SECTION 28 05 00 - COMMON WORK RESULTS FOR ELECTRONIC SAFETY AND SECURITY

PART 1 - GENERAL

1.1 SUMMARY

A. Section Includes:

1. Basic requirements for providing additions to the Access Control and Alarm Management System (ACAMS) and Security Surveillance System as specified and shown on the Contract Drawings.

B. Related Documents:

1. Drawings and general provisions of the Contract apply to this Section.

1.2 REFERENCES

A. Abbreviations and Acronyms:

1. ACAMS: Access control and alarm management system.
2. ACU: Access control unit.
3. API: Application programming interface.
4. AWG: American Wire Gauge.
5. B/W: Black and white.
6. CBR: Constant bit rate.
7. CCTV: Closed circuit television.
8. CMOS: Complementary metal–oxide–semiconductor.
9. DC: Direct electrical current.
10. DMS: Device monitoring system.
11. DPDT: Double pole double throw.
12. ESS: Electronic security system.
13. FO: Fiber optic.
14. FTP: File transfer protocol.
15. I/O: Inputs and outputs.
16. IC: Interchangeable.
17. IDF: Intermediate Distribution Frame.
18. IP: Internet protocol.
19. ITE: Information technology equipment.
20. JPEG: An acronym for the Joint Photographic Experts Group which created a commonly used method of lossy compression for photographic images having the same acronym, and defined in ISO/IEC 10918 1, ISO/IEC 10918 2, ISO/IEC 10918 3, ISO/IEC 10918 4, and ISO/IEC FCD 10918 5; ITU T T.81, ITU T T.83, ITU T T.84, and ITU T T.86.
21. LAN: Local area network.
22. MDF: Main Distribution Frame.
23. MIRO: Monitor inputs and relay outputs.

24. MJPEG: Motion JPEG, an informal name for a class of video formats where each video frame or interlaced field of a digital video sequence is separately compressed as a JPEG image.
25. MOP: Maintenance of Operations Plan.
26. NTP: Notice to proceed.
27. NTSC: Named for the National Television System Committee, the analog television system used in most of North America, South America, Burma, South Korea, Taiwan, Japan, the Philippines, and some Pacific island nations and territories.
28. O&M: Operation and maintenance.
29. PIN: Personal identification number.
30. PoE: Power over Ethernet.
31. RAM: Random access memory.
32. REX: Request-to-exit.
33. RS422: EIA RS422 communication interface standard.
34. RS485: EIA RS485 communication interface standard.
35. SD/SDHC: Secure digital/high-capacity secure digital.
36. SPDT: Single pole double throw.
37. SPIFF: Still picture interchange file format.
38. SSI: Sensitive security information.
39. TCP: Transmission control protocol.
40. TGB: Telecommunications grounding busbar.
41. TMGB: Telecommunications main grounding busbar.
42. VBR: Variable bit rate.
43. VMS: Video management system.
44. WIRO: Wiegand interface and relay outputs.

B. Definitions:

1. Arming a Detector or Disarming a Detector:
   a. When a detector is “armed”, triggering an alarm point in the electronic security system (ESS) will cause the system to time-stamp and record the event in the database, print out the event at the event logging printer, list the event in the alarm historical page, update and emphasize the status in related animated display pages using a blinking attribute, and activate the related audio/visual annunciation device or devices.
   b. When a detector is “disarmed”, triggering an alarm point in the electronic security system (ESS) will cause the system to only time-stamp and record the event in the database, and update the related status in the related animated display pages without the blinking attribute.
2. Authority Having Jurisdiction (AHJ): Building Code officials, zoning officials, inspectors, and government and regulatory agencies given the authority to protect the public’s health, safety, and welfare.
3. Credential Database: The database in which the list of identifiers and related data is stored.
4. Duress Alarm: An alarm condition which results from a set of pre-established conditions such as entering a special code into a keypad or activating a switch.

a. This alarm category takes precedence over other alarm categories.

5. Enclosure: Control panel, console, cabinet, or instrument housing.

6. Entry Control Alarm: An alarm resulting from improper use of entry control procedures or equipment.

7. Entry Control Devices: Any equipment which gives a user the means to input identifier data into the entry control system for verification.

8. Environmental Alarm: An alarm during environmental conditions which exceed those specified for system operation.

9. Ethernet: A family of frame-based computer networking technologies for local area networks (LANs).

10. Exit Device: A mechanical assembly of door lock hardware installed at the internal side of the building or room.

    a. An exit device is intended to operate the door lock mechanism and thereby allow the door to be opened.

11. Facility Interface Device: A type of mechanism which is controlled in response to passage requests, and that allows passage through a portal.

12. Fail-Safe Alarm: An alarm resulting from detection of diminished functional capabilities.

13. False Alarm: An alarm when there is no alarm stimulus.

14. Guard Tour Alarm: An alarm resulting from a guard being either early or late at a specified check-in location.

15. H.264/MPEG 4 AVC: A block oriented motion compensation based codec standard for video compression as specified in ITU T H.264, ISO/IEC 14496 10, and ISO/IEC 23002 4.

16. Identifier: A card credential, keypad personal identification number or code, biometric characteristic, or any other unique identification entered as data into the entry control database for the purpose of identifying an individual.

    a. Identifiers are used by the electronic security system for the purpose of validating passage requests for areas equipped with entry control equipment.

17. Intrusion Alarm: An alarm resulting from the detection of a specified target, caused by an attempt to intrude into the protected area, or caused when entry into an entry controlled area is attempted without successfully using entry control procedures.

18. Nationally Recognized Testing Laboratory (NRTL): An organization which is recognized by the Occupational Safety and Health Administration (OSHA), and which tests for safety, and lists or labels or accepts, equipment or materials which meet the criteria specified in 29 CFR 1910.7, Definition and Requirements for a Nationally Recognized Testing Laboratory.

19. Nuisance Alarm: An alarm resulting from the detection of an appropriate alarm stimulus, but which does not represent an attempt to intrude into the protected area.

20. Passage: Ingress and/or egress past an entry control device, or through a portal.

21. Power Loss Alarm: An alarm resulting from a loss of primary power.

22. RS422: A Telecommunications Industry Association (TIA) recommended standard for the interchange of serial binary signals between data terminal equipment (DTE) and data circuit-terminating equipment (DCE) or in any point-to-point interconnection of serial binary signals between digital equipment as specified in ANSI/TIA 422 B.

23. RS485: A Telecommunications Industry Association (TIA) recommended standard for multipoint communications using two twisted-pairs.

24. Secured Side: The side of a controlled door or gate on which the door hardware is operable either

without the need of a key, or when enabled by related access controller.

25. Standard Intruder: The standard intruder is a person weighing 70 pounds or more, is 40 inches tall or more, and unless environmental conditions at the Site require protective clothing, is dressed in a long-sleeved shirt, slacks, and shoes.

26. Standard Intruder Movement: Any movement such as walking, running, crawling, rolling, or jumping through a protected zone in the most advantageous manner for the intruder.

27. System Heavy-Load Conditions: The occurrence of alarms at the rate of 10 alarms per second distributed evenly among all entry-control local processors in the system.

    a. For the purpose of system heavy-load definition, the system is considered to consist of electronic security system (ESS) server computer equipment, system network, and required entry-control local processors.

C. Codes and Standards:

1. American National Standards Institute (ANSI):
    a. ANSI/J-STD-607-A – Commercial Building Grounding (Earthing) and Bonding Requirements for Telecommunications.
2. American Society for Testing and Materials (ASTM):
    a. ASTM F2200 – Standard Specification for Automated Vehicular Gate Construction.
3. Building Industry Consulting Services International (BICSI):
    a. BICSI TDMM - Telecommunications Distribution Methods Manual.
    b. BICSI OSPDM – Outside Plant Design Manual.
4. Industry Canada (ICES):
    a. ICES 003 – Digital Apparatus.
5. Institute of Electrical and Electronics Engineers (IEEE):
    a. IEEE 802.3AF – Part 3: CSMA/CD Access Method and PHY Specifications – Data Terminal Equipment (DTE) Power ‘Via Media Dependent Interface (MDI).
6. International Code Council (ICC):
    a. ICC International Building Code (IBC) as Amended by the Authority Having Jurisdiction (AHJ).
7. International Committee for Information Technology Standards (INCITS):
    a. ANSI/INCITS 231 – Information Systems – Fibre Distributed Data Interface (FDDI) – Physical Layer Protocol (PHY-2).
8. International Standards Organization/International Electrotechnical Commission (ISO/IEC):
    a. ISO/IEC 10918 1 - Information Technology – Digital Compression and Coding of Continuous-Tone Still Images: Requirements and Guidelines.
    b. ISO/IEC 10918 2 - Information Technology – Digital Compression and Coding of Continuous-Tone Still Images: Compliance Testing.
    c. ISO/IEC 10918 3 - Information Technology – Digital Compression and Coding of Continuous-Tone Still Images: Extensions.
    d. ISO/IEC 10918 4 - Information Technology – Digital Compression and Coding of Continuous-Tone Still Images: Registration of JPEG Profiles, SPIFF Profiles, SPIFF Colour Spaces, APPn Markers, SPIFF Compression Types and Registration Authorities (REGAUT).
    e. ISO/IEC FCD 10918 5 - Information Technology – Digital Compression and Coding of

Continuous-Tone Still Images: JPEG File Interchange Format.

f. ISO/IEC 11801 – Information Technology – Generic Cabling for Customer Premises.

g. ISO/IEC 14496 10 - Information Technology – Coding of Audio-Visual Objects – Part 10: Advanced Video Coding.

h. ISO/IEC 23002 4 - Information Technology – MPEG Video Technologies – Part 4: Video Tool Library.

i. IEC 60529 - Degrees of protection provided by enclosures (IP Code).

j. IEC 62262 - Degrees of protection provided by enclosures for electrical equipment against external mechanical impacts (IK code).

