4. Anchoring: Support and fasten boxes securely per SNEC.

5. Sizes: Provide boxes of sizes adequate to meet SNEC volume requirements, but in no case smaller than sizes indicated.

6. Do not use sectional (gangable) boxes.

7. Do not use device plates as covers for boxes in exposed locations.

8. Do not use round boxes where conduit must enter box through side of box, which would result in difficult and insecure connections when fastened with locknut or bushing on rounded surface.

9. Threaded Hubs: Use threaded hub type boxes with gasketed weatherproof covers in all exterior locations; where installed on unfinished walls, columns or plasters; where exposed to moisture laden atmosphere; or where indicated.

10. Extension Rings: Where extension rings are required on existing outlet boxes, drill new mounting holes in the rings to align with the mounting holes on the existing boxes.

E. Pull and Junction Boxes:

1. Conform to SNEC.

2. Locate junction and pull boxes in accessible locations.

3. Do not locate boxes in finished areas.

4. Supports: Provide in each box sufficient clamps, grids, or devices to which cables are secured in neat and orderly fashion permitting ready identification and so that no cable will have an unsupported length of more than 30 inches.

F. Raceway Supports:

1. Compliance: Install hangers, sleeves, seals, U-channel supports and fasteners as indicated and in accordance with manufacturer's written instructions. Comply with requirements of SNEC and American National Standards Institute (ANSI)/National Electrical Manufacturers Association (NEMA) for installation of supporting devices.

2. Provide individual and multiple (trapeze) raceway hangers, and riser clamps as necessary to support raceways. Provide U-bolts, clamps, attachments, and other hardware necessary for hanger assembly, and for securing hanger rods and conduits.

3. Arrange for grouping of parallel runs of horizontal raceways to be supported together on trapeze type hangers where possible.

4. Support individual horizontal conduits and EMT 1.5 inches in size and smaller by either one-hole pipe straps or separate pipe hangers. Use separate pipe hangers for larger sizes. Spring steel fasteners may be used in lieu of pipe straps or hangers for sizes 1.5-inch and smaller in dry locations. For hanger rods with spring steel fasteners, use 0.3-inch diameter or larger threaded steel. Use steel fasteners that are specifically designed for supporting single conduits or EMT. Unless otherwise indicated, do not use wire as a means of support. Use spring steel conduit supports only for lighting system branch circuit raceway in suspended ceilings in dry locations.

5. Except as otherwise indicated, space supports for metallic and non-metallic raceways in accordance with the requirements of this Section and the requirements of the SNEC.

6. Provide support for exposed or concealed raceway as close as practical to and not exceeding 12 inches from an unsupported box or access fitting. In horizontal runs a support at a box or access fitting may be omitted when the box or access fitting is independently supported and the raceway termination is not made with a chase nipple or threadless box connector.

7. In vertical runs provide such support that the load produced by the weight of the raceway and the enclosed conductors is carried entirely by the conduit supports, with no weight load on raceway termination's or conductor terminals.

G. Miscellaneous Supports :

1. Provide supports for all miscellaneous electrical components as required to produce the same safety allowances as specified for raceway supports above. Provide metal channel racks for mounting cabinets, panelboards, disconnects, control enclosures, pull boxes, junction boxes etc.

2. In open overhead spaces, cast boxes threaded to raceways need not be separately supported except where used for fixture support; support sheet metal boxes directly from the building structure or by bar hangers. Where bar hangers are used, attach the bar to raceways on opposite sides of the box and support the raceway with an equally acceptable type fastener not more than 24 inches from the box. When penetrating reinforced-concrete members, avoid cutting any reinforcing steel.

3. Wood backing shall not be used for mounting any equipment except as required for temporary power or telephone terminal strips or unless noted otherwise on drawings. Only steel frame work or strut type channels shall be used for equipment mounting.

4. In hollow masonry, tile, plaster or gypsum board, use toggle type bolts to secure equipment, conduit runs and outlet boxes in place.

H. Fasteners:

1. Unless otherwise indicated securely fasten all electrical items and their supporting hardware including, but not limited to, conduits, raceways, cables, busways, cabinets, panelboards, wall-mounted transformers, boxes, disconnect switches and control components to the building structure.

2. Fasten by means of wood screws or screw-type nails on wood; by toggle bolts on hollow masonry units; by concrete inserts or expansion bolts on concrete or brick; by machine screws; welded threaded studs, or spring-tension clamps on steel work. Do not weld conduits or pipe straps to steel structures. In partitions of light steel construction use sheet metal screws.

3. Do not use powder charged devices or Ramsets to attach fasteners (unless otherwise approved by the District).

4. Holes cut to a depth of more than 1.5 inches in reinforced concrete beams or to a depth of more than 3/4 inches in concrete joints shall not be allowed. Notify the District if such penetration is needed.

5. Loads applied to any fastener shall not exceed one-fifth of the proof test load. Use vibration and shock-resistant fasteners.

3.02 ADJUSTING AND CLEANING

A. Upon completion of installation of raceways, inspect interiors of raceways at all outlet, junction and pull boxes, remove burrs and obstructions.

B. Run a swab or mandrel to remove dirt and blockages. Raceways which are deformed and prevent the passage of a mandrel shall be replaced.

C. Remove dirt and construction debris from all outlet, junction and pull boxes.

END OF SECTION

SECTION 281300 - ACCESS CONTROL SYSTEM

PART 1 GENERAL

1.01 SUMMARY

A. The Security Management System (SMS) shall be the key central component for managing physical security. The system shall provide a variety of integrated functions including access control, alarm monitoring, intrusion detection, visitor management and video

1.02 RELATED REQUIREMENTS

A.	280500	Electronic Systems General Requirements
B.	280513	Conductors and Cables
C.	280514	Fiber Optics
D.	280528	Raceways and Boxes
E.	281500	Electronic Systems and Components
F.	282300	Video Management System

1.03 REFERENCES

A. Abbreviations

1. ACS: Access Control System
2. API: Application Programming Interface
3. DAS: Direct Attached Storage
4. DPS: Door Position Sensor
5. DRI: Dual Reader Interface
6. FIPS: Federal Information Processing Standard
7. IP: Internet Protocol
8. LAN: Local Area Network
9. LDAP: Lightweight Directory Access Protocol
10. NAS: Network Attached Storage
11. NFC: Near Field Communications
12. NVR: Network Video Recorder
13. OCM: Output Control Module
14. ODBC: Open Database Connectivity

