM w/dual DVI outputs 35 simultaneous Video Channels – 1GB
   e. Software: Microsoft .NET 3.5 Framework and DirectX 9.0 or newer.

C. Switches: All IP camera installations must be connected to a campus standard PoE rated switch.

2.3 RACEWAYS, AND ELECTRICAL BOXES AND FITTINGS:

A. General: Provide raceways, electrical boxes and fittings complying with Division-26 Basic Electrical Materials and Methods sections "Raceways" and "Electrical Boxes and Fittings", in accordance with the following listing:
   a. Rigid Steel Conduit.
   b. Rigid Metal Conduit Fittings. Type 1.
   c. Electrical Metallic Tubing (EMT).
   d. EMT Fittings.
   e. Interior Outlet Boxes.
   f. Junction and Pull Boxes.
   g. Bushings, Knockout Closures and Locknuts.

PART 3 -EXECUTION

3.1 EXAMINATION:

A. Examine areas and conditions under which video surveillance systems are to be installed, and notify Contractor in writing of conditions detrimental to proper completion of the work. Do not proceed with the work until unsatisfactory conditions have been corrected in a manner acceptable to Installer.

3.2 INSTALLATION OF VIDEO SURVEILLANCE SYSTEMS:

A. Install video surveillance systems and components where indicated, in accordance to NFPA 70, with equipment manufacturer's written instructions, in compliance with National Electrical Code, and with recognized industry practices, to ensure that video surveillance system complies with requirements and serves intended purposes.

B. Wiring Method: Install all wiring only in raceways, 3/4" minimum, or cable trays. Multiple home runs may be contained in a single conduit of appropriate size. Conceal raceways except in unfinished indoor spaces. Conduit fill shall not exceed 40%.
C. Wiring within enclosures: Label, bundle, wrap, and train the conductors to terminal points with 6-inches of slack minimum, 12-inches of slack maximum. Provide and use cable management hardware and distribution spools. Wire shielding, where used, should remain un-cut as much as possible.

D. Number of Conductors: As recommended by system manufacturer for functions indicated.

E. Splices, Taps, and Terminations: Make splices, taps, and terminations on numbered terminal strips in junction, pull and outlet boxes, terminal cabinets, and equipment enclosures.

F. Tighten connections to comply with tightening torques specified in UL Standard 486A.

G. Identification of Conductors and Cables: Color-code conductors and apply wire and cable marking tape to designate wires and cables so media are identified and coordinated with system wiring diagrams.

H. Install power supplies and other auxiliary components for camera devices at the locations pre-approved by UCard.

3.3 GROUNDING: Grounding is a critical installation practice for the University’s video surveillance system. There are two types of grounds used with video surveillance equipment; Electrical/Power-Supply ground and Electronic or signal ground. Proper grounding of the electrical or power supplies will eliminate shock hazards and provide increased safety for field technicians working on the video surveillance equipment. Proper electronic grounding vastly improves the quality of communications connectivity to the many types of devices interconnected within the video surveillance system. Proper electronic or signal grounding is important to minimize ground loops, common mode returns, noise pickup, cross talk, and other impairments within the University’s video surveillance system.

A. Ensure that any power supplies are properly connected to an earth ground near the AC input wiring.
B. For devices appropriate for cable shield grounding, ensure that any shield wires are grounded at the power supply end of the cable to the ground referenced above.
C. Do NOT connect the shield to ground at the far end cabled device. (This will avoid the potential for “ground loops”.)
D. When disconnecting wiring, disconnect ground wires last (to provide maximum protection to the equipment and personnel.)

3.4 ADJUSTING AND CLEANING:

A. Set field-adjustable video surveillance system components for input voltages, current settings and frequency settings.
B. Touch-up scratched and marred surfaces to match original finishes; remove dirt and construction debris.

3.5 FIELD QUALITY CONTROL:

A. Upon completion of installation of video surveillance system components, and after circuitry has been energized with normal power source, test video surveillance systems to demonstrate view quality, capability and compliance with requirements. Where possible, correct malfunctioning units at site, then retest to demonstrate compliance, otherwise remove and replace with new units and proceed with retesting.

END OF SECTION 282300