9. International Telecommunication Union (ITU):

a. The International Telegraph and Telephone Consultative Committee:

1) CCITT G.726 - General Aspects of Digital Transmission Systems; Terminal Equipments 40, 32, 24, 16 kbit/s Adaptive Differential Pulse Code Modulation (ADPCM).

b. Telecommunication Standardization Sector of ITU:

1) ITU T G.711 – General Aspects of Digital Transmission Systems Terminal Equipments Pulse Code Modulation (PCM) of Voice Frequencies.

2) ITU T H.264 - Series H: Audiovisual and Multimedia Systems Infrastructure of Audiovisual Services – Coding of Moving Video Advanced Video Coding for Generic Audiovisual Services.

3) ITU T T.81 - Digital Compression and Coding of Continuous-Tone Still Images: Requirements and Guidelines.

4) ITU T T.83 - Digital Compression and Coding of Continuous-Tone Still Images: Compliance Testing.

5) ITU T T.84 - Information Technology – Digital Compression and Coding of Continuous-Tone Still Images: Extensions.

6) ITU T T.86 - Information technology – Digital Compression and Coding of Continuous-Tone Still Images: Registration of JPEG Profiles, SPIFF Profiles, SPIFF Tags, SPIFF Colour Spaces, APPn Markers, SPIFF Compression Types and Registration Authorities (REGAUT).

10. National Fire Protection Association (NFPA):

a. NFPA 70 - National Electrical Code (NEC).

11. Society of Motion Picture and Television Engineers (SMPTE):

a. SMPTE 274M - Television - 1920 x 1080 Image Sample Structure, Digital Representation and Digital Timing Reference Sequences for Multiple Picture Rates.

b. SMPTE 296M - Television - 1280 X 720 Progressive Image Sample Structure – Analog and Digital Representation and Analog Interface.

12. Telecommunications Industry Association/Electronic Industries Association (TIA/EIA):

a. ANSI/TIA 422 B – Electrical Characteristics of Balanced Voltage Digital Interface Circuits.

b. ANSI/TIA/EIA-568-B.1 - Commercial Building Telecommunications Cabling Standard – Part 1: General Requirements.

c. ANSI/TIA/EIA-568-B.2 - Commercial Building Telecommunications Cabling Standard – Part 2: Balanced Twisted Pair Cabling Components.

d. ANSI/TIA/EIA-568-B.3 – Optical Fiber Cabling Components Standard.

e. ANSI/TIA/EIA-606-A – Administration Standard for Commercial Telecommunications Infrastructure.

f. ANSI/TIA/EIA-758-A – Customer Owned Outside Plant Telecommunications Infrastructure Standard.

g. ANSI/TIA J STD 607 - Commercial Building Grounding and Bonding Requirements for Telecommunications.

13. Telecommunications Industry Association (TIA):

a. TIA-569-B – Commercial Building Standard for Telecommunications Pathways.

b. TSB-140 – Additional Guidelines for Field Test Length, Loss and Polarity of Optical Fibers.

14. Underwriters Laboratories, Inc. (UL):

a. UL 294 – Standard for Access Control System Units.

b. UL 325 Standard for Door, Drapery, Gate, Louver, and Window Operators and Systems

c. UL Online Certifications Directory, http://www.ul.com/regulators/quickguide.html.

d. UL Performance Verification Service Requirements.

e. UL Qualification Tests and Follow-Up Service Requirements.

15. United States Government:

a. Federal Communications Commission (FCC):

1) 47 CFR 15 Radio Frequency Devices.

b. Occupational Safety and Health Administration (OSHA):

1) 29 CFR 1910 Occupational Health and Safety Standards.

2) 29 CFR 1926 Safety and Health Regulations for Construction.

c. Office of the Secretary of Transportation:

1) 49 CFR 15 Protection of Sensitive Security Information.

d. Transportation Security Administration, Department of Homeland Security:

1) 49 CFR 1520 Protection of Sensitive Security Information.

e. United States Code (U.S.C.):

1) 5 U.S.C 552 Public Information, Agency Rules, Opinions, Orders, Records, and Proceedings.

2) The Freedom of Information Act.

3) Protected National Security Documents Act of 2009.

4) Voluntary Control Council for Interference by Information Technology Equipment (VCCI):

a) VCCI Council Rules.

1.3 ADMINISTRATIVE REQUIREMENTS

A. Coordination:

1. Coordinate all electronic safety and security work with the Program/Project Manager and the approved Contract schedule.

a. Adhere to the approved installation schedule.

b. Give required notices for items affecting the Contract schedule.

2. Coordinate delivery of extra materials, spare parts, and maintenance materials to the Site with the Program/Project Manager and obtain receipts for these materials prior to requesting final payment.

3. Coordinate acquisition of dedicated communications bandwidth and system storage devices with the Owner as necessary.

4. Coordinate creating an integrated, secure security environment for electronic security system (ESS) communications with the Owner.

5. Existing Security System Equipment Suppliers:

a. Coordinate with the Suppliers of the existing security system to ensure that the new security access and surveillance equipment is compatible and functions with the existing system.

6. Electrical and Communications Subcontractors:

a. Coordinate interconnection of the Electronics Safety and Security Systems equipment and electrical equipment with the electrical Subcontractor.

b. Coordinate interconnection of the Electronics Safety and Security Systems equipment and the communications infrastructure equipment and network equipment with the communications Subcontractor.

7. Provide the final coordination and field routing required for completing the Electronics Safety and Security Systems as indicated in the Contract Documents.

B. Pre-Installation Meetings:

1. Contract Planning Meeting:

a. The Contractor’s project manager and key staff must participate in a Contract Planning Meeting, as required by the Program/Project Manager.

1) The purpose of the Contract Planning Meeting is to ensure proper coordination between the parties responsible for the successful completion of the Work of this Contract.

2. Contract Status Meetings:

a. The Contractor’s project manager must attend weekly and monthly Contract status meetings with the Program/Project Manager to discuss the status of the installation of the Electronics Safety and Security Systems.

C. Scheduling:

1. In the construction schedule, designate system startup periods in conjunction with the initial system performance testing for the Electronics Safety and Security Systems.

a. For time dependent testing, include a commissioning period having a minimum duration of 30 days in the construction schedule.

1.4 QUALITY ASSURANCE.

A. Regulatory Agency Approvals:

1. Submit the documents required by State Licensure inspectors and other Authorities Having Jurisdiction to the appropriate agencies.

a. Secure and pay for plan check fees, permits, fees, and licenses necessary for the execution of the Electronics Safety and Security Systems Work as applicable for this Contract.

b. Submit the approval documents from the regulatory agencies to the Program/Project Manager for information.

B. Contractor’s Qualifications for the Electronics Safety and Security Systems:

1. Firms regularly engaged in the installation of Electronics Safety and Security Systems and that have five (5) years of installation experience with systems similar to that required for this project.

2. Provide references to include client names, phone numbers and a summary of project details. These references will be checked, and the clients will be asked questions relative to the performance of your company.

3. Provide verification that installation personnel responsible have been properly trained to install the products required for this project.

4. Provide full time project manager with a minimum of five (5) years field experience in installation of Electronics Safety and Security Systems. Project manager shall be assigned for the duration of the project and shall not be replaced without written consent from the Owner.

5. Submit the Electronics Safety and Security Systems service contractor’s qualifications to the Program/Project Manager for approval.

C. Certifications:

1. Electrical Listing and Labeling:

a. Provide electrical components, devices, and accessories that are listed and labeled for the location the product is installed in, and the application intended, by a Nationally Recognized Testing Laboratory (NRTL), as defined in Article 100 of NFPA 70, acceptable to the Authorities Having Jurisdiction (AHJ), such as Underwriters Laboratories, Inc. (UL), unless products meeting the requirements of these nationally recognized testing laboratories are not available or unless standards do not exist for the products.