15. OPC: OLE for Process Control
16. OSDP: Open Supervised Device Protocol
17. PACS: Physical Access Control System
18. PIV: Personal Identity Verification
19. POE: Power-Over-Ethernet
20. RAM: Random Access Memory
21. REST: Representational State Transfer
22. REX: Request to Exit
23. RFID: Radio Frequency Identification
24. RIM: Reader Interface Module
25. SAN: Storage Area Network
26. SIA: Security Industry Association
27. SMS: Security Management System
28. SQL: Structured Query Language
29. SRI: Single Reader Interface
30. SSL: Secure Sockets Layer
31. TCP: Transport Control Protocol
32. TDE: Transparent Data Encryption
33. TWIC: Transportation Worker Identity Card
34. UPS: Uninterruptible Power Supply
35. VMS: Video Management System

B. Definitions

1. Alarm aggregation: A mechanism of combining several alarms into a single item (group) based on certain criteria.
2. Credential: Data assigned to an entity and used to identify that entity.
3. Designated One Person Control: Requires that a designated cardholder is present before anyone else is allowed to access a certain area.
4. Designated Two Person Control: Requires the presence of two cardholders, designated as special “Team Members”, to restrict individuals from being alone in restricted or highly secure areas as well as restricting the type of personnel allowed in those areas.

5. Devices Global Hard Anti-passback: Once access has been granted via a valid badge presentation, (1) a cardholder cannot present their badge to another entry card reader within the same area without first presenting it to the area's exit card reader, and (2) any attempt to use any card reader in the same area other than exit card reader shall result in access denied and an alarm report.

6. First Card Unlock: Function where a pre-determined time zone activated unlock command is suppressed until a valid credential has been presented and granted access to the portal.

7. Global Soft Anti-passback: As defined in Devices Global Hard Anti-passback with the exception that the cardholder shall be allowed access to a new area for which he is authorized.

8. (Guard) Tour: One or more checkpoints (card readers or alarm inputs) checked during a guard's predetermined path.

9. Interlock group readers: Configuration for local, but not global, anti-passback whereby only one door may be opened at a time within the area and an alarm is generated for any denied access.

10. Pass-Through: The ability assigned to a person's credential that allows them to access a door even if in lockdown state.

11. Occupancy Limit: Restricts the number of cardholders that shall be present in an area at any given time.

12. Region: A separate instance of the distributed database.

13. Representational State Transfer (REST): A software architecture style consisting of guidelines and best practices for creating scalable web services.

14. RESTful API's (Application Programming Interfaces): Term given to Web services using the REST architecture.

15. Runaway detection: A situation when there are more than a specified number of alarms coming from a given device within a specified time interval.

16. Tailgate Control: Triggered when a person receives an access granted, an output will be fired momentarily for a single person or twice for two people, for a maximum duration of one second.

17. Timed Anti-passback: Configurable wait time between an initial badge swipe and the time at which the same badge will be accepted again at the same card reader.

18. Timezones: Time-based periods, encompassing time of day, day of the week and holidays, which are stored on the ISC and control hardware behavior, cardholder access, online mode of the readers, activation of outputs, masking of inputs, and logging events to the database.

19. Two Person Control: Restricts access to certain areas unless two (2) cardholders are present, where the second badge must be presented within a designated time interval of the first to provide access.

C. Reference Standards

1. Underwriters Laboratories
    a. UL 294 - Standard for Access Control System Units
    b. UL 1076 - Standard for Proprietary Burglar Alarm Units and Systems
    c. UL 1981 - Standard for Central-Station Automation Systems
    d. UL 1610 - Central Station Automation System Software
2. ISO/IEC 14443-3:2011 – Identification Cards
3. ADA – Americans with Disabilities Act
4. National Fire Protection Association
    a. NFPA 70 National Electric Code
    b. NFPA 101 – Life Safety Code
    c. NFPA 731 - Standard for the Installation of Electronic Premises Security Systems
5. Institute of Electrical and Electronic Engineers
    a. IEEE 802.3 Ethernet Standards
6. National Institute of Standards and Technology (NIST)
    a. Federal Information Processing Standard Publication 140-2 – Security Requirements for Cryptographic Modules
    b. Federal Information Processing Standard Publication 197 – Advanced Encryption Standard
    c. Federal Information Processing Standard Publication 201 – Personal Identity Verification
    d. SP 800-116 A Recommendation for the Use of PIV Credentials
7. Security Industry Association
    a. Open Supervised Device Protocol (OSDP)
8. Video
    a. ISO / IEC 10918 – JPEG
    b. ISO / IEC 14496 –10, MPEG-4 Part 10 (ITU H.264)

D. Submittals
1. Informational Submittals
    a. Product Data

b. Manufacturer product data sheets

c. Manufacturer product instructions, and installation and operating manuals

d. Shop Drawings

1) Complete set of proposed drawings, identifying equipment locations, types of cabling, numbers of conductors, raceway locations, and termination points of each conductor.
2) Complete listing of proposed devices, indicating interconnection equipment locations and specifying terminal/connecter termination locations.
3) Operational narrative of each component/system.

2. Closeout Submittals

a. Warranty Documentation:

1) Manufacturer warranty statements for all system components and applicable equipment.

3. Record Documentation:

4. Maintenance Material Submissions:

a. Listing of spare parts required to maintain the system.

5. Closeout Submittals

a. Final listing of doors, locations, and normal status in MS Excel format.

b. Complete set of supplier's operating instructions, installation instructions, and troubleshooting guide, to include but not be limited to instructions for:

c. Schematic drawings depicting type and location of interface equipment/components, number of cables and conductors, raceway locations, types of connectors, circuit requirements and type and dimensions of enclosures.

1.04 QUALITY ASSURANCE

A. Contractor qualifications:

1. Company with a minimum of 2 (two) years system design, engineering supervision, and installation experience in the access control industry.

2. Contractor must be a current, authorized reseller for the SMS product and manufacturer, and provide evidence thereof.

B. Manufacturer Qualifications

1. The SMS Hardware and software manufacturer(s) shall have delivered security management products for at least 10 (ten) years, and shall have a sufficiently large and diverse installed base to ensure competence in delivering, deploying, and supporting systems of this type and scale throughout their expected service life.

1.05 PRODUCT DELIVERY, STORAGE, AND HANDLING

A. Acceptance: Upon delivery to the site, Contractor shall inspect all products and materials for any damage.

1.06 PROJECT CONDITIONS

A. Maintain environmental conditions (temperature, humidity, and ventilation) within limits recommended by manufacturer for optimum results.

