BSA-Architects, Inc.

12946 Dairy Ashford, Suite 360
Sugar Land, Texas 77478
Main: (713) 529-5071
www.bsa-architects.com

Addendum 002

Date: September 20, 2018
Project: Texana Administrative Office Building
Owner: Texana
Architect: BSA-Architects, Inc. – Project No. 217130
To: Invited Bidders
No of Pages: 2 Sections (Two)

This Addendum forms a part of the Contract Documents and modifies the Bidding Documents dated August 28, 2018 with amendments and additions noted below.

Acknowledge receipt of this Addendum in the space provided in the Bid Form. Failure to do so may disqualify the Bidder.

Description:

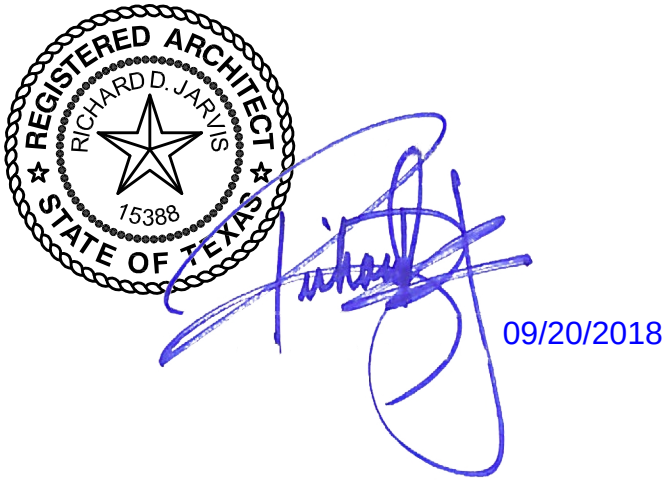
Disregard the second occurrence of Spec Section 281300 and Spec Section 282300. The first occurrence of Spec Section 281300 will govern Access Control & Video Surveillance Systems.

Sheets:

Second occurrence of Spec Section 281300 and Spec Section 282300

- End of Document -

Submitted by
Richard D. Jarvis, AIA
15388, State of Texas
Project Architect



Disregard this Sheet
Refer to first Section 28 13 00 in Spec Book for Access Control

SECTION 28 1300

SECURITY – ACCESS CONTROL

PART 1 - GENERAL

1.01 WORK INCLUDED

A. Comply with provisions of Section 27 05 00.
B. Provide new and functional security equipment. Ensure proper operation of all new equipment provided under this project. Provide the following new equipment.
   1. Proximity door contact switch, recessed in jamb.
   2. Request to Exit contacts in locking hardware on all doors with card access control.
   3. Card Reader access unit do not include alarms.
C. Visit the site prior to bidding to verify existing conditions.
D. Provide all materials and equipment, and perform all work and testing for the complete execution of the work as shown on the drawings, as herein and specifically shown on the drawings or herein specified, but required to insure complete operation of the Security System per design intent inherent in the subject project. All equipment shall be UL listed.

1.02 RELATED WORK

A. Comply with the following sections issued for construction.

1.	Section 27 15 00	Cable Plant Overview
2.	Division 26	Conduit
3.	Division 26	Pull and Junction Boxes
4.	Division 26	Hangers and Supports
5.	Division 08	Door Hardware

1.03 REFERENCES

A. American Society for Testing and Materials (ASTM)
   1. ASTM E814 - Fire Tests of Through-Penetration Firestops
B. Underwriters Laboratories, Inc. (UL)
   1. UL 1479 - Fire Tests of Through-Penetration Firestops
C. National Fire Protection Association (NFPA):
   1. NFPA 70 - National Electrical Code, 2005.
   2. NFPA 101 – Life Safety Code.
   3. NFPA 730 – Premises Security.
   4. NFPA 731 – Security System Installation.
D. Americans with Disabilities Accessibility Guidelines.
E. Code of Federal Regulations, Title 29, Chapter XVII, Part 1910 SHA).
F. International Building Code 2000 Edition.

1.04 SUBMITTALS

A. The installing contractor and/or equipment supplier shall provide complete and detailed shop drawings and include:
   1. Control panel wiring and interconnection schematics.
   2. Riser diagrams.
   3. Complete floor plan drawings locating all system devices.
   4. Factory data sheets on each piece of equipment proposed.
   5. Detailed system operational description. Any specification differences and deviations shall be clearly noted and marked.

Disregard this Sheet
Refer to first Section 28 13 00 in
Spec Book for Access Control

6. Complete system bill of material.

B. All submittal data will be in bound form with Contractor's name, supplier's name, project name, and state security license number adequately identified.