1) Provide products marked with their intended use or classification.

2) Submit evidence with the Product Data that the products represented meet testing agency quality verification requirements, including agency listing and labeling requirements.

3) Such evidence may consist of either a printed mark on the data or a separate listing card.

b. Submit a written statement from those product manufacturers that do not provide evidence of the quality of their products that indicates why an item does not have quality assurance verification.

1) Such statements provided in lieu of quality assurance verification are subject to the acceptance of the Owner and the Program/Project Manager.

1.5 SUBMITTALS

A. Action Submittals:

1. Submit the following to the Program/Project Manager for approval:

a. Product Data:

1) Prepare a Bill of Materials for Electronics Safety and Security systems which will then function as the Table of Contents for the security surveillance system hardware Product Data submittal.

2) Obtain Product Data for the products proposed, consisting of, but not limited to, data sheets and catalog cuts which document compliance of the devices and components with the requirements specified in this Section.

3) Any exceptions taken to the specified requirements must be noted and addressed.

4) Submit product data sheets for approval prior to procurement of equipment and software.

5) On the product data sheet, clearly identify what model and part numbers are being proposed and which ones are not.

6) On the product data sheet, clearly identify what optional equipment or functions are being proposed and which ones are not.

7) Furnish a description of any modification or custom design required to meet the Contract requirements that are not covered by the standard software.

8) Include each device's unique identifier, the device function, its manufacturer, and its model/part/catalog number used for ordering.

9) System Schematics:

a) Furnish system schematics that shows the control and mechanical devices associated with the system.

b) Include a system schematic drawing for each sub-system.

10) Communication-System Architectures:

a) Furnish complete communication system architectures.

11) System Drawing Index:

a) Furnish a system drawing index that shows the name and number of the building or other similar designation; and that lists the system drawings, including the drawing number, sheet number, drawing title, and computer filename when used.

b) Furnish a system legend on the system drawings that shows generic symbols and the name of the devices shown.

2. Within the 2 months after the official Notice to Proceed (NTP), submit the Electronics Safety and Security Systems Shop Drawings to the Program/Project Manager for approval.

a. Shop Drawings:

1) System Drawing Index:

a) At the beginning of the shop drawing submittal provide a table of contents or index that clearly identifies the names of the drawings included and page numbers for each of the drawings.

b) Use the same abbreviations, symbols, nomenclature and identifiers used in the Contract Documents.

2) Furnish each system element shown on a system drawing with a unique identifier.

3) Submit system documents that include all or part of the following as applicable:

a) Include system descriptions, analyses, and calculations that were used to size the equipment specified.

4) Submit marked up construction drawings showing any deviations.

5) Include more detail, when compared to the project plans and typical details, system configuration information related to each installation.

6) Include coordination details required for between trades.

7) Include conduit pathways, mounting details, space requirements, naming and addressing suggestions.

8) Submit system schematics identifying how each component is interconnected.

B. Delegated and Deferred Design Submittals:

1. Related structural supports, poles, and foundations proposed.

2. Fire alarm system.

3. Other types of related deferred submittals required.

C. Special Procedure Submittals:

1. System Test Plans.

2. Sequence of Operation Narratives:

a. Furnish a sequence of operations that reflects the language and format of this Section, and that refers to the devices by their unique identifiers.

1) A description of how the system will operate.

2) A description of any integrations to other systems and how they are interconnected and are programmed to interact.

D. Qualification Statements:

1. Submit the following:

a. Electronics Safety and Security Systems installers' qualifications.

E. Informational Submittals:

1. Submit the following to the Program/Project Manager for information:

a. Manufacturer's Instructions:

1) Installation manuals.

2) User manuals

3) Recommended installation procedures and materials.

b. Site Quality Control Submittals.

F. Closeout Submittals:

1. Submit the following to the Program/Project Manager:

a. Maintenance Contracts:

1) Proposal for new service contracts if requested.

2) Proposal for modifying existing service contracts if requested.

b. Warranty Documentation:

1) Electronics Safety and Security Systems Equipment Materials Warranty.

2) Electronics Safety and Security Systems Installation Warranty.

c. Record Documentation:

1) System Commissioning Report.

2) Record Drawings showing As-Built conditions with all Shop Drawing development and installation development notated.

3) Electronics Safety and Security Systems proof of licensing.

4) Electronics Safety and Security Systems Inspection and Functional Test Reports.

5) Electronics Safety and Security Systems User Acceptance Test Reports.

6) Electronics Safety and Security Systems Configuration files.

a) Immediately following the completion of user acceptance testing, submit electronic copies of all configuration files such that the system can be restored to the accepted state.

d. SPARE PARTS DELIVERY

1) Provide transmittal of spare parts delivery.

1.6 SITE CONDITIONS

A. Existing Conditions:

1. All existing underground and aboveground utilities, services, and improvements, if any, are indicated in the Contract Documents to the best of the Owner's and Designer's knowledge and belief; however, the Owner and Designer has not verified this information by on-site verification of available as-built documentation, and the Contractor shall notify the Program/Project Manager of discrepancies discovered in the information provided in accordance with the notification and change procedures of the Contract.

B. Maintenance of Operations Plan (MOP):

1. Work shall include preparation of a Maintenance of Operations Plan (MOP) to keep the existing Electronics Safety and Security Systems functioning during construction.

2. Prepare and submit for approval a Maintenance of Operations Plan (MOP) for Electronics Safety and Security Systems. Each MOP shall provide sufficient detail on the required sequencing to ensure the continuous operation of the existing system. The Contractor is hereby advised that the long term shut downs, per the discretion of the Owner, of the existing Electronics Safety and Security Systems will not be permitted.

3. The MOP at the minimum include the following:

a. Timing and method for each tie-in that may impact the operation of the existing system.

b. Method of keeping existing system functioning prior to disrupting the existing system. This may include temporary tie-ins, and temporary connections to back-up system operations.

c. Detailed schedule for overall installation, including the preparation of a construction sequencing plan. The schedule for the construction work shall align with the sequencing plans or a revised sequencing plan approved by the Program/Project Manager.

d. Timing and method of temporary improvements necessary for maintaining continuous system operations. Detail shall be provided as to the temporary materials/connections used.

C. Working Hours:

1. The Contractor shall work outside the normal working hours, as directed by the Program/Project Manager, to minimize impact to the operations as well as accidental disruptions to the existing Electronics Safety and Security Systems.

1.7 DELIVERY, STORAGE, AND HANDLING

A. Delivery and Acceptance Requirements:

1. Package each item of the Electronics Safety and Security Systems equipment in its original and individual container, complete with all necessary fastenings, instructions, and templates.

2. Check in and sign for all the Electronics Safety and Security Systems equipment delivered to the Site and take responsibility for the material delivered thereafter until Final Acceptance.

3. Deliver materials and equipment in a clean condition.

a. Provide packaging that plugs, caps, or otherwise seals openings both during shipping and temporary storage.

4. Inspect materials and equipment for signs of damage prior to accepting delivery of those items at the Site; and reject, segregate, and remove damaged items.

B. Storage and Handling Requirements:

1. Handle materials and equipment in accordance with the manufacturer's written instructions.

2. Follow the manufacturer's written instructions for storing the items.

3. Store all products whether on-site or off-site, indoors on blocking or pallets.

a. Provide a room with sufficient space and shelving in which to arrange, securely lockup, and store the Electronics Safety and Security Systems equipment.

b. Store the Electronics Safety and Security Systems equipment and products under cover in air conditioned warehouses or enclosed buildings that provide protection from the weather on all sides.

C. Packaging Waste Management:

1. Dispose of packaging waste.

1.8 WARRANTY

A. These warranty requirements represent the minimum requirements for the Electronics Safety and Security Systems. If other sections of the contract documents have additional warranty requirements, then they both shall apply, and the more stringent warranty requirement shall be provided.

B. Manufacturer Warranty:

1. Materials Warranty for the Access Control and Alarm Monitoring System (ACAMS):

a. Warrant the ACAMS equipment materials against defects within the 1 year period after the Date of Substantial Completion:

1) Submit, to the Program/Project Manager for approval, Equipment Materials Warranty on the ACAMS equipment Subcontractor’s standard or customized form, without monetary limitation, in which the ACAMS equipment Subcontractor agrees to replace equipment materials that fail within the specified warranty period.

2. Materials Warranty for the Security Surveillance System:

a. Warrant the Security Surveillance System equipment materials against defects within the 1 year period after the Date of Substantial Completion:

1) Submit, to the Program/Project Manager for approval, Equipment Materials Warranty on the Security Surveillance System equipment Subcontractor’s standard or customized form, without monetary limitation, in which the Security Surveillance System equipment Subcontractor agrees to replace equipment materials that fail within the specified warranty period.