1.07 MANUFACTURER CAPABILITIES

A. Advanced Services - The SMS Manufacturer shall have an in house Advanced Services group available to contract for:

1. Professional engineering services to include on-site or remote advanced support, enterprise planning and advanced deployments, system design, supporting software tools, database migrations and conversions, emergency service, system assessments.

2. Remote Management and Embedded Services to include project management and coordination, contract management, VAR coordination, and Manufacturer resource coordination

3. Custom applications and reports.

B. 3rd Party Product Certification Program

1. The SMS Manufacturer shall have a Partner Program that allows other products to develop interfaces to the Security Platform based on a RESTful Web Services API.

a. Third-party integrations shall have been certified by SMS Manufacturer personnel.

b. Each new revision or version of the third-party system shall be subject to recertification.

2. Interfaces developed shall be tested and certified by the SMS Manufacturer for each new version of product released.

3. The Certification Program shall have integrations which include, as a minimum, Command and Control, Key Management, Fire Detection, Intrusion, Elevator and Critical Communication products, and the capability to integrate with other security and non-security products, as desired by the customer.

C. Global Support Capability

1. The SMS Manufacturer shall have dedicated global support mechanisms in place to provide local support to any installation covered by this specification, regardless of location throughout the world.

2. The SMS Manufacturer shall have multiple independent Value Added Reseller (VAR) options to support customers in each market.

3. The SMS Manufacturer shall have a proven and demonstrable history of deploying Enterprise-scale solutions to Global customers.

1.08 WARRANTY AND SUPPORT

A. Manufacturer shall warrant that the physical media on which the Software is distributed, if applicable, is free from defects in materials and workmanship and that the Software will function in substantial accordance to the Documentation that accompanies the Software for a period of one (1) year from the date of shipment of the Software to the reseller. This limited warranty is void if failure of the Software results from accident, abuse, modification, misapplication, misuse, abnormal use or a virus.

B. Hardware warranties shall be provided by the original manufacturer of the specific hardware device or component.

C. Manufacturer shall offer a supplemental software support program to include software updates and upgrades.

1.09 LICENSE

A. The SMS shall only require a single license key to be present on the database server for the SMS to operate.

1. A license key on the database server shall determine the number of client workstations that shall be able to connect to the SMS and access its functionality.

a. The license key shall either be a physical device or a software license key.

b. License keys shall not be required at the client workstations.

2. The SMS shall allow the SMS user the ability to activate, return, or repair the software license key.

3. The software license shall only be used on a physical computer or in a VMware virtual environment.

1.010 LOCALIZATION (LANGUAGE)

A. The SMS (Security Management System) shall provide language support for interface and database by default or by installation of specific localization packages. Support shall be written using Unicode format and have the capability to support both single-byte and double-byte languages, with the list of languages to available. Localized versions of documentation may be available.
1. Required languages: English

PART 2 PRODUCTS

2.01 MANUFACTURER

A. LenelS2

1. 1212 Pittsford-Victor Road, Pittsford, NY 14534-3820
Phone: +1 585 248-9720
info@lenel.com
2. Products

a. Security Management Software: 7.4 OnGuard

2.02 GENERAL DESCRIPTION

A. The Security Management System ("SMS") shall be the key central component for managing physical security access control, video, alarm monitoring, visitor management.

B. Scalability

1. The SMS shall be capable of processing an unlimited number of credential readers, scalable from single site to multiple sites.

C. Database

1. The SMS shall be based upon one or more independent secure SQL database instances, one of which has been designated as the system master.

D. The SMS shall provide a variety of integrated core functions to include:

1. regulation of access and egress

2. provision of identification credentials

3. video management

4. monitoring and managing alarms related to both access control and intrusion

5. visitor management

E. Integrations – The SMS shall employ a RESTful, Web Services API to enable the integration of select third party products and functions with the core functions of the SMS.

F. User Interface

1. The SMS shall provide access to licensed and installed applications through a common browser-based launcher application that can invoke various components and modules of the SMS from a single location, with users able to customize, rearrange, and retain configurations.

a. This launcher shall offer Single Sign On and enable launch of both Windows and browser clients.

G. Communication Security

1. All communication paths within the SMS shall support encryption to provide end-end communication security.

H. User Login and Authentication

1. The SMS shall offer both a native capability to manage system users, as well as the option to authenticate system users through an external Active Directory, LDAP, or OpenID Connect (OIDC) system. Solutions that do not support OpenID Connection authentication of system users shall not be acceptable. System shall also allow for denial of login after a specified number of failed retries.

2. System shall also log the user out of any browser clients after a specified period of inactivity.

3. Customizable login message and ability to link to external websites or documents.

I. The SMS should provide the ability for control of expiration and complexity for the User Account Passwords internal to the system such that system could comply with existing NIST and NERC guidance.

J. Complexity options to include: Upper/Lower Case, Numeric, Special Characters, Minimum Length, Prohibited List, and Password history

K. Expiration options to include: Number of days as well as administrator enforced update of password.

L. Operational Efficiencies

1. The SMS shall offer a self-service portal for employees to request access and for area owners to approve, hold or deny requested access. This web portal shall also offer administrator-configurable self service functions for cardholders such as PIN change, setting up a visitor and visit record, and resending a mobile credential to their mobile device.

2. Transactions shall be reportable within the SMS.

3. The SMS shall offer an expedient means to identify access rights provided in violation of corporate policies and to automatically revoke access rights for these violations.

4. The SMS shall offer a browser-based analysis tool that collects system data for comprehensive system health monitoring and displays it on a customizable, intuitive dashboard.

2.03 ARCHITECTURE

A. Open Architecture – The SMS shall support an ‘open architecture’ allowing for additional support of products outside of the vendor proprietary options.

1. SMS shall support hardware that is non-proprietary such that other vendors could readily offer support for these devices. Access Control Panels that are only supported by a single SMS provider shall not be acceptable.

2. SMS shall support a RESTful Web Services Application Programming Interface (API) that supports the opportunity for 3rd party integration. Access to this API should be managed through a program to ensure that certified integrations utilize this API appropriately.

3. The SMS shall, when possible, leverage open or industry standards for device and system design.

B. System Topology

1. The SMS shall include a central or distributed server component for managing security and any associated integrations.

a. The SMS server shall function as an application server for connectivity of workstation based or browser-based clients for support of configuration and management.