C. Before final acceptance of work, the Contractor shall deliver five (5) copies of composite "Operating and Shop Maintenance Manual." Each manual shall contain, but not be limited to:

1. A statement of guarantee date of termination and name and phone number of the person to be called in the event of equipment failure.
2. Individual factory issued manuals containing all technical information on each piece of equipment installed. In the event such manuals are not obtainable from the manufacturer, it shall be the responsibility of the Contractor to compile and include them. Advertising brochures or operational instructions shall not be used in lieu of the required technical manuals.
3. As-built conduit layout diagrams including wire color code and/or tag numbers.
4. Complete as-built wiring diagrams.
5. Copy of acceptance test reports.

1.05 WARRANTY.

A. The Contractor shall directly guarantee the system equipment to the Owner for a period of one (1) year from the date of final acceptance of the system against defects in materials and workmanship.

1.06 QUALITY ASSURANCE

A. Manufacturer Qualifications
B. The manufacturers of all hardware and software components employed in the SMS shall be established vendors to the access control/security monitoring industry for no less than five (5) years and shall have successfully implemented at least 5 systems of similar size and complexity.
C. Contractor / Integrator Qualifications
   1. The security system integrator shall have been regularly engaged in the installation and maintenance of integrated access control systems and have a proven track record with similar systems of the same size, scope, and complexity.
   2. The security system integrator shall supply information attesting to the fact that their firm is an authorized product integrator certified with the SMS. A minimum of one technician shall be a Certified C•CURE 9000 installer.
   3. The security system integrator shall supply information attesting to the fact that their installation and service technicians are competent factory trained and certified personnel capable of maintaining the system and providing reasonable service time.
   4. The security system integrator shall provide a minimum of three (3) references whose systems are of similar complexity and have been installed and maintained by the security system integrator in the last five (5) years.
   5. The security system integrator shall provide references of Marathon ever-run high ability fail over systems experience in the last (5) years.

1.07 PRICING

A. Vendors shall bid ACM's, and other components with labor for each listed separately in each of the two categories (ACM's, other).
B. Provide each itemized price list as follows:

Disregard this Sheet
Refer to first Section 28 13 00 in
Spec Book for Access Control

1. Individual hardware components. The list should indicate by component, quantity, unit price and total price.
2. Associated cable and hardware.
3. Installation labor.
4. Applicable local, state and federal taxes.
5. Total system cost.

PART 2 - PRODUCTS

2.01 EQUIPMENT

A. Access Control System Description

1. The existing system is the CCure 9000 Enterprise access control system. It shall be configured to connect to an "Enterprise Solution" network at an off-site location with no additional modification. Contractor shall ensure all network requirements are connected to controllers for control by existing CCURE 9000.
2. The standard ACM's system consists of an access control system capable of reading and supporting the owner's 26 bit and 35-bit HID Corporate 1000 card formats and be configured to support the following:

Number of Online Inputs	128
Number of Online Outputs	512
Number of addressable**	512
paces unlimited Number of Cardholders*	40
Number of Assets	40
Number of Simultaneous Client PC's	4
Number of definable Client PCs	250

3. The ACM's shall be maintained as a networked, continuous duty, on line, computer based, integrated access control and alarm monitoring system with capability of integral electronic badge production and imaging.
4. ACM's data communication networks shall be dedicated exclusively for the bi-directional transfer of data between host/server, workstations, multiplexed field panels and field installed security devices. The networks shall be continuously active, fully supervised and shall be designed to support multiplexed data communications. The data communications network shall be configured such that failure or malfunction of a single component, which is connected to the network, shall not interfere with the normal basic operation of other components connected to the network. Workstations not on the supervised ACM's data network, (LAN, Internet or dial-up) must be approved by the owner on an individual basis.
5. Access control and/or alarm monitoring device transaction messages generated from field installed devices shall be transmitted to the ACM's host/server from a series of remote multiplexed field panels via the fully supervised data communications network. Similarly, operator initiated and automatic system commands shall be transmitted to remote field panels via the data communications network. It shall be the responsibility of the Security Contractor to determine the exact number of multiplexed field panels, elevator interface panels and communications network required in compliance with manufacturer's recommendations. Field panels not on the supervised ACM's data network (LAN, Internet or dial-up) must be approved by the Owner on an individual basis.
6. All additional ACM's APC field panels shall have at least one (1) megabyte of memory and must support a minimum capacity of 128 proximity card readers, 512 monitoring or intrusion alarm inputs and 512 outputs and 40,000 access card holders.