C. Special Warranty:

1. Installation Warranty for the Access Control and Alarm Monitoring System (ACAMS):

a. Warrant the ACAMS installation workmanship against failures beginning at the Date of Substantial Completion and extending until 1 year after the Owner has conducted a systems acceptance test on all components and provided the Contractor with a Systems Acceptance approval letter:

1) Include the removal and reinstallation of the ACAMS in the Warranty.

2) Submit, to the Program/Project Manager for approval, a ACAMS Installation Warranty on ACAMS Subcontractor’s standard or customized form, without monetary limitation, in which installer agrees to repair ACAMS that fail within the specified warranty period.

2. Installation Warranty for the Security Surveillance System:

a. Warrant the Security Surveillance System installation workmanship against failures beginning at the Date of Substantial Completion and extending until 1 year after the Owner has conducted a systems acceptance test on all components and provided the Contractor with a Systems Acceptance approval letter:

1) Include the removal and reinstallation of the Security Surveillance System in the Warranty.

2) Submit, to the Program/Project Manager for approval, a Security Surveillance System Installation Warranty on Security Surveillance System Subcontractor's standard or customized form, without monetary limitation, in which installer agrees to repair ACAMS that fail within the specified warranty period.

PART 2 - PRODUCTS

2.1 MANUFACTURERS:

A. Manufacturer List:

1. Subject to compliance with the requirements specified herein, provide the Basis-of-Design product indicated in the Contract Documents or a comparable product.

B. Substitution Limitations:

1. No substitutions are allowed for the Electronic Security Safety and Security System components.

2.2 REGULATORY REQUIREMENTS:

A. Sensitive Security Information (SSI):

1. This document and all related documents stemming from it are considered Sensitive Security Information (SSI) that is controlled under the provisions specified in 49 CFR 15 and 49 CFR 1520.

a. No part of this document, related documents, or record may be disclosed to persons without a "need to know," as defined in 49 CFR 15 and 49 CFR 1520, except with the written permission of the Program/Project Manager or Federal Authorities.

b. Unauthorized release may result in civil penalties or other action.

c. For United States Government agencies, public disclosure is governed by 5 U.S.C § 552 and 49 CFR 15 and 49 CFR 1520.

2. It is the Contractor's responsibility to follow the Sensitive Security Information (SSI) protocol, and to control and account for all documents stemming from this Contract.

2.3 PERFORMANCE:

A. Install Electronics Safety and Security Systems so that it operates in accordance with its manufacturer's standards and Owner requirements.

2.4 MATERIALS AND EQUIPMENT:

A. All materials and equipment used in carrying out these specifications are to be new and have UL listing, or listing by other recognized testing laboratory when such listings are available.

B. Model numbers and manufacturers included on the project drawings are listed to establish as standard of product quality.

C. Other qualified manufacturers may be substituted only with the Owner's written consent. To request a substitution, the Contractor shall submit complete technical data, samples, and if requested, results of independent testing laboratory tests of proposed equipment.

1. If proposed System includes equipment other than specified model numbers, submit a list of major items and their quantities, with a one-line schematic diagram for review.

2. Material not specifically identified within this document, but which is required for the successful implementation of the intended system(s) shall be of the same class and quality as the specified material and equipment.

3. Include a list of previously installed projects using proposed equipment that are similar in nature to specified system.

PART 3 - EXECUTION

3.1 EXAMINATION

A. Verification of Conditions:

1. Although the Contract Drawings are generally indicative of the Work, take field measurements to verify actual conditions.

2. Verify that the installed conduit and wire quantities, sizes, and types are suitable for the Electronics Safety and Security Systems equipment being provided under this Contract.

   a. Verify that conduit stub-ups to be mated with the Electronics Safety and Security Systems equipment are the correct type and size, and are at the proper location.

   b. Inspect the condition of the existing conduit that is required for the Work.

B. Evaluation and Assessment:

1. Proceed installing the Electronics Safety and Security Systems only after unsatisfactory conditions have been corrected.

3.2 PREPARATION

A. Protection of In-Place Conditions:

1. Protect adjacent areas from damage resulting from installation of the Electronics Safety and Security Systems equipment.

B. Demolition / Removal:

1. Perform cutting and patching, if required.

3.3 CONTINUITY OF SERVICE

A. Follow the approved Maintenance of Operations Plan (MOP) for the Access Control and Alarm Monitoring System (ACAMS) and for the Security Surveillance System.

B. The Contractor shall not take any action that will interfere with, or interrupt, existing airport services unless previous arrangements have been made with the Owner’s Representative. Arrange the Work to minimize shutdown time.

C. Owner’s personnel will perform shutdown of operating systems. The Owner requires the Contractor submit a request at least fourteen (14) days prior to any system shutdown, and all requests must go through the Owner’s approval process.

D. Should services be inadvertently interrupted, Contractor shall immediately furnish labor, including overtime, material, and equipment necessary for prompt restoration of interrupted service.

3.4 INSTALLATION

A. Conduit:

1. Install the Electronics Safety and Security Systems wiring in a dedicated metal raceway system.

   a. For installing wire aboveground, provide only electrical metallic tubing (EMT) raceway having a diameter of at least 3/4 inch.

1) Free air wiring or exposed wiring is unacceptable.

b. For installing wire underground, provide polyvinyl chloride (PVC) conduit having a diameter of at least 1 inch that is buried at code specified depths.

c. For installing wire that will be subjected to physical damage, provide intermediate metallic conduit (IMC).

d. Providing plenum rated cable in lieu of the raceway system is unacceptable.

2. Conduit Color:

a. Provide only green conduit for the Electronics Safety and Security Systems.

b. If the conduit is not green in color, an acceptable substitute is to provide green conduit fittings and green junction box covers.

3. In conduit runs between pull points, do not allow the total angle of bends to exceed 180 degrees.

4. Support conduits in accordance with code requirements, and properly seal penetrations.

a. At penetrations through fire rated floors, walls, and similar assemblies, provide approved firestopping.

b. Seal conduit penetrations through floor slabs on grade in buildings with a floor penetration seal.

c. Install a wall penetration seal at all wall penetrations.

1) Size wall penetrations to accommodate the conduit outside diameter plus either 1/4 inch or a hole allowance to allow the installation of the wall penetration seal.

B. Fittings:

1. Provide compression type fittings only.

C. Special Techniques:

1. Communications Grounding:

a. Ground the communications equipment in accordance with the requirements specified in ANSI/TIA J STD 607.

1) Isolated telecommunications main grounding busbars (TMGB) have been installed by others in the power panels located in each communications Main Distribution Frame (MDF) and Intermediate Distribution Frame (IDF) room.

2. The raceway connections and associated grounding within the room will be provided by others.

a. Provide ground connections to field cabinets and panels using grounding conductors, but do not attach more 3 cabinets/panels on 1 wire segment connected in series.

1) Neatly dress the grounding conductors together within the power trays from the cabinets to the telecommunications main grounding busbar (TMGB) using no crosses grounding conductors.

2) Provide grounding connectors for attaching the grounding conductors to the rear of the cabinets where directed by the Program/Project Manager.

3) Tightly crimp and secure the grounding lugs at the telecommunications main grounding busbar (TMGB) or telecommunications grounding busbar (TGB).

3.5 CLEANING

A. Perform cleaning on a daily basis.

1. Contractor shall provide a clean work environment, free from trash/rubbish accumulated during and after daily installations.

2. When work area is adjacent to or writing Aviation or Tenant occupied space, leave the work area in a broom clean or equivalent condition.

B. Clean and protect construction in progress and adjoining materials in place during handling and installation.

C. After completing system installation, including outlet fittings and devices, inspect exposed finish. Remove burrs, dirt, dust, and construction debris and repair damaged finish, including chips, scratches, and abrasions. This includes touching up paint removed for grounding.

D. Contractor shall keep all liquids (drinks, Sodas, etc.) off finished floors, carpets, tiles, racks and equipment. If any liquid damage to above finishes or equipment, Contractor shall provide professional services to clean or repair scratched/soiled finishes or damaged equipment at own expense.

3.6 SYSTEM STARTUP

A. System Performance Verification and User Acceptance Tests:

1. Submit, to the Program/Project Manager for approval, proposed testing plan (procedures and test forms) for the System Performance Verification and User Acceptance Tests. Perform the System Performance Verification and User Acceptance Tests per the approved testing plan.

2. If the system does not pass the Performance Verification and Acceptance Tests due to deficiencies, continue the commissioning period until the Performance Verification and Acceptance Tests are completed and the system is accepted.

3. Note that in order to receive sign off on a completed test, all required stakeholder representatives must have been present to witness the testing and sign the field test sheet. Coordinate with the Program/Project Manager to have all required personnel present.