2. An input or output linkage feature shall allow linking of input points to output control points.

3. Tasks shall be accessible from compatible client workstations on the network utilizing any of the following:

    a. Traditional client-server architecture, using either Windows clients or browser clients for common day-to-day tasks.

    b. Support for federated system architecture (multi-server, multi-database) where the SMS supports the expansion of the system architecture and allows for user deployment based upon their system architectural needs

    c. Centralized distribution (publishing) of applications using Windows Terminal Server and Citrix® on Windows, UNIX, Linux or Apple Macintosh based systems through any compatible internet browser application and/or by means of a mobile computing platform using a wearable computer, Tablet PC, or mobile device.

4. Redundancy - The SMS shall support the following means of fault tolerance and SMS redundancy:

    a. Hot Standby Servers - A Primary Server shall be the main server that is in use when the SMS is operating under normal conditions, and the SMS shall mirror its database information to a Backup/Secondary Server.

        1) Field hardware shall be configured for both the Primary Server and the Backup Server, which shall each recognize the same TCP/IP ISC address on the network.
        2) Upon sensing Primary Server failure, the Backup Server shall automatically initiate itself as the Primary Server and shall begin communication with the Field Hardware.
            a) Frequency of check for Primary Server failure: 5 seconds
            b) Resynchronization time upon Primary Service restoration: 5 minutes maximum

    b. Cluster/Warm Standby – A Primary Server shall be the main server that is in use when the SMS is operating under normal conditions.

        1) Field hardware shall be configured for both the Primary Server and the Backup Server, which shall each recognize the same TCP/IP ISC address on the network.
        2) Upon sensing Primary Server failure, the Backup Server shall bring the necessary services online and shall begin communication with the Field hardware.
        3) Shared media devices, either single or dual, shall be employed to house the hard disk used by both servers.
            a) Resynchronization time upon Primary Service restoration: 5 minutes maximum

    c. Disk Mirroring - This configuration shall allow data to be stored on dual hard disks running simultaneously.

    d. RAID Level 10 - The SMS shall offer a Fault Tolerant Redundant Array of Independent Disks Level 10 (RAID Level 10) with a hot standby disk.

        1) Redundant components: disk storage, controller channels, high efficiency power supplies

e. Distributed Intelligence - In the event SMS communications is lost or the database server fails, Intelligent System Controllers shall provide complete control, operation and supervision of the system's monitoring and control points.

1) Should the downtime exceed the capacity of the Field Hardware buffer and events are overwritten, an alarm shall appear in the Alarm Monitoring Window notifying the System Operator that events were overwritten.

C. Inter-site Communications

1. The SMS shall support a distributed system (application and database) installation to support geographical or logical separation and management of installations while maintaining a centralized system for reporting.

a. Each distributed system shall support operation of the local clients and hardware, and provide configuration, event, and transactional events to the central system.

b. The SMS shall use a message architecture to transfer necessary incremental credential data from one site to another. This architecture shall provide data queuing, guaranteed delivery, and secure transmission of this data.

D. External Interaction of Data

1. The SMS shall be able to connect to and interface bi-directionally with external data sources utilizing the following methods:

a. ASCII with support for XML formatted text exchange

b. Real-time exchange of data via Active Directory or LDAP

c. Software Application Programming Interface (API)

E. Database - The SMS shall utilize a single supported relational database.

1. Acceptable databases: Microsoft SQL, Oracle

2. Acceptable operating systems: Microsoft Windows Servers or Clients

3. Protection of 'Data at Rest' within the database shall be provided via SQL Transparent data encryption (TDE) and shall be supported to perform real-time I/O encryption and decryption of the database and database log files.

4. The SMS database server shall support an unlimited number of cardholders and visitors limited by the available memory, storage, and processing of the devices. The SMS database server shall support an unlimited number of system events and System Operator transactions in the history file limited only by available hard disk space. The SMS database server shall support an unlimited number of system events and System Operator transactions in the history file limited only by available hard disk space.

5. The SMS shall support bi-directional data interface to external databases in real-time or in a batch mode basis.

a. The SMS shall support a one-step download and distribution process of cardholder and security information from the external database to the SMS database and through the system to Intelligent System Controller (ISC) databases.

b. If a required communication path is broken, the data shall be stored in a temporary queue and shall be automatically downloaded once the communication path is restored.

F. Security

1. Each page in the cardholder record shall be permission protected.

2. Each field in the database shall be permission protected.

3. Communication throughout the SMS shall be AES encrypted, using TLS where practical.

4. All cardholder PIN codes within the system shall be encrypted.

G. A Network Account Management Module shall integrate SMS cardholders with external user network accounts, allowing System Administrators to perform a set of administrative tasks in Windows domains from the System Administration Module, and to create a link between physical access control and logical domains.

H. The SMS shall allow, through standard API toolkits, System Administrators to expose specific SMS data and events that are relevant to IT information or other third-party systems or to allow, System Administrators to accept and process information exposed from the IT information or other third-party systems.

2.04 CORE FUNCTIONALITY

A. Access Control - access granted or denied decisions, define access levels, and set time zones and holidays. The SMS shall support features such as area control (two-man control, hard, soft, and timed anti-passback), database segmentation, and time zone or holiday overrides

1. Configuration

a. Credentials

1) SMS credential management functionality shall allow:
   a) enrollment of cardholders via traditional thick client and/or by a browser-based credential application for the storage of cardholder records in the database
   b) formatting of cardholder records
   c) capturing of images, biometric data, and signatures
   d) user-defined fields in the cardholder record
   e) issuance/reissuance of traditional plastic badges and/or mobile credentials using information in the cardholder record. It shall be possible to print to a designated, configured badge printer from both browser-based and Windows clients. This mechanism shall be based on a print server architecture supported by the SMS. Solutions requiring a printer directly connected to the device on which the browser client is used shall not be acceptable.
   f) import or export of cardholder data from internal or third-party systems
      i. data delimiter: definable
      ii. import-export filters: selectable
   g) assignment and modification of access rights and levels
   h) definition of cardholder escort requirements
   i) cardholder use limits

j) user definition of extended individual strike and door held open times
k) deactivation of credential following a period of non-use
l) furnishing and management of digital certificates for smart cards
m) searching for records and images based on any fields in the database

2) Field types: text, date, numeric, drop-down lists

b. Access Levels shall consist of a combination of readers and time zones.

1) Minimum number of supported access levels per controller: 32,000
2) Minimum number of supported access levels per badge: 255
3) Card readers shall be assignable to any or all access levels.
4) Each access levels shall have the option for “First Card Unlock”.
5) Temporary access levels – Within the constraint of number of access levels, the SMS shall have provision for access levels with definable start and end dates.
6) Precision access levels – Beyond the constraint of number of access levels, the SMS shall be able to assign access levels with unlimited card reader and time zone combinations.
7) Access Groups – The SMS shall provide for access groups, assignable to an alphanumeric name, containing up to 32 access levels.
8) Time zones – Pre-defined card reader settings shall have the flexibility to be overridden or modified for locking state and required authentication means.

c. Holidays shall be assignable via an embedded calendar with an alphanumeric name and to individual timezones.