Disregard this Sheet
Refer to first Section 28 13 00 in
Spec Book for Access Control

7. Other than additional multiplex field panels, field devices and workstations, additions to host/server hardware or software shall not be required in order to accommodate future expansion of the initial ACM's configuration as described herein and as shown on the drawings, to the minimum capacities as specified above.
8. The Security Contractor shall be responsible for the provision and connection of 24 VDC power supplies and associated circuitry as required for operation of NOC electric locksets, NIC strikes and electromagnetic locks at card reader controlled doors. Electric locksets, strikes and electromagnetic locks are NOT provided and installed by the Security Contractor, but rather the door hardware contractor. Electric lockset, strike and magnetic lock power supplies shall be located in the telecommunications closets. If the ACM's requires any additional equipment to accomplish the connection and interface, the Security Contractor shall furnish and install all equipment.
9. The Security Contractor shall be responsible for providing all final connections to the 24 VDC power supplies at access-controlled doors utilizing electrified panic exit hardware must have REX contacts. The power supplies for the electrified panic exit hardware shall be provided and installed by the door hardware contractor above the ceiling at each door location. All connections between the lockset and or Rim device and pass through hinge and to the power supply above the ceiling shall be provided by the door hardware provider.
10. Electronic locksets with REX contacts are preferred to magnetic locking devices for non-critical applications and shall be specified when appropriate.
11. Door hardware shall be based upon Sargent 80 Series electrified hardware. Contractor to reference Door Hardware specifications in section 08 71 10 for details.
12. All security doors controlled by the ACM's shall have a door position switch.
13. The Security Contractor shall be responsible for compliance with all codes and for obtaining any required lock and/or alarm permit(s). Required drawings for permitting must be requested from the architect or security consultant. Unless required by code, all devices should fail- secure.
14. The Security Contractor is responsible for all necessary relays to interface security access controls and locks with automatic door openers or door locking devices provided by the door hardware vendor contractor. The automatic door hardware contractor shall provide a cable for the connection above the door for activation upon a successful card read.
15. The Security Contractor shall provide an interface between the ACM's and the locking hardware at access controlled doors such that the ACM's can unlock and lock the door locally with the card reader and remotely from any ACM's workstation. The fail-safe locksets and power supplies shall be powered and controlled by the fire alarm system.
16. The door monitoring system shall be composed of a door position switch with prop open alarm on each perimeter exit door and any other doors identified by the owner. All door position switches (DPS or DS) shall be monitored by the ACM's or a commercial security system is to be provided if no ACM's is available.
17. Standard door position switches shall be the internal recessed type. External door contacts shall have concealed wiring or be connected by armored cable.
18. The Security Contractor must identify needs for wall space within the telecommunications closets for multiplex field panels and step-down transformers for the ACM's. All components for the ACM's requiring 110 VAC shall be wall mounted at these locations. Coordination of wall space in existing IDFs with the ISD Project Manager and GC is required.
19. The Security Contractor shall coordinate 110 VAC power for the multiplex field panels, elevator interface panels and devices from circuits provided by others.
20. All necessary information to allow the Security Contractor to load individual card data into the ACM's system database shall be provided by the Owner to the Security Contractor. It shall be the responsibility of the Security Contractor to initiate and coordinate this process. If the required data is available in an electronic form, the Security Contractor shall coordinate with the Owner to establish a mutually agreed data format to facilitate batch

Disregard this Sheet
Refer to first Section 28 13 00 in
Spec Book for Access Control

import. The Security Contractor shall be responsible to provide all software, hardware, customization and manpower necessary to import all necessary data into the initial ACM's database.