4. Correct defects as they are detected to put the system into operation.

5. Conclude the commissioning period upon successful completion of all Inspection, Performance Verification and User Acceptance Tests.

3.7 OBSERVATIONS

A. When field observation services are a part of the project scope, the Owner’s representatives will provide periodic observation of the progress of Work specified herein. The purpose of the observation service is to ensure compliance of Contractor's Work with specifications and drawings. The Owner’s representatives may also observe tests required .

B. Specifications and drawings represent Work to be done in view of total project requirements. To eliminate possible conflict with other trades, final location of conduits, jacks, outlets, components, etc., is responsibility of this Contractor. Contractor to provide all supervision required for his personnel to ensure that installation is made in accordance with specifications and drawings and all safety rules and regulations are observed. In event of conflicts of Work on project with other trades, Contractor is to make every reasonable effort to resolve conflict through meetings and discussions with other parties involved, by preparation of drawings, or other appropriate action. Only after this has been done shall the Designer's assistance be requested through the RFI process.

C. When the Designer is requested to visit the project to aid in resolution of conflicts, or for witnessing tests, they shall be given a minimum of 48 hours’ notice prior to time their presence is requested at job site.

3.8 CLOSEOUT ACTIVITIES

A. Training:

1. Perform training, if required.

B. Record Documentation:

1. Legibly mark drawings to create Record Drawings that record the final and actual “As-Built” security access and surveillance system installation.

a. Mark each edited electronic as-built drawing with the words "Record Document".

b. Include all noted and design changes pertaining to the security access and surveillance system "as built" conditions, and a set of permitted construction documents for the Owner's records.

c. Include communication conduit, cabling, and pathways used; field changes of dimensions and details; changes in details from those indicated on the Contract Drawings; details not on the original Contract Drawings; the make and model of the actual products installed, and the following additional information:

1) Drawing Index and a system legend.

2) A system schematic and equipment schedule.

3) The Sequence of Operation.

4) Complete communication-system architectures, including information on applicable network addressing, DIP switches, and jumpers.

5) Floor plans showing the location of key system components, and the routing of the communication system trunk lines.

6) Enclosure drawings, segregated by enclosure, and including the following:

7) Bill of material, including required spares.

8) Component layout plans.

9) Complete wiring schematics having information on applicable network addressing, DIP switches, and jumpers.

10) Port/connector layout plans for cross-patch termination assemblies.

11) An Instrument Index, listing all instruments integrated into the system, and segregated by areas.

12) An input and output (I/O) point listing, including all software and hardware points, and complete with configuration details for each point, segregated by enclosure.

d. Include schedules and related drawings documenting the usage/assignments of each of the following assemblies:

e. Include cable lists specifying the cable, wire pair, and connector and pin assignments for all signal, power, and ground leads.

f. Include the operating parameters of individual devices.

g. Operation and Maintenance Data:

2. 30 days before the date scheduled for the training course, submit the Record Documentation to the Program/Project Manager for review.

a. Should additional information or revisions be required, the reviewed documents will be returned to the Contractor for correction and re-submittal to the Program/Project Manager.

END OF SECTION

(THIS PAGE IS INTENTIONALLY LEFT BLANK.)

SECTION 28 13 00 - ACCESS CONTROL AND ALARM MANAGEMENT SYSTEM (ACAMS)

PART 1 - GENERAL

1.1 SUMMARY

A. Section Includes:

1. Access control (ACAMS) and device monitoring system (DMS) work consists of furnishing all equipment, tools, labor, and materials necessary to install and test the access control and device monitoring system components as specified in these contract documents. All attachments, connections, controllers, network equipment, line drivers, and miscellaneous hardware needed for a complete end-to-end system to be integrated with the Owner's head end system, without interference with the remaining system network, shall be the responsibility of the access control and device monitoring system Contractor.

2. The Contractor shall furnish and install all access control and device monitoring system components and cabling necessary at each project location and at the Owner's head end system. The Contractor shall coordinate with the projects inside and outside plant communications cabling systems provider to coordinate pathway space for the access control and device monitoring system components. The communication cabling contractor is NOT responsible for the installation of the access control and device monitoring system cabling. The Contractor shall coordinate with the project electrical systems provider to ensure proper power and proper cabling pathway is provided to the access control and device monitoring system device locations. The Contractor shall coordinate with project elevator system provider and project trades providing other components (i.e., doors, gates, escalators, AED defibrillator units, and associated hardware) to verify the locations and equipment that access control and device monitoring end device components will be connected to.

3. Pay all required sales, gross receipts, and other taxes. Contractor shall secure and pay for plan check fees, permits, fees, and licenses necessary for the execution of work as applicable for the project.

4. Comply with all codes, ordinances, regulations, and other legal requirements of public authorities which bear on performance of work.

B. Related Documents:

1. Section 28 05 00 - Common Work Results for Electronic Safety and Security

1.2 ADMINISTRATIVE REQUIREMENTS

A. Coordination:

1. Refer to Specification Section 28 05 00, COMMON WORK RESULTS FOR ELECTRONIC SAFETY AND SECURITY.

2. Existing Cylinders and Locks:

a. The Owner desires to preserve previously installed Access control (ACAMS) and device monitoring system (DMS) equipment.

b. The Owner has installed unique cylinders and locks on the doors.

c. Prior to the security access control equipment to be installed under this Contract is ready for installation, coordinate with the Program/Project Manager to have the Owner's representative uninstall and remove the airport's unique cylinders and locks. Additionally coordinate with the Owner to uninstall previously installed Access control (ACAMS) and device monitoring system (DMS) equipment that may be of value as spare parts.

1.3 QUALITY ASSURANCE.

A. Refer to Specification Section 28 05 00, COMMON WORK RESULTS FOR ELECTRONIC SAFETY AND SECURITY.

PART 2 – PRODUCTS

2.1 DESCRIPTION

A. Access Control and Alarm Monitoring System (ACAMS) Equipment:

1. The Access Control and Alarm Monitoring System (ACAMS) equipment to be provided shall be fully compatible with the Airport's existing access control system.

2.2 DESIGN CRITERIA

A. Review the design documents and provide Access Control and Alarm Monitoring System components as specified in this Section and depicted on the Contract Drawings.

1. Provide the components designed to operate within the environment specified. Provide climate control in the enclosures if required to comply with this requirement.

2. Doors

a. The Contractor shall provide access control at the door locations identified on the project plans to prevent unauthorized access to secure areas of the facility. The following devices shall be used for door control and monitoring:

b. Card Reader/Keypad: A combination card reader/keypad shall be installed on the designated doors. Some doors will be badge in/badge out while others are free exits. Refer to project plans for details.

c. Balanced Magnetic Switch (BMS): A door contact shall be used to monitor the status of all door locations identified in the project plans for access control.

d. Electric Strike Lock: An electric strike shall be installed on stairwell doors furnished with crash bars and the electric strike shall be installed on lever set doors on the doors shown in the contract documents to have electric strikes.

e. The electric strike lock shall be controlled and powered by the Access Control Unit (ACU) Panels.

f. Most locations are installed with an audible strobes/horn to indicate when a breach has occurred.

g. Request to Exit Motion Detector (REX): The request-to-exit devices shall be of the passive infrared motion detection type for interior mounted locations. The detector shall be as listed on the design drawings and match existing devices currently in use. Refer to design drawings for additional information.

h. PoE (eLock): A combination card reader/keypad shall be installed on the designated doors. Refer to project plans for details.

3. Access Control Unit (ACU) Panels:

a. Provide and configure access control unit (ACU) panels in the locations identified on the Contract Drawings.

b. If the Contract Drawings do not indicate a panel location, coordinate the locations with the Program/Project Manager.

c. Provide access control unit (ACU) panels designed to monitor the access control and device end devices identified on the Contract Drawings.

d. Provide access control unit (ACU) panels having the necessary components housed internally.

e. Provide access control unit (ACU) panels that constantly monitor the access control and device monitoring end devices to detect changes.

f. In the event an exception or alarm event takes place, provide access control unit (ACU) panels designed to report the situation to the Access Control and Alarm Monitoring System (ACAMS) head end system.

g. Provide access control unit (ACU) panels that function in a stand-alone mode in the event that communication to the Access Control and Alarm Monitoring System (ACAMS) head end system is interrupted.

h. Provide access control unit (ACU) panels that when operating in standalone mode are designed to buffer up to 5000 transactions, and to upload buffered data once communication is restored.

i. Provide access control unit (ACU) panels having battery backup designed to keep the access control panel online for up to 4 hours without primary power.

j. Provide access control unit (ACU) panels designed to report alarms to the head end on an alternating electric current (AC) failure alarm and/or a low battery alarm.

k. Provide access control unit (ACU) panel enclosures each equipped with a tamper alarm.