1) Minimum number of holiday assignments: 255
2) Number of holiday group types: 8
3) Repeat frequency: annual
4) Daylight Savings Time: definable for automatic time conversion
5) Span: configurable for multiple days

d. Time zones
1) The SMS shall be capable of creating time zones, each with intervals assignable to any day of the week.
a) number of time zones: 255 minimum
b) Intervals: 6 minimum
2) Time zones shall be allowed to belong to any or all access levels so that the time zone only has to be defined once.

e. Scheduling - The SMS shall have a scheduling utility to allow System Administrators to schedule actions to occur on a one-time or a recurring basis and to maintain a log of actions executed.

f. Field Hardware
1) The SMS shall allow for a Windows-based configuration of the following types of field devices which participate in the access control function:
a) Intelligent System Controllers (ISC’s)
b) Input Control Modules (ICM’s)
c) Output Control Modules (OCM’s)
d) Access card readers
e) Integrated lock-readers
2) The SMS shall provide a device discovery utility to aid in configuration.
a) Scope: local subnet or multiple subnets

b) Display categories: brand, discovery service, device status, device type
c) Available functions: ping, reboot, default password check, version discovery, launch device web server, save credentials, update IP address. Functions depend upon specific capabilities within a device

3) When a field hardware device is configured, the device shall appear in a graphical system overview tree and be available in drop down lists which support operator access.
4) The SMS shall have the ability for bulk add, modify, and delete privileges for ISCs and card readers to allow for the ease of addition and maintenance of themes.
5) The System Administrator shall have the ability to group field devices into monitor zones.
6) System status update frequency shall be configurable.

g. Alarm Masking Groups - System Administrators shall be able to create groups of alarm inputs that enable them to mask or unmask multiple Input Control Module inputs and card reader inputs simultaneously.
1) Alarm Masking Groups shall be able to be masked or modified as a group or as individual points.
2) Alarm masking shall support two-man control.
3) Number of Alarm Masking Groups: maximum 64 per ISC
4) Alarm inputs: maximum 128 per Alarm Masking Group

h. Event Linkage – The SMS shall support a global linkage feature whereby any input or output or event shall be linked to any other input or output or event., with the following additional characteristics:
1) support global I/O function lists, consisting of sequences of up to six actions
2) association with panel areas

i. Graphical Maps - The SMS shall support graphical maps that display device or group status, function lists and video cameras dynamically in real-time, and support the following:
1) configuration to appear on command or when specified alarms are acknowledged
2) graphical map creation software that allows the import of map backgrounds from supported file formats: BMP, PD, DFX, DWG, EPS, IBM, FPX, TIFF, EMF, WMF, PNG, IOCA, JPEG, JIFIF, PNG.
3) associate various maps with each area to provide for the creation of a map hierarchy
4) user-defined text and icons
5) configuration of map icon shape and color to represent the state of the associated device

2. Badging – SMS badging functionality shall allow for the creation of different badge types based on a database field, the linking of that field to a badge type to automate the process of credential production, and the use of security colors, chromakey, and ghosting, to allow quick identification of personnel access authority.

a. The SMS shall have the ability to create and maintain badge designs, with tools and support for image import and export, ghosting, signature capture, bar code, and smart card chips.
1) Image formats: all standard industry image formats
2) Support image processing and effects with a pre-defined effects gallery.

3) A badge layout and creation module shall support custom badge designs by the User.

b. Additional badging related functionality shall include the following:
1) assignment of access levels and access groups, including bulk assignment, modification or deletion of access levels
2) custom badge layout
3) mobile and remote badging
4) printing: print limits, batch printing
5) magnetic stripe encoding using any of three tracks
6) support for all industry standard bar code formats

c. Credential images shall be digitized using industry standard JPEG image compression and printed using a high quality and direct card printing process.

d. The System Operator shall have the following functions available when enrolling cardholders: choose a badge type, select access levels, enter personal identification numbers (PIN), and/or any other user-defined fields.

e. A badge form shall keep a complete history of every badge that was assigned to the cardholder's record to include cardholder badge ID, issue code, badge type, badge status, activation and deactivation dates and times, PIN numbers, embossed numbers, and anti-passback information.

3. Ingress and Egress
a. Individual Use
1) Access Cards
a) Card types supported:
i. proximity – 30 mil thickness, ISO compliant
ii. smart cards – contact and contactless
- MIFARE – 1 kB (8 kb) and 4 kB (32 kb)
- DESfire
- HID iClass
- U.S. Government FIPS 201 and HSPD-12 compliant, including TWIC

iii. PIV standard formats
iv. Mobile Credentials to be installed and used from a smart phone

b) Data formats supported:
i. Magnetic stripe – with card number, facility code, and issue code combinations up to nine-digit card number and two-digit issue code
ii. Wiegand – all industry standard variations
iii. HID Corporate 1000 – 32 bit and 48 bit
iv. 200 bit BCD FASC-N output of FASC-N readers
v. 75-bit Wiegand Binary output of GSA approved FASC-N readers
vi. Custom

c) The SMS shall support the provisioning and usage of Mobile Credentials.
i. Mobile Credentialing shall be configurable from the SMS to include:
- name for the credential service
- URL for issuing credentials
- requirements for certificate based authentication and/or username password to access web portal

ii. Supported mobile credentials:

- Lenel – BlueDiamond
- HID
- Allegion

d) The SMS shall support desktop smart encoding and inline smart encoding for relevant affected reader technologies.
e) The SMS shall support a card reader cipher mode, emulating the presentation of a card credential by manually entering their badge ID.
f) The SMS shall support a configurable denied access attempts counter for each card reader.
g) Extended Held-Open Time – Authorized cardholders shall have the ability on demand to extend the time for which a door is help open after access is granted for up to 30 minutes.
h) An alarm shall be generated upon an attempt to use any badge that is not marked active in the SMS.

2) Biometrics shall provide multi-factor (or alternate) identification through the measurement and comparison of human characteristics including fingerprints, hand geometry, iris imaging, and facial features. The SMS shall have the capability to verify the identity of enrolled individuals using products from approved manufacturer partners.
a) Capture of biometric data (template) shall be accomplished via the biometric device or associated reader.
b) Cardholder biometric data (template) storage means: smart card; in access controller; in the biometric partner database.