21. Access controlled doors with electrified locksets; electrified panic exit devices are to be designed for free mechanical egress. These doors shall also be interfaced to the fire alarm system, such that when a fire system alarm is activated, the locking mechanism will disengage and be rendered inoperable allowing free egress through the doors. The Security Contractor shall provide all connections, boxes, conduit, additional relays, etc. for a complete interface in full compliance with current fire codes. The Security Contractor shall be responsible for all required lock and alarm permits.
22. The Security Contractor shall be responsible for connection of the ACM's host/server, workstations, badge stations, printers, etc. to the uninterruptible power supply circuits provided by others behind the security console and equipment racks. It shall be the Security Contractors responsibility to extend these circuits to complete connection to all security equipment as required.
23. The Security Contractor shall be responsible for interfacing the ACM's to specified Delayed Egress System(s) (DES) for authorized temporary bypass of non-automatic doors utilizing the delayed egress magnetic locks. The card reader on the secure side of the door and the request to exit motion detector on the non-secure side of the door shall unlock the delayed egress magnetic locks upon a valid entry or exit. The interface between the ACM's and the DES shall also provide for monitoring the status of all emergency exit doors. For each delayed exit door, the DES shall annunciate and individual alarm point in the ACM's system when the timing sequence has been initiated.
24. The Security Contractor shall be responsible for providing an interface between the ACM's and automatic door equipment for access control operations at automatic doors. All equipment associated with the automatic doors shall be provided and installed by the door hardware contractor. Upon a valid access request, the ACM's shall enable the push pad for a programmable time period during which the door shall open and the magnetic locks unlock when the push pad is depressed. The ACM's shall not release and/or open the door directly. The request to exit motion detector on the exit side shall be designed to only shunt the door contacts associated with the security system. The automatic door shall utilize its own exit push pad or motion detector to release the magnetic locks and open the door. The request to exit motion detector must be passive infrared or multiple technology type.
25. The Security Contractor shall be responsible for providing an interface between the ACM's and the automatic door equipment for access control operations at handicapped doors. Upon a valid access request, the ACM's shall unlock the associated locking hardware and enable the push pad for a programmable time period during which the door shall automatically open when the push pad is depressed. The ACM's shall unlock the door and shunt the door contacts but shall not initiate the automatic door operator. The request to exit motion detector on the exit side shall be designed to unlock the associated locking hardware and shunt the door contacts associated with the security system. The automatic door shall utilize its own exit push pad or motion detector to automatically open the door.
    Under counter door open override buttons for automatic sliding doors shall be provided and installed by the automatic door contractor.
26. The Security Contractor shall be responsible for providing all required coordination to verify exact locations of and affecting the work of ACM's.
27. The Security Contractor shall check with the owner to verify that applicable licenses for the number of doors being added to the system is available.

B. Software Requirements for the ACM's shall utilize the (CCure 9000) access control system software, configuration of expansions or connections shall include, but not limited to the following:

Disregard this Sheet
Refer to first Section 28 13 00 in
Spec Book for Access Control

1. Communication Supports
   a. Communications between Host/Server and local workstations shall be accomplished via industry standard network protocols including TCP/IP over 10/100Mbs Ethernet. Any communication via a non-dedicated network must be approved by the Owner.
   b. The ACM's software shall support communications between the Host/server and multiplexed field panels or controllers via multiple RS-232 or RS-485 serial interfaces.

2. Password Control:
   a. ACM's software shall support a user-defined number of operators (at a minimum 128 operators). The name and an operator definable unique alphanumeric password shall be required to log on the ACM's system. Through user programmable assignments, multi-level operator groups can be set up such that access privileges and allowable operations, for which each individual ACM's operator is authorized, can be strictly defined. The minimum number of distinct system access levels or operator privilege groups shall be 64.

3. System and Data Protection:
   a. ACM's shall provide for the protection of system functions and database access. Such protection shall be user definable according to the access privilege granted to a particular operator group the operator is associated with. After a successful login the protection feature may restrict display at operator workstation's, view of "edit only" view, only those database data and system transactions which are associated only with a predefined portion of the data.
   b. Password control shall be utilized for database access by all remote ACM's workstations.

4. Access Control Operations:
   a. Access Authorized: Upon confirmation that a request for access is valid, a "door-open" command shall be generated by the multiplex field panel and shall be subsequently cause the release of the associated electric locking mechanism for a predetermined interval and shall shunt the associated monitor devices for a user-defined period of time. All information pertaining to valid access transactions shall be stored on the ACM's hard disk.
   b. Access Denied: In the event that an access request is not valid, no "door open" command shall be transmitted and the alarm monitor devices shall not be shunted. All information pertaining to invalid access requests shall be stored on the ACM's hard disk and break through alarm as well as an audible alarm shall sound at the selected operator workstations.
   c. Reader Override: The ACM's software shall provide for override of card reader operations and door unlock via manually initiated keyboard commands at an operator workstation or by an automatically executed time schedule which has been pre- programmed by the user in the ACM's database. All such override events shall be stored on the ACM's hard disk.

5. Breakthrough Alarms:
   a. The ACM's software shall provide for the display of "breakthrough" alarm messages or graphics at the selected operator workstations such that operators will be alerted to an active alarm condition during periods when other than standard ACM's display is presented on the operator workstations. Breakthrough alarms shall cause activation of the audible sounder at the selected operator workstations.
   b. For alarm events requiring operator acknowledgement, a data input dialogue window containing user programmable information, list box and data input screen

Disregard this Sheet
Refer to first Section 28 13 00 in
Spec Book for Access Control

shall be provided for operator to acknowledge, record actions taken or enter comments.

c. The protection function shall also provide for alarm handling such that alarm transactions can be vectored to one, several or all operator workstations. This function shall be assignable on a point-by-point basis.

6. Failure reporting:
   a. All failures and/or malfunctions associated with the ACM's data communications network, multiplex field panels or hard-wired operator workstation components shall cause immediate activation of the audible sounder at operator workstations, display of a unique message on the workstations, printing of the messages at the workstation printers and storage of the event in the system historical records. Failure reporting messages shall be programmable allowing the messages to be routed to selected operator workstations.