4. Alarms:

a. Design the access control unit (ACU) panels so that alarms originating from the end device monitoring points will appear in the head end system alarm summary page and event log.

b. Design the access control unit (ACU) panels so that device monitoring alarms are acknowledged in exactly the same way as regular Access Control and Alarm Monitoring System (ACAMS) alarms by selecting the alarm acknowledge button from the alarm summary window.

c. Alarm points to be monitored by the electronic security system (ESS) are implied by the alarm definitions and include the detector “detection” status, and system conditions such as “tamper”, “health” and “enclosure-door opened” status of the subsystems.

d. Provide Underwriters Laboratories, Inc. (UL) approved access control unit (ACU) panels.

5. Gates:

a. The Contractor shall provide access control at the gate locations identified on the project plans to prevent unauthorized access to secure areas of the airport facilities. The following devices shall be used for gate control and monitoring:

b. Card Reader/Keypad: A combination card reader/keypad shall be installed on one side of all gate locations identified in the project plans for access control.

c. Balanced Magnetic Switch (BMS): Shall be used to monitor the status of all gate locations identified in the project plans for access control.

d. Access Control and Alarm Monitoring System components are to be housed in the equipment cabinet per the contract drawings.

e. Readers are to be mounted as indicated on the contract drawings, using hi/lo pedestals when indicated.

f. Emergency vehicle access is to be provided per code.

2. DEVICE LICENSES

a. The Contractor shall furnish and install all required licenses for the Access Control and Alarm Monitoring System components.

2.3 COMPONENTS

A. Access Control and Alarm Monitoring System (ACAMS) Equipment:

1. Refer to the design drawings for list of components. Immediately notify the project manager of any components that are not notated in the contract drawings.

2. All access control and device monitoring system hardware and software must be 100% compatible and fully integrated with the existing ACAMS system.

3. Installation of additional access control and device monitoring system components shall fully meet the specifications of the existing ACAMS installation and provide for seamless integration with that system.

4. The ACU shall constantly monitor all access control and device monitoring end devices to detect changes. If an alarm event takes place, the ACU shall report the situation to the ACAMS head end system. ACU shall also function in a stand-alone mode if communication to the ACAMS head end system is interrupted.

B. Panel Devices:

1. Provide Access Control and Alarm Monitoring System (ACAMS) equipment identified on the contract drawings, and that includes the following items:

2. Labels:

    a. Provide 2-inch by 4-inch engraved black plastic labels having 1inch high white characters for the access control unit (ACU) panels.

        1) To attach the labels to the panel, provide number 6 screws that do not extend more than 1/8 inch past the interior side of the door.

3. Indoor Enclosure

    a. Provide standard enclosures for new access control unit (ACU) panels.

4. Cabinet Tamper Switches:

    a. Provide safety interlock switches to detect the opening of the cabinet doors or removable covers and prevent access to the dangerous or sensitive parts of the access control unit (ACU) panels.

        1) Manufacturer: UTC

        2) Part Number: SR-3012-N Plunged tamper switch, NO contacts, wire leads for ACAMS cabinets.

        3) Approved equal.

5. Controller:

    a. Provide controllers for the access control unit (ACU) panels.

6. Input Module:

    a. Provide input module (MIRO) boards for the access control unit (ACU) panels.

7. Output Modules:

    a. Provide input output module boards for the access control unit (ACU) panels.

8. Ethernet Interface Module:

    a. Provide an Ethernet interface module for the access control unit (ACU) panels.

9. Power Supplies and Batteries:

    a. Provide appropriate power supplies and batteries for the access control unit (ACU) panels identical to the existing power supplies but sized for the number of outputs being served.

        1) Manufacturer: Altronix Corporation

        2) Part Number: ALX1024ULXPD16 12VDC Power Supply Charger with PD16

        3) Part Number: AL1024ULXPD8 24VDC Power Supply Charger with PD8

        4) Approved equal.

10. Batteries:

a. Provide appropriate batteries for the access control unit (ACU) panels identical to the existing batteries but sized for the loads being served.

1) Manufacturer: Altronix Corporation

2) Part Number: BT1240 Altronix:12VDC Batt 40 Ah

3) Part Number: BT126 12VDC Batt 7 Ah

4) Part Number: BC1240 BT1240 battery enclosure with lock

5) Approved equal.

11. Relays

a. Provide appropriate relays and mounting track for the access control unit (ACU) panels that are sized for the devices being served.

C. Field Devices:

1. Provide Access Control and Alarm Monitoring System (ACAMS) equipment identified on the contract drawings, and that includes the following items as necessary to achieve a complete and fully functional system:

a. Resistor Packs:

b. Current Status Switches:

1) Provide fixed or adjustable current status switches, as applicable, for the access control unit (ACU) panels. Used to monitor escalator status.

c. Surge Suppression Kit

d. Door Contacts

e. Request to Exit

f. Horn/Strobe

g. Keypad/Badge Reader

h. Programmable Timer

i. Power Converter

j. Elevator Interface Box Relays

k. Relay Board

l. AED Contact Closures

m. Duress Buttons

D. Wiring:

1. Grounding Connectors:

a. Provide zinc plated compression type grounding connectors capable of handling up to 2 wires sized up to 4AWG, and having a hole sized for one 12 24 mounting screw.

1) Manufacturers: Chatsworth Products, Inc., http://www.chatsworth.com.

2) Part Number: 40158-020, or Approved Equal.

2. Grounding Conductors:

a. Provide bare or insulated copper AWG wire grounding conductors complying with the requirements specified in ASTM B 3, ASTM B 8, and ASTM B 33.

b. For communications systems, provide stranded, insulated copper conductor having a minimum size of 6 AWG, since this will accommodate different code requirements and allow for future changes.

c. Where single conductor insulated grounding conductors are required, furnish green color (or tape marking) insulation rated for 600 volts.

1) Manufacturers: The Okonite Company, www.okonite.com.

2) Anixter, www.anixter.com..

3) Continental Cables Company, www.continentalcables.com.pk.

4) Pirelli Cable Corporation.

5) Superior Essex, www.superioressex.com.

6) Approved equal.

3. All wiring for the system shall be in accordance with Articles 725 and 800 of the National Electric Code and local electrical codes. Wiring shall be UL Listed for use on access control systems:

PART 3 - EXECUTION

3.1 GENERAL

A. The access control components of the system shall monitor and control the hardware used to secure the facilities at the locations identified on the project plans and recalls the data needed for access management. Access control devices at entry points shall detect the credentials of the individual with information stored internally and determine if the person can be granted entry.

3.2 INSTALLATION

A. The Contractor shall install all access control and device monitoring system components in accordance with the manufacturer's recommendations, in accordance with applicable codes and standards referenced in the contract documents, and the approved Maintenance of Operations Plan (MOP).

1. Review the proper installation of each type of ACAMS device with the equipment Supplier.

2. Install using best practices and consistent with established preferences within the Owner's systems.

B. Conduit:

3. Install the conduit for field device wiring into the top of the access control unit (ACU) panel cabinet.

4. All access control system wiring shall be installed in a conduit to nearest cable tray system. If no cable tray system is available, cabling will be installed in a complete conduit system back to the nearest ACU cabinet. All cabling shall be plenum rated cable.

5. Conduit (EMT) must be used for wire installation – the minimum acceptable size is 3/4 inch. No free air wiring or exposed wiring will be acceptable. Any wiring run underground will be run in PVC conduit 1 inch minimum, buried at code specified depths (cabling will need to be rated for outside plant application). Intermediate metallic conduit will be used for installations that are subjected to physical damage. Conduit runs shall not exceed 180 degrees of total bends between pull points.

6. The Contractor is responsible for assuring that conduit size and wire quantity, size and type are suitable for the equipment supplied. The Contractor shall review the proper installation of each type of device with the equipment supplier. Final connections between the wiring and equipment shall be made under the direct supervision of the equipment supplier's representative.

7. Conduit must be green in color. If the conduit is not green in color, acceptable substitutes would be green conduit fittings and green junction box covers. Conduits must be supported per code and penetrations must be properly sealed.

8. All fittings must be steel and compression type. No setscrew fittings will be accepted.

C. Electrical Requirements:

1. Provide continuous and unbroken wires from the access control panel (ACU) to the point of origin in the electrical panel from which the circuit is derived.

   a. For the circuit breaker in the electrical panel, provide a clear, legible, and permanent marking explaining that the circuit feeds an access control panel (ACU) and that indicates the ACU number.

   b. Update the electrical panel schedule in the associated electrical panel in to indicate the access control panel (ACU) number in a clear, legible and permanent manner.

   c. At the point of termination in the access control panel (ACU), clearly indicate the source of the 120 Volt circuit using an easily read and permanent label.