3) Request to Exit (REX) - The SMS shall be able to provide an event when a REX is initiated.

4) The SMS provide the ability to alert the System Operator when a cardholder does not present their credential at a required location in a designated period of time.

5) Pre-Alarm - The SMS shall support a card reader pre-alarm feature which sounds a tone prior to a door held open alarm for a configurable period.
a) The SMS shall allow operator response instructions to be specified for each type of alarm and delivered via text and/or audio.

b. Area Control – The SMS shall implement area control implementing functionality affecting more than one person, and have the following elements:
1) Global and Local Hard Anti-passback
2) Global and local Soft Anti-passback
3) Timed Anti-passback
4) Two Person Control
5) Designated One Person Control
6) Designated Two Person Control
7) Tailgate Control
8) Occupancy Limit
9) Interlock group readers

c. Mustering - The SMS shall provide a mustering function to automatic register cardholders that are on site during an incident.
1) Muster Mode shall mean that an incident has occurred and an evacuation is required of one or more a Hazardous Locations.
a) Triggers
i. automatic: occurrence of a designated hardware event

ii. manual: by System Operator

b) Reset: manual by System Operator or Automatic based on Global I/O

2) Hazardous Location (s) shall be defined using entry and exit readers associated with the location.
   a) One or more safe locations shall be designated for each a Hazardous Location.
   b) Entry and exit card readers shall be provisioned at each portal with the requirement that a badge always be used to enter or exit Hazardous and Safe Locations.

3) Muster Alarm and Reporting
   a) When a Hazardous Location is in Muster Mode, all associated Alarm Monitoring Workstations shall be notified with a breakthrough notification and Muster Reporting shall be active.
   b) Live Muster Report
      i. display the last location of each cardholder based on card swipe.
      ii. activation:
         - immediately upon entering into Muster Mode
         - after a specified time period from Muster Mode activation
         - after the number of personnel in the Hazardous Location reaches a given count.
      iii. configurable for automatic refresh time and automatic end
   c) Muster Status Reporting: individual cardholders in Hazardous Location
   d) Live Hazardous Location and Safe Location Reports: cardholder listing and record selection
   e) Operator Display
      i. Hazardous Locations and Safe Locations shall be placed on graphical maps' System Hardware Status Tree as Area Icons with associated head counts.

4. Guard Tour
   a. A tour shall consist of a series of checkpoints that shall include card readers and/or alarm inputs.
   b. Each tour shall be assigned to one or more alarm monitoring Workstations indicating from where automatic tours are to be launched.
   c. Tour checkpoints shall be assigned minimum and maximum times within which to be reached.
   d. The SMS shall handle both scheduled and random tours.
      1) Scheduled tours shall have an Alarm Monitoring Window pre-departure notification.
   e. Tours will have the option of being linked to live video.
   f. Guard tours shall capable of being monitored through a tracking window including tour details and status.
   g. The SMS shall support aggregation of tours into tour groups.
5. Elevator - The SMS shall provide elevator control using standard access control field hardware that will permit the restriction of cardholder access to certain floors while also allowing general access to other floors, with the following additional functions:
   a. Allow, at the elevator, the use of any card reader and card reader modes used on any other card reader in the SMS
   b. Track which floor was selected by an individual cardholder for auditing and reporting purposes

c. Provide an option where the floors of a building are able to be configured into logically divided sections (floor groups) to prevent passenger requests between designated sections.

6. Field Devices
   a. Interface
      1) The SMS shall be equipped with the access control field hardware required to receive alarms and administer access granted or denied decisions.
      2) The SMS shall be capable of interfacing with the following **<categories of>** field devices:
         a) Controllers (ISC)
            i. LNL-X3300
         b) Intelligent Single Door Controller (ISDC)
            i. LNL-X2210
         c) Intelligent Dual Reader Controller (IDRC)
            i. LNL-X2220
         d) Advanced Dual Reader Controller(ADRC)
            i. LNL-X4420
         e) Input Control Module (ICM)
            i. LNL-1100-S3
         f) Output Control Module (OCM)
            i. LNL-1200-S3
         g) Single Reader Interface Module (SRI)
            i. LNL-1300-S3
         h) Dual Reader Interface Module (DRI)
            i. LNL-1320-S3
         i) Power over Ethernet (PoE) Enabled Door Controller
            i. LNL-1300e
         j) Wireless Gateway Interface
            i. PIM400-1501-KIT
         k) Communication Star Multiplexer
            i. LNL-8000
         l) Network ready power supplies and enclosures
         m) Intelligent and combination locks
      3) The SMS must be able to retrieve device serial numbers from field hardware, excluding card readers, biometric readers, and keypads.
   b. Data download
      1) The SMS shall provide for the downloading of data to the ISCs. Downloads shall load SMS information (timezones, access levels, alarm configurations, etc.) into the ISC's first, followed by cardholder information and card reader configurations.
      2) Information on cardholder status, badge status, timezones or access levels shall download in real time as they are added, modified, or deleted from the SMS.
   c. Permission control - The SMS shall allow System Administrators to set permission control for individual devices within a monitoring zone for command override.
   d. Device grouping – The SMS shall support device grouping for uniform command and control of groups of devices within the system.
   e. Card readers
      1) Options to include:
         a) User commands
         b) Door strike, REX and DPS functionality
         c) Duress actions
         d) Alarm masking
         e) Logging requirements

f) Selection as “In” or “Out” reader
g) Use limits

2) The SMS shall provide connectivity to, proximity/mobile ready, Smart Card and smart card/mobile ready readers which provide continuous supervision and monitoring of reader processor and wiring integrity by means of a non-proprietary communications protocol standard.
3) The SMS shall support encrypted reader to panel communications using the SIA OSDP Secure Channel protocol.

f. Input Control Modules (ICM’s) options to include:
1) Alarm masking
2) Local linkage of inputs and outputs
3) Output activation rules
4) Input configuration for Guard Tour
5) Entry (latched, not latched) and Exit delay modes

g. Intelligent System Controller (ISC) capabilities shall include:
1) Administrator functions to group, add, modify or delete ISC’s in the system
2) Ability to update firmware or replace hardware while maintaining complete hardware and data configuration settings
3) A distributed intelligence redundancy mode, whereby the ISC, configured with a UPS battery to maintain the unit for 24 hours, participates with other ISC's to provide complete control, operation and supervision of the system’s monitoring and control points in the event of SMS server failure.
a) cardholder capacity: configurable up to 1,000,000
b) event capacity: configurable up to 50,000

h. A system Operator shall have the option to manually control the output points or input points connected to the SMS.

i. The SMS shall support a real-time graphical system status tree or list window that graphically depicts configured field hardware devices.