7. Audit Trail:
   a. The ACM's software shall provide for an audit trail feature which is designed to record all changes or modifications to the ACM's database. The time at which a record was last changed and which system operator made the change shall be recorded. Audit trail information shall be automatically stored on the ACM's hard disk. Additionally, all additions, deletions or modifications to the ACM's database shall be routed to a workstation printer in order to provide a permanent record of such changes
   .

8. Alarm Monitoring Database:
   b. The computer based processing, display and storage of information related to intrusion detection, hold-up and alarm devices shall be governed by a separate menu which is incorporated in the ACM's software applications package. The ACM's alarm monitoring database shall support, at a minimum, the number of points or zones described in the System Description Section.
   c. Operator access to various functions and operations related to the intrusion detection sub-system shall be password controlled.
   d. The ACM's software shall support an independent database, which is specifically designed to define the various attributes associated with the intrusion detection devices.
   e. All transactions related to intrusion detection devices shall be displayed at the operator
   f. Intrusion detection device alarm transactions shall cause activation of an audible sounder at the operator workstations until the alarm condition is acknowledged by the operator via keyboard entry. Similarly, reset of a previously acknowledged alarm condition shall require acknowledgement by the system operator.
   g. Alarm transactions shall be prioritized. A minimum of 8 levels of priority shall be assigned to each alarm point. Unacknowledged alarm messages shall be displayed in order of priority.
   h. Subsequent to acknowledgment by the operator, alarm messages shall be cleared from the workstation display.
   i. In addition to message displays at operator workstations, all intrusion detection transactions shall be printed on the associated workstation printer and stored in the system archive file.
   j. Upon reset or "return too normal" of an alarm condition, a corresponding message shall be displayed. Reset messages shall be continuously displayed until acknowledged by the operator.
   k. The ACM's alarm monitoring database shall provide for "breakthrough" alarm such that the operator is alerted to an alarm condition if not operating in the standard

display format.

l. The ACM's alarm monitoring database shall provide for transfer of alarm groups between "access" and "secure" modes.

m. The ACM's alarm monitoring database shall provide for transfer of monitor points or alarm groups between access and secure modes automatically via programmed time schedule or manually via keyboard command at operator workstation.

n. When in the access mode, intrusion device wiring shall continue to be monitored such that circuit failures and/or trouble condition messages shall be immediately displayed at the operator workstation and stored in the system historical record. Trouble messages shall indicate the specific origin of the trouble and the device with which the trouble is associated.

9. Alarm Graphics:

a. The ACM's software shall provide a graphical map software module for the display of graphic alarm maps using graphical objects and icon buttons.

b. The software shall provide for a minimum of three (3) graphic screens or floor plans alarm device. The alarm graphics shall operate automatically, such that the initiation an alarm shall cause the appropriate graphic screen with embedded icon objects description to appear without user intervention. Activation of the graphic alarm function shall be programmable on a point-by-point basis.

c. Alarm graphics shall be based on architectural background computer aided design files. These files shall be provided by the Owner in electronic media format and the Security Contractor shall be responsible to import and modify as needed to create alarm maps acceptable to the Owner.

d. The ACM's software shall allow the operator to draw, edit and copy color graphic bitmap or vector files using built-in module and to import files in industry standard TIFF, JPEG (.jpeg), Microsoft© PC Paintbrush, Microsoft© Windows bitmap (.bmp), Microsoft© Meta File (. wife), Auto Cad© Release 13 (.dwg) and universal (. def.) formats. Function shall be programmable on a point-by-point basis.

e. Alarm graphics shall be based on architectural background computer aided design files. These files shall be provided by the Owner in electronic media format and the Security Contractor shall be responsible to import and modify as needed to create alarm maps acceptable to the Owner. The ACM's software shall allow the operator to draw, edit and copy color graphic bitmap or vector files using built-in module and to import files in industry standard TIFF, JPEG (.jpeg), Microsoft© PC Paintbrush, Microsoft© Windows bitmap (.bmp), Microsoft© Meta File (. wife), Auto Cad© Release 13 (.dwg) and universal (. def.) formats.