2. Install the 120 Volt wiring within the access control panel (ACU) cabinet in separate conduit,

   a. “Free wiring” is unacceptable.

   b. Do not use the control panel (ACU) cabinet as a wire pathway for any equipment not installed within the ACU cabinet.

3. The circuit breaker will have a clear, legible, permanent marking explaining that the circuit feeds an ACU. The label should also describe the ACU number. The associated panel schedule shall be updated in a clear, legible, and permanent manner and shall contain the ACU number.

4. At the point of termination in the ACU, the source of the 120-volt circuit shall be clearly labeled in a manner which is easily read and permanent in nature.

5. All 120-volt wiring within the ACU cabinet shall be installed in separate conduit, “free wiring” is not allowed. The ACU shall NOT be used as a wire pathway for any equipment not installed within the ACU cabinet.

D. Wiring:

1. Multiple cables contained in one composite assembly that serve one portal will be allowed on above grade installations. Composite cables will not be allowed in underground installations.

2. All access control and device monitoring system cabling routed in cable tray system shall be neatly bundled to one side of the cable tray to provide separation between the data cabling on the other side of the cable tray. Coordinate with communications contractor. No cables are to cross or interlace with the communications cabling system. Provide Velcro cable tie wraps if needed to maintain separation.

3. All wiring at the panel must be labeled 6 inches from the termination point with permanent machine generated labels (no handwritten labels). Labels will be formatted consistently and be pre-approved by the Access Control Committee. A typical label would be formatted in this manner, ACU#- Building-Floor-Portal-Device.

4. Include all noted and design changes pertaining to the “as built” conditions and a set of permitted construction documents for the Owner’s records. The drawings are to be handed over to the Program/Project Manager at the end of the project for close out.

5. Control panels shall be labeled with 2-inch by 4-inch engraved black plastic labels with 1-inch white characters. All labels will be attached to the panel using #6 screws that do not extend more than 1/8 of an inch past the interior side of the door.

6. Control panel layout will be consistent from panel to panel and will be identical to the standard existing panels.

7. Door status switches will be external to the magnetic door locks. The use of internal door status switches on magnetically locked doors is prohibited.

E. Systems Integration:

1. Integration with Device Monitoring System (DMS):

    a. The Contractor shall provide all contact closures and relay boards to support the various devices on the project plans requiring device monitoring. These relay boards shall be located within the ACU panel enclosures and shall be connected to, integrated with, and configured within the Contractor provided ACU and existing ACAMS head end equipment to provide a fully functional system from device end to remote head end.

    b. Any alarms occurring from the end device monitoring points shall appear in the ACAMS head end system alarm summary page and event log. Device monitoring alarms shall be acknowledged in exactly the same manner as regular ACAMS alarms, which is by selecting the alarm acknowledge button from the alarm summary window.

    c. The following devices shall be used for device monitoring:

        1) Duress Button: The duress button shall be a latching mechanical hold-up switch designed for silent operation. The switch must reset with a key. The switch shall be an American Security Equipment Company Model HUSK-10, or approved equal, and match existing devices currently in use.

        2) Escalator Monitoring: The device used to monitor escalator status is a current sensor. The sensor must have an amperage range of 1.25-50 amps and be split core. The sensor shall be a Veris Industries Hawkeye Model 608 series, or approved equal, and match existing devices currently in use.

        3) Automated External Defibrillators (AED): The device used to monitor the door of the cabinet used to house AED's shall be a magnetic contact. The magnetic contact shall be mounted inside of the enclosure. The magnetic contact shall be a Sentrol Series Model 1038T, or approved equal, and match existing devices currently in use.

        4) Emergency Vehicle Entry components will be integrated to notify the command center upon activation.

        5) Cabinet tamper components will be integrated to notify the command center upon activation.

    d. Fully integrate the Access Control and Alarm Monitoring System (ACAMS) equipment provided under this Section into the existing ACAMS system.

        1) The Access Control and Alarm Monitoring System (ACAMS) access control unit (ACU) assembly, including all subcomponents provided under this Section, will communicate back to the existing ACAMS head end system.

    e. Provide the contact closures and input boards necessary to support the various devices indicated on the Contract Drawings to be monitored.

        1) Locate these boards within the access control unit (ACU) panel enclosures; and connect them to, integrate them with, and configure them within the access control units (ACU) provided under this Section and the existing head end equipment to provide a fully functional system from device end to remote head end.

2. Integration with Video Surveillance System shall function as follows:

    a. Upon receipt of an alarm by the ACAMS, with surveillance cameras associated with it, the ACAMS shall send a command signal to the video management system (VMS) defining camera number and the monitor number for which video is to be called upon to assist the operator in assessment and resolution of the ACAMS alarm.

3.3 SYSTEM STARTUP

A. Refer to Specification Section 28 05 00, COMMON WORK RESULTS FOR ELECTRONIC SAFETY AND SECURITY.

B. Inspections and Functional Tests:

1. Inspections:

a. The Access Control and Alarm Monitoring System (ACAMS) must be inspected for the following:

1) Craftsmanship of installation.

2) Conformance with approved shop drawings.

3) Wiring and component labeling.

4) Panel schedule accuracy.

5) Compliance with contract documents and best practices.

2. Alarm Condition Testing:

a. The Access Control and Alarm Monitoring System (ACAMS) must be tested to verify all alarm conditions are promptly and reliable delivered to, and displayed within, the ACAMS head-end system. Test the following control panel components to verify their proper installation and operation:

1) Door forced.

2) Door held open.

3) Power failure alarm.

4) Low battery alarm.

5) Communication failure alarm.

6) Alarm reporting following a communications failure.

7) Portal testing will include:

3. Portal Testing:

a. The Access Control and Alarm Monitoring System (ACAMS) must be tested to verify all alarm conditions are promptly and reliable delivered to, and displayed within, the ACAMS head-end system. Test the following control panel components to verify their proper installation and operation:

1) Craftsmanship of installation.

2) Door lock functionality.

3) Wire labeling.

4) Location labeling.

5) Valid badge and PIN.

6) Valid badge no PIN.

7) PIN no badge.

8) Invalid badge.

9) Inactive badge.

10) Lost badge.

11) Stolen badge.

12) Expired badge.

13) Terminated badge.

14) Normal time out.

15) Extended time out.

16) Elevator floor selection.

17) PIN duress.

18) Audio visual activation.

19) Door forced alarm.

20) Door held open alarm.

21) Proper REX operation.

4. Device Monitoring System (DMS) Testing:

a. In the performance verification test procedures, refer to each access control unit (ACU) panel by its unique identifier; and explain, step-by-step, the actions and expected results that will demonstrate that the system performs in accordance with the specified sequences of operation, and other Contract requirements.

b. For connected devices, proceed with approved user acceptance testing.

5. Access Control Test verifying component functionality:

a. The Access Control and Alarm Monitoring System (ACAMS) must be tested by the installer prior to acceptance testing with the Owner or Owner's representative.

1) Perform component level testing followed by the system testing per the previously submitted and approved test procedures.

2) Installer should successfully conduct all tests prior to inviting the Owner or their representative to official User Acceptance Testing.

3) Signed copies of the test are to be presented to the Owner or their representatives prior to User Acceptance Testing.

b. User Acceptance Testing will involve testing the user scenarios in real-world system-related passenger processing or airport movement and operational scenarios. Test Plans shall contain at a minimum:

1) The procedures to be followed, including the use of any test or sample data.

2) Test equipment used for the test.

3) Step-by-step operations.

4) Expected results associated with each step.

5) Tester's signature.

6) Witness's signature.

7) Date performed.

8) Pass or fail evaluation with comments.

9) A copy of the original signed test document with field notes shall be delivered to the Owner within 7 days after the testing.

A. Non-Conforming Work:

1. Correct the discrepancies or problems identified during each test at no increase in Contract Price.

B. Within the 30 days after completion of the Access Control Unit (ACU) Panel Performance Verification Test, submit the Access Control Unit (ACU) Panel Performance Verification Test Report to the Program/Project Manager for approval.

1. Include the data collected during the system inspections and the User Acceptance Testing.

3.4 CLOSEOUT ACTIVITIES

A. Refer to Specification Section 28 05 00, COMMON WORK RESULTS FOR ELECTRONIC SAFETY AND SECURITY.

END OF SECTION

(THIS PAGE IS INTENTIONALLY LEFT BLANK.)

SECTION 28 23 00 - SECURITY SURVEILLANCE SYSTEM

PART 1 - GENERAL

1.1 SUMMARY

A. Section Includes:

1. Fixed and pan/tilt/zoom (PTZ) cameras to be provided as required throughout the project for surveillance of the SIDA, Sterile, AOA and other restricted access-controlled portals as well as other areas as requested by the Airport.