7. Distributed Access Level Management
a. The SMS shall provide a browser-based interface for the assignment of access rights to individuals or groups of cardholders, using a simple user-interface paradigm suitable to general employee use, and not requiring specialized training on the SMS
b. The SMS administrator shall have the ability to designate for which areas a manager has assignment rights. These rights shall then be reflected in the browser interface accessible by the area manager, such that only areas for which they have authority are available for assignment.
c. The browser-based tool for access rights assignment by area managers shall have the ability to search for cardholders and to view cardholder details, constrained by the permissions of the manager

B. Alarm Monitoring - The SMS will provide the ability to monitor system and device Alarms/Events, Field Hardware Command and Control and Status Monitoring and system support functions, for the use of the operators of the system.
1. The SMS shall provide monitoring options thru workstations installed or browser-based clients.
2. An Alarm Monitoring window shall provide System Operators information about the time, location, and priority of an alarm and provide the ability to sort pending and new alarms based on event detail.
a. Detail shall include at a minimum: Date/Time, Description, Priority, Controller, Device, and person.
3. Alternate alarm view windows shall be available to support: Alarm or Badge Activity Monitoring, Event Tracing (Live/Historical), and Alarms Pending Response

a. Operators shall be able to acknowledge alarms from any alarm view window.

4. Monitor support shall include the ability to view live and recorded surveillance video and link video to alarm events.
5. Monitor support shall include options for comparison of the in-person cardholder to their stored image either in person or via live video. Cardholder Verification and Video Verification.
6. The SMS shall allow a System Operator to:
   a. monitor alarms in their assigned monitor zone and to perform field device control actions on specified devices in that zone from either thick client, web client or mobile client platform
   b. delete the alarm from the alarm monitoring window without acknowledging the alarm
   c. enter and edit an Acknowledgement note detailing the cause of specified alarms and the actions taken
   d. activate, deactivate, or pulse outputs configured and associated with a card reader
   e. mask or unmask each individual card reader door forced open alarms, door held open alarms, and associated auxiliary alarm inputs
   f. display a cardholder record with the stored cardholder's image
   g. verify that a person using a credential matches their stored photo
   h. open multiple cardholder verification windows to cover multiple readers at the same time
   i. initiate several traces of cardholders, assets, and/or field hardware devices while monitoring alarms
   j. initiate an historical trace for a device, specifying a date and time range
   k. filter alarms from the trace window to include access granted, access denied, system, duress, and area control alarms and by alarm source
   l. perform a trace on any ISC, ICM, Alarm Input, Credential, Intrusion Detection Device, Monitor Zone, or card reader
   m. manually override card readers, alarm points, and relay outputs
   n. combine, enable, or disable alarms for aggregation
   o. acknowledge or delete a group of aggregated alarms
   p. view runaway devices
7. System Administrators capabilities shall include:
   a. set permission control for individual devices within a monitoring zone for command override
   b. assign default monitor zones to monitoring workstations
   c. option to define monitor zones to include sub devices of an ISC
   d. configure how the SMS handles the annunciation of alarms on an individual alarm or event basis
   e. set display parameters for unacknowledged alarms
8. Notifications - Upon alarm, the SMS shall allow for:
   a. automated sending of texts or e-mail messages
   b. forwarding alarms to another location.
9. Annunciation - The System Administrator shall have the ability to configure how the SMS handles the annunciation of alarms on an individual basis.
   a. These attributes and actions shall be assignable on a 'global' basis to all devices that share an alarm description.
10. System Administrators shall be able to route and re-route device alarms and events to defined monitoring client workstations on the network, regardless of where the alarm is generated in the field.
11. A real-time graphical system status tree on the screen shall indicate the status of devices to reflect secured, unsecured, in alarm, or offline and provide command and control functions for authorized users.

12. Output control operations shall be available to lock, unlock or pulse control points.
13. An automatic cardholder call-up feature shall allow the quick search and display of images in the database.
14. Logging
    a. All alarms and events in the SMS shall, by default, always be recorded in the database.
        1) System Administrators shall have the ability to select on a time zone basis, the times required for the SMS to log specific events to the database.
        2) System Administrators shall have the option for Alarm or Events to be set to log or not to log particular alarms or events by individual reader or input.
    b. A System Operator journal shall be available to log important daily events.
15. A trace function shall be available for System Operators to locate and track activity on specific cardholders, assets, video cameras, or card readers. An image comparison feature must be provided for use in conjunction with a CCTV interface.
16. The SMS shall support a Test Mode for Alarm Inputs, Door Forced Open, and Access Grants to verify that all inputs within the group are operational.

C. Intrusion Detection
1. The intrusion detection function shall employ keypad used in conjunction with a card reader, both supplied from the Manufacturer. The LNL-CK Keypad is quired for this feature.
2. The Alarm Monitoring interface shall be able to control the intrusion detection function.
3. Intrusion zone point types:
    a. 24-hour point
    b. Interior point
    c. Perimeter point
4. Arming options:
    a. Exit delay
    b. Entry delay
    c. Forced
5. Actions under User command:
    a. Disarmed
    b. Disarmed Fault
    c. Armed Away
    d. Armed Stay
    e. Armed Instant
    f. Forced Armed Away
    g. Force Armed Stay
    h. Force Armed Instant
    i. Entry Delay
    j. Exit Delay
    k. Alarm
    l. After Alarm
    m. Chime
    n. Silence
6. System Administrators shall have the ability to define Alarm Mask Groups for sets of points to be treated as an intrusion area.
    a. Indication of events from these points shall be masked (disarmed) or unmasked (armed).

7. The SMS shall support Intrusion Mask Groups to contain individually configured intrusion points and to have the capability reporting of arming mode and state for the group.
8. Alarms shall be reported for the intrusion mask group by the SMS based on the current arming mode and state of the intrusion mask group.