10. Access Cards

a. There are two standardized proximity card formats in a standard 26 bit and a proprietary HID 35-bit format. Unless otherwise specified, all access control readers and systems must be capable of reading both formats.

b. Standard HID cards utilized are as follows;

c. a. ID badge type – HID Dupris II, plain white on both sides with sequential matching numbers.

d. b. Standard proxy card type – HID Proxy II, plain white front with sequential matching numbers.

e. 2. Standard HID readers utilized are as follows;

a. Standard applications Multiclass Contactless Reader RP40 Reader.

b. Parking applications –Multiclass Contactless Reader with Keypad RPK40 Reader

2.02 OPERATION OF SYSTEM

Disregard this Sheet
Refer to first Section 28 13 00 in
Spec Book for Access Control

A. It is the intent of this specification that any new equipment provided as specified herein and as detailed on the drawings be compatible with the existing security system.
   A. Equipment furnished under this specification shall be the standard product of a manufacturer who has been engaged in production of this type of equipment for at least ten (10) years, and has a fully equipped service organization within fifty (50) miles of the installation. Equipment descriptions are intended to indicate type and quality of design and material, as well as operating features required.

2.03 MANUFACTURERS
- A. ACAMS
  - a. Software house C-Cure 9000 Enterprise ISTAR PRO with power supply as required depending on readers provided.
  - b. Or approved equal
- B. Card Readers
  - a. Part# HID RP40 Multiclass proximity reader except at ambulance entry RPK40 proximity and keypad reader
  - b. Or approved equal
- C. Mag locks
  - a. Part# Alarm Controls AL-1200 or RCI-8310.
  - b. 1200 lb holding force
  - c. Or approved equal
- D. Door contacts
  - a. Part# Interlogix 1078C-M Recessed Steel Door Contact
  - b. # Interlogix 2202AU-L armored surface mount Door Contact
  - c. Or approved equal
- E. Request to exit sensor
  - a. Part# Bosch DS150I Request To Exit PIR Motion Sensor Passive Infrared Occupancy Wall or Ceiling, Light Gray
  - b. Or approved equal
- F. Push buttons
  - a. Part# TS14 Alarm Controls
  - b. Or approved equal
- G. Access Control Cable
  - a. Part# Windy City Wire #4461030 18/4, 22/6, 22/2, 22/4
  - b. Or approved equal

PART 3 - EXECUTION

3.01 INSTALLATION

A. Provide equipment and cable infrastructure where shown in accordance with manufacturer's written instructions, and with recognized industry practices to ensure that equipment complies with requirements and serves intended purpose.

B. The security contractor shall be responsible for coordination of extension of all commercial/emergency power circuits for connection to security equipment cabinets, power supply cabinets and all other security devices as required.

C. The security contractor shall coordinate his work with the work of all other trades. In the event of a conflict with equipment locations, the security contractor must verify with general contractor, architect and/or project manager.

D. Cabling:
   1. All vertical and horizontal security cable shall be provided by the security contractor, incidental security cable required for interconnection of security equipment racks and cabinets shall be provided by the security contractor.
   2. Cable routed within the security control center racks for interconnection of security equipment shall be responsibility of the security contractor.

Disregard this Sheet
Refer to first Section 28 13 00 in
Spec Book for Access Control

Security contractor submittals shall reflect all cable provisions and associated cable labels.

4. All low voltage cabling routed inside the buildings shall be plenum rated
5. All low voltage cabling routed outside the building and in parking garages shall be Outside Plant Grade Cable (OSP) unless otherwise noted on drawings.

E. The security contractor shall have the option to subcontract with the cable contractor to perform the required work. All employees and subcontractors of the security contractor working on the job site shall be required to obtain owner-required safety training. The security contractor shall insure employees and subcontractor meets employee identification requirements of the owner.

F. For system or component replacement projects, the Security Contractor shall have responsibility for removal of all unused and unusable security cabling and devices. No security devices or cabling shall be removed from the premises without the owner's permission.

G. Installation shall comply with the requirements of the National Electrical Code, local, city and state codes, and applicable portions of the NECA's "Standard of Installation."

H. All wall penetrations must be properly fire stopped in compliance with local, state and federal regulations.

I. Control equipment and other devices shall be mounted with sufficient clearance for observation and testing. All system junction boxes must be clearly marked for easy identification. All wiring shall be of sizes specified by the manufacturer, in accordance with the National Electrical Code. Mounting boxes, junction boxes and panels shall be securely hung and fastened with appropriate fittings to insure positive grounding throughout the system.

J. Wiring splices are to be avoided to the extent possible, and if needed, they must be made only in junction boxes or specified cross connect fields. Transposing or changing color-coding of wires shall not be permitted. All conductors in conduit containing more than one wire shall be labeled on each end with "E-Z Markers" or equivalent. Conductors in cabinets shall be carefully formed and harnessed so that each drops off directly opposite to its terminal.

3.02 TESTING

A. Upon completion of installation of the system and after connection to power source, test equipment to demonstrate compliance with requirements. When possible, field correct malfunctioning equipment and then retest to demonstrate compliance. Replace equipment, which cannot be satisfactorily corrected.