2. The Video Management System (VMS) is a combination of tools for video surveillance and video forensics. The existing system is an IP video management software (VMS) designed for large-scale and high-security installations. It is designed to ensure end-to-end protection of video integrity and boost overall performance with hardware accelerated video decoding and centralized management of all servers, cameras and users.

3. The Contractor shall furnish and install all security camera components necessary at each project location and provide materials as necessary for the expansion of the Video Management System server environment. The Contractor shall coordinate with the projects inside and outside plant communications cabling systems provider to coordinate pathway space for the surveillance systems components. The Contractor is responsible for the installation of all category networking cable within the pathways that are provided by the contractor.

4. Pay all required sales, gross receipts, and other taxes. Contractor shall secure and pay for plan check fees, permits, fees, and licenses necessary for the execution of work as applicable for the project.

5. Comply with all codes, ordinances, regulations, and other legal requirements of public authorities which bear on performance of work.

B. Related Documents:

1. Section 28 05 00 - Common Work Results for Electronic Safety and Security

1.2 ADMINISTRATIVE REQUIREMENTS

A. Coordination:

1. Refer to Specification Section 28 05 00, COMMON WORK RESULTS FOR ELECTRONIC SAFETY AND SECURITY.

1.3 QUALITY ASSURANCE.

A. Refer to Specification Section 28 05 00, COMMON WORK RESULTS FOR ELECTRONIC SAFETY AND SECURITY.

PART 2 – PRODUCTS

2.1 DESCRIPTION:

A. Security Surveillance System:

1. The security surveillance system equipment to be provided shall be fully compatible with the Airport’s existing security surveillance system, which is also referred to as the video management system (VMS).

2.2 DESIGN CRITERIA:

A. Review the design documents and provide security surveillance system components as specified in this Section and depicted on the Contract Drawings.

1. Video Management System (VMS):

a. Video Recording Servers shall be added at the rate of 1 server per 30 cameras.

b. The video storage system shall be expanded to accommodate the additional cameras being added and connected to the VMS.

1) Provide expansion of the as directed by the Owner to support the storage needs of the additional cameras being added.

c. Provide VMS licensing for each additional camera.

2. Video Cameras

a. The video management system (VMS) Work to be performed consists of providing closed circuit high-definition television (HDTV) cameras at the locations indicated on the Contract Drawings.

1) The camera system proposed for the Work of this Contract must integrate with the existing VMS platform with proof of interoperability.

b. The cameras to be provided shall be IP-based and comply with established network and video standards.

c. Cameras shall be powered by utilizing the copper network cable, minimum Category 6, which is connected to a Power Over Ethernet (POE) capable network switch supporting IEEE standard POE (802.3af, 15.4W max), POE+ (802.3at, 30W max), and POE++ (802.3bt, 60W max).

d. POE devices must run either the vendor-neutral Link Layer Discovery Protocol (LLDP), or an approved proprietary protocol supported by the existing communications infrastructure network switches and routers.

e. Use of power injectors is not acceptable and will only be allowed when explicit permission is given by the Owner. Power injectors shall be provided by the contractor when approved for proper operation.

f. Powering the camera from an AC to DC converter is rarely acceptable, and will only be allowed when explicit permission is given by the Owner. AC to DC converters shall be provided by the contractor when approved for proper operation.

g. Units shall be fully supported by an open and published API (Application Programmers Interface), which shall provide necessary information for integration of functionality into third party applications.

h. Units shall comply with relevant ONVIF profile as defined by the ONVIF Organization.

i. Cabling between the camera and the equipment room shall be copper, minimum Category 6, with rare exceptions made to allow fiber optic connections to accommodate extremely long distances. In the event fiber is approved, an alternate to Power-over-Ethernet will be required.

j. Provide surveillance cameras designed to operate within the temperature ranges specified, and provide climate control in the surveillance camera housings if required to comply with this requirement.

k. For the duration of the project, the installer will maintain a log showing the camera number, the camera model and a narrative description of the cameras purpose.

2.3 COMPONENTS:

A. Closed Circuit High-Definition Television (HDTV) Cameras:

1. As identified in the Contract Drawings, or otherwise approved by the Program/Project Manager.

B. Closed Circuit High Definition Television (HDTV) Camera Accessories:

1. Provide the following accessories for the video cameras:

a. Connector kits.

b. Domes, smoked vs clear, request direction if not specified in contract drawings.

c. Lens as appropriate for the application.

d. Mounting as appropriate for the environment.

e. Wall mount brackets and wall bracket accessories where required.

f. Midspan High Power over Ethernet (PoE) ports.

g. Illuminators if specified on contract drawings.

h. Sunshields as appropriate for the environment.

B. Wiring

1. Grounding Connectors:

a. Provide zinc plated compression type grounding connectors capable of handling up to 2 wires sized up to 4AWG, and having a hole sized for one 12 24 mounting screw.

1) Manufacturers: Chatsworth Products, Inc., http://www.chatsworth.com.

2) Part Number: 40158-020.

3) Approved equal.

2. Grounding Conductors:

a. Provide bare or insulated copper AWG wire grounding conductors complying with the requirements specified in ASTM B 3, ASTM B 8, and ASTM B 33.

b. For communications systems, provide stranded, insulated copper conductor having a minimum size of 6 AWG, since this will accommodate different code requirements and allow for future changes.

c. Where single conductor insulated grounding conductors are required, furnish green color (or tape marking) insulation rated for 600 volts.

1) Manufacturers: The Okonite Company, www.okonite.com.

2) Anixter, www.anixter.com..

3) Continental Cables Company, www.continentalcables.com.pk.

4) Pirelli Cable Corporation.

5) Superior Essex, www.superioressex.com.

6) Approved equal.

3. All wiring for the system shall be in accordance with Articles 725 and 800 of the National Electric Code and local electrical codes.

PART 3 - EXECUTION

3.1 GENERAL

A. The security surveillance components of the system shall gather and stored visual assets used to surveil and secure the facilities at the locations identified on the project plans and recalls the data needed for situational awareness and forensic evidence.

B. The security surveillance system is a critical system for the Airport and needs to operate reliably without obstructions or outages. Any knowledge of obstructions or system vulnerabilities should immediate be brought to the attention of the Program/Project Manager.

3.2 INSTALLATION

A. The Contractor shall install all security surveillance systems in accordance with the manufacturer installation procedures, in accordance with applicable codes and standards referenced in the contract documents, and the approved Maintenance of Operations Plan (MOP).

B. Labeling:

1. Provide permanent machine generated labels to label wiring at the panel 6 inches from the termination point.

a. Do not provide hand written labels.

b. Format the labels consistently.

c. Provide labels that have been preapproved by the Program/Project Manager.

C. Systems Integration:

1. Fully integrate the security surveillance systems provided under this Section into the existing security surveillance systems.

2. Integrate the security surveillance camera equipment and components into the existing video management system (VMS).

3. Integrate the security surveillance camera equipment and components into the existing Access Control and Alarm Management System (ACAMS) head end system.

3.3 SYSTEM STARTUP

A. Refer to Specification Section 28 05 00, COMMON WORK RESULTS FOR ELECTRONIC SAFETY AND SECURITY.

B. Inspections and Functional Tests:

1. Inspections:

a. The Security Surveillance System must be inspected for the following:

1) Craftsmanship of installation.

2) Conformance with approved shop drawings.

3) Wiring and component labeling.

4) Compliance with contract documents and best practices.

2. Security Surveillance System Test verifying component functionality:

a. The Security Surveillance System must be tested by the installer prior to acceptance testing with the Owner or Owner’s representative.

1) Perform component level testing followed by the system testing per the previously submitted and approved test procedures.

2) Installer should successfully conduct all tests prior to inviting the Owner or their representative to official User Acceptance Testing.

3) Signed copies of the test are to be presented to the Owner or their representatives prior to User Acceptance Testing.

3. User Acceptance Testing will involve testing the user scenarios in real-world system-related passenger processing or airport movement and operational scenarios. Test Plans will contain at a minimum:

a. The procedures to be followed, including the use of any test or sample data.

b. Test equipment used for the test.

c. Step-by-step operations.

d. Expected results associated with each step.

e. Tester's signature.

f. Witness's signature.

g. Date performed.

h. Pass or fail evaluation with comments.

i. A copy of the original signed test document with field notes shall be delivered to the Owner within 7 days after the testing.

A. Non-Conforming Work

1. Correct the discrepancies or problems identified during each test at no increase in Contract Price.

B. Within the 30 days after completion of the Security Surveillance System User Acceptance Test, submit the Test Report to the Program/Project Manager for approval.

1. Include the data collected during the system inspections and the User Acceptance Testing.

3.4 CLOSEOUT ACTIVITIES

A. Refer to Specification Section 28 05 00, COMMON WORK RESULTS FOR ELECTRONIC SAFETY AND SECURITY.

END OF SECTION

(THIS PAGE IS INTENTIONALLY LEFT BLANK.)