B. System shall be tested to the satisfaction of the Engineer, Owner and authorities having jurisdiction.

C. The system shall be capable of testing such that no replacement parts will be required to test the operation of the system.

D. The Contractor shall perform all tests required or recommended by the equipment manufacturer. All test and report costs shall be in the Contract Price. A checkout report shall be prepared by the technician and submitted in triplicate, to the Owner. The report shall include, but not be limited to:

1. A complete list of equipment installed and tested.
2. Indication that all equipment is properly installed and functions and conforms to these specifications.
3. Technicians name, certification number and date.
4. Acceptance of the system shall also require a demonstration of the stability of the system. This shall be adequately demonstrated if the system operates for a ninety (90) day period without any unwarranted malfunctions. This demonstration shall not start until the Owner has obtained beneficial use of the building under test.

E. Instruct Maintenance Personnel in complete operation, including actual staff use of system, by authorized distributor personnel. The instruction period shall not commence until the equipment has been made fully operational as determined by the Owner.

G. The Contractor shall make available to the Owner, a local manufacturer's service department which is to stock the manufacturer's standard parts. On-the-premises maintenance is to be

provided during normal working hours at no cost to the Owner for a period of twelve (12) months from the date of completion and acceptance of the installation.

END OF SECTION

Disregard this Sheet
Refer to first Section 28 13 00 in Spec Book for Access Control

Disregard this Sheet
Refer to first Section 28 13 00 in Spec Book for Video Surveillance

SECTION 28 23 00

VIDEO SURVEILLANCE

PART 1 GENERAL

1.01 SUMMARY

A. General: Provide engineering, labor, materials, apparatus, tools, equipment, transportation, temporary construction, and special or occasional services as required to make a complete working video surveillance system installation, as described in this specification.

B. The successful bidder will supply all software, hardware, wiring, and Servers.

C. Provide an Itemized pricing list of all components showing material and labor cost for each component.

D. Section Includes:
1. Network video recording system shall be Avigilon Servers
2. Network video management software shall be Avigilon Enterprise
3. Network video cameras shall be Avigilon.

E. Products Supplied But Not Installed Under This Section:
1. 120V power

F. Related Sections:
1. Consult other Divisions, determine the extent and character of related work and properly coordinate work specified herein with that specified elsewhere to produce a complete and operable system.
2. Section 280526 Grounding and Bonding for Electronic Safety and Security
3. Section 280528 Pathways for Electronic Safety and Security
4. Section 280544 Sleeves and seals for Electronic Safety and Security
5. Section 281300 Access Control

1.02 SYSTEM DESCRIPTION

A. Overview
1. This scope includes IP video surveillance cameras to monitor areas as shown on drawings. Cameras shall be supplied, installed and terminated as noted on drawings.
2. The VSS consist of host servers, storage devices, video management software, fixed network cameras, and integration with other subsystems.
3. The VSS software will utilize PoE network cameras within the interior and exterior spaces of the building.

Disregard this Sheet
Refer to first Section 28 13 00 in
Spec Book for Video Surveillance

B. Video Surveillance System
   1. Provide Avigilon Enterprise video management software and camera licenses to support the devices shown on the project drawings. (Enterprise Licenses for software are to be provided) Provide rack-mount NVR device in the Security Room to allow for 30 days of storage with 60% recording. (Four Post rack provided by others)
   2. **Security contractor to provide Access Control Integration License for CCure 9000.**
   3. Provide Network fixed cameras as shown on the project drawings.

1.03 SUBMITTALS

A. Contractor Qualifications: Submit certifications for the manufacturers of the video surveillance equipment.

B. Product Data: Submit product information for components specified herein.

C. Shop Drawings:
   1. Device placement on floor plans
   2. Point-to-Point Diagrams: Include wiring, points of connection and interconnecting devices between the following:
      a. Video surveillance system, storage and recording equipment
      b. Devices connected to the system
      c. Miscellaneous control relays
      d. Conductors (identify conductors on the point-to-point diagrams with the same tag as the installed conductor)
   3. Block Diagram/Riser Diagram: Show the video surveillance system components, conduit, wire types, and sizes between them, including cabling interties between termination hardware.
   4. Custom mounting details

1.04 WARRANTY
   1. Provide a manufacturer's warranty covering repair or replacement of defective parts for a period of three years from the date of shipment from the factory.

PART 2 PRODUCTS

2.01 NETWORK VIDEO RECORDER

A. General
   1. Complete software-based open platform that encompasses recording video, viewing video, reviewing video, and storing video for indefinite periods of time.
   2. Designed for a fully scalable network video recording solution.
   3. The system enables multiple video streams for live, record, alarm, and meta-data collection.

B. Features
   1. Support for MJPEG, MPEG-4, and H.264 video compression formats. ONVIF compliant.

Disregard this Sheet
Refer to first Section 28 13 00 in
Spec Book for Video Surveillance

2. Standards-based, open architecture software that is capable of running on non-proprietary hardware.
3. Supports desktop, web browser, and mobile web clients. Capable of pushing live video on-demand to and from any client.
4. Integrated virtual matrix switch for distributed video wall management.
5. Search Capabilities
   a. Motion detection time line
   b. Auto-generated time intervals with thumbnail image previews
   c. Object or zone based search
   d. Alarm or event via ACAMS or video analytics behaviors
   e. Supports an unlimited amount of configurable camera group views
6. Recording Configuration
   a. Advanced motion detection with configurable motion sensitivity, size, and speed
   b. User configurable archiving schedules and sequences that do not impact uptime
   c. Hardware and bandwidth utilization for monitoring and recording video and different frame rates and resolutions
   d. Multiple channel audio recording
7. Virtual Matrix Switch Configuration
   a. Supports graphical keypads, touch screen monitors, and dynamic mapping
   b. Supports an unlimited number of cameras, monitors, and operators
   c. Capable of pushing camera streams to any video wall monitor or remote display within the video management system
   d. Capable of creating custom groups on-demand
   e. Utilizes a one-touch or one-click selection from active maps to specific floor plans with detailed camera locations and viewing angles
   f. Integrates with video analytics, and ACAMS
   g. Enables real-time notification, reviewing, and acknowledgement of events and alarms
8. Network Configuration
   a. Capable of utilizing multiple networks and subnets
   b. Capable of utilizing user authentication via MS Windows User Account and Groups
   c. Capable of running as a MS Windows service
   d. Support for MS Active Directory
   e. Support for VMware and MS Virtual PC

C. Manufacturer
1. Avigilon
   a. Model HDNVR Part #HD-NVR-3PRM-48TB-NA or larger depending on bandwidth and camera settings. Minimum settings 10 FPS, Quality 6 and 45 days archived video at full framerate with 20% spare for future expansion. Provide and install Software House CCure 9000 software Integration Avigilon #ACC5-SWHS-CCURE
   b. Or approved Equal.

2.02 CAMERAS
1. Manufacturers

Disregard this Sheet
Refer to first Section 28 13 00 in
Spec Book for Video Surveillance

a. Avigilon 5MP (Exterior) Part #5.0-H3-DP1 with MNT-PEND-Wall mount or 5.0-H3-DO1 surface mount camera (under canopy's)
b. Avigilon 2MP (Interior) Part #2.0-H3-DC1 with IND-CEL-PNL ceiling support panel
c. Or Approved Equal.

2.03 POE SWICH

1. Provided by Owner

2.04 UPS

1. Manufacturers
   a. Minuteman E1000RT2U one for each server provided
   b. Or approved Equal.

2.05 CABLING.

A. CABLING TO BE INSTALLED BY DIVISION 27 CONTRACTOR

PART 3 EXECUTION

3.01 INSTALLATION

A. Network Video Recorder
   1. Program record rate for network cameras at 10 IPS at full resolution (2596x1944) using H.264 compression format.
   2. Coordinate with Owner's IT and Security representatives to set the following criteria:
      a. Administrator and operator passwords
      b. Camera and video device naming conventions
      c. Maximum bit rate
      d. Bandwidth throttle
      e. Camera groups and operator views
      f. Mapping features and criteria for a fully interactive graphical display of each floor plan
      g. Alarm events and integration into ACAMS

B. Interior Network Cameras
   1. Provide flush ceiling mount for fixed network cameras within ceiling space. Install camera body above ceiling line when camera located in ceiling so only dome exposed.
   2. Provide surface mount ring and electrical back box adapter plate for fixed network cameras in stairwells or other wall mounted locations.
   3. Field determine exact placement of cameras to ensure complete coverage.
   4. Adjust the wide dynamic range, gain control, and noise reduction settings on each camera as required to provide clear and crisp video images.

C. Exterior Network Cameras
   1. Provide outdoor housing and mounts for exterior cameras.
   2. Field determine exact placement of cameras to ensure complete coverage.

Disregard this Sheet
Refer to first Section 28 13 00 in
Spec Book for Video Surveillance

3. Coordinate a meeting with Owner's IT and Security representatives and Division 26 contractor to walk site and confirm actual mounting locations for each CCTV camera prior to installation.

D. Field determine fixed camera lens size and settings to ensure complete coverage.

3.02 TESTING

A. Commission the video surveillance system in accordance with owner acceptance.

END OF SECTION