D. Visitor Management System

1. The SMS shall have an integral Visitor Management traditional client or browser-based client to provide the following functionality:
   a. Allow an operator to enroll, schedule, assign to an employee, capture photos, capture signature, assign access levels, sign in or out, and track visitors as they move throughout the facilities
   b. Support for enrollment at a desktop computer, portable computer, or mobile device
   c. Provide visitor data and image capture / import capability as well as image edits using pre-defined effects, Chroma key (background transparency) and aspect ratio settings
   d. Allow for re-assignable badges and sticker badges
   e. Provision visitor credentials and maintain visitor data, including credentials and visit history, in the SMS database to minimize re-entry of data.
   f. Search for records and images using any fields in the database relevant to them.
   g. Assign visitors to existing valid cardholders with email notification
   h. Pre-schedule visits/events
   i. Visitor sign-in and sign-out at a desktop computer, portable computer, or a tablet
2. The system shall support the use of a browser-based self-service portal to create a Visit Event that will include the visitor(s) record creation or modification.
   a. Any cardholder with permissions shall be able to create a visit using a self-service portal to self-enroll visitors and create/manage events.
   b. The Host application shall allow any Cardholder with appropriate permissions to use their Directory Account to log in and create the Event/Visit record to include:
      1) Visitor Name, email, phone and other personal information
      2) Purpose
      3) Sign-in location
3. The Visitor Management System shall provide a visit status user interface to include:
   a. in-progress visits, including overstayed visits
   b. pending visits, including late visitors
   c. completed visits
4. Self-Service app
   a. The Visitor Management System shall have a self-service iPad-based visitor app which allows visitors to:
      1) sign themselves into or out of events without assistance from a front desk attendant
      2) sign in/sign out a pre-registered visit or a “walk-up” visit
      3) update personal information (including photo capture)
      4) view and complete pre-recorded video content during the sign-in process (example: safety or security procedures or guidelines)
      5) sign or accept up to five documents (example: non-disclosure agreements)
      6) print an adhesive-backed paper badge with latest photo and other pertinent information via supported printer devices
   b. Allow for customizations related to end-user branding (logos or colors) to facilitate inclusion in the environment

c. Upon Sign In and Sign Out, an email, which can include a captured image of the visitor, shall be sent to notify host and security personnel of a signed in or signed out visitor.

d. Administration of the self-service app shall allow for custom configurations of

1) App Theme Color, Logos, and custom messages to be defined by customer
2) Required documents (up to 5) such as a Non-Disclosure Agreement (NDA) or Privacy Agreement and associated acceptance and signature requirements
   a) Such documents shall be available records stored in the database.
   b) An Administrator set the renewal period for updating a photo, required signed or completed documentation based on Visit Type
3) The administrator may also save a VSS image or “Pre-Set” of a configured VSS iPad and store it into the SMS database.
   a) When new Check In locations are created, the user may download the image or Preset that is stored in the SMS database

e. Visitor self-service application must be a native iOS application that automatically launches on iPad startup, and cannot be terminated or exited by the visitor

E. Third Party Application Programming Interface (API)

1. Software Integrations

a. Software integrations shall be based upon a RESTful Web Services API.

b. Access control integrations shall provide for the following functionality:

1) Full Alarm Management - Send and Receive and Acknowledge alarms
2) Full identity/card management (add/modify/delete) identities, cards, visitors, access permissions, etc.
3) Main command and control operations including – Set Reader modes
4) Add/modify/delete of operator/user permissions of the system
5) Access to device and other security system configuration (e.g. panels, readers, segments, badge types, etc.)
6) API support for the same functions as used by manufacturer’s browser clients, such that it is possible to implement the same features and functions as the manufacturer, but in custom applications or integrations.

2. Hardware Integrations

a. Hardware integration shall be based upon native API plug-ins that allow for 3rd parties to map their hardware into the access system to extend the supported device set including but not limited to, Fire, Intrusion, Intercom, Video, Cameras, Readers, etc.

b. Integration shall provide full support for alarms, hardware status, and command and control for integrating third-party devices into the alarm monitoring software

c. Video integration shall allow for both third-party video to be integrated into the SMS as well as SMS video to be accessed by a third-party

F. Video

1. Integrated Video Management System (VMS)

a. An integral VMS shall provide video response options upon alarm events to include:

1) auto-launch
2) change camera resolution and/or frame rate
3) activation and positioning of PTZ camera
4) event monitoring
5) display of alarm location on multimedia graphical maps
6) event investigation
7) automatic archive of event video for selected alarm types

b. Further capabilities:

1) export of security evidence clips in industry standard formats
2) switching between live and recorded video
3) 2-way audio support
4) search recorded video by specific badge or alarm point
5) operation using same user SMS authenticated credentials

2. Integrated Network Video Recorder

a. Supported resolutions: QVGA (320 x 240) to 20 Megapixel (5472x3648)

b. Recording modes: continuous, time-lapse, event-driven, synchronized audio and video

c. Storage options: Direct Attached Storage (DAS), Network Attached Storage (NAS), and Storage Area Networks (SAN).

2.05 COMMUNICATIONS

A. The SMS shall communicate with the ISCs via TCP/IP through IPv4 or IPv6 protocols.

B. Download communication between the SMS and the ISC shall be fully multi-tasking and shall not interfere with operational functions.

C. Upon loss of communications between the SMS Server and an ISC, an alarm shall be created with a time stamp.

1. Upon re-established communication, the SMS and the ISC shall automatically re-synchronize from the point of communication loss without operator intervention.

2. The SMS shall support Dual Path communications between the SMS Server and the ISC's to allow for a fully functional redundant communication path.

a. During a fail over period, the ISC shall periodically check to see if the primary path has been re-established and will automatically switch back upon a successful connection.

b. Alarms shall be generated upon loss or restoration of communications.

D. Encryption – The SMS shall provide encrypted communication capabilities as follows:

1. Credentials to Reader: DESFire EV1 or EV2, or HID iCLASS or SEOS

2. Reader to Downstream Panels: OSDP Secure Channel Encryption

3. Downstream Panels to ISC: AES-128 bit or AES-256 bit

4. Data on ISC AES-256 bit Encryption of Data at Rest

5. ISC to SMS Server: AES-128 bit or TLS1.2 with AES-256 bit

6. SMS Server to Client: HTTPS

7. Client to Printers and Badge Encoders: Encrypted encoder communications

2.06 SYSTEM MANAGEMENT

A. System Configuration - The SMS shall provide system icons and/or menu selections for each function requiring configuration of SMS options or peripherals including client workstations, field hardware, network functions, communications, and reports.

1. A set-up assistant utility shall be available for the initial system configuration prior to first log in.

2. The SMS shall support configuration setup wizards to guide System Administrators through the configuration of the access control module of the system.

B. In addition to capabilities previously mentioned herein, System Administration capability shall include the following:

1. Customize cardholder, asset, and visitor forms.

2. Import customized map backgrounds and custom icons

3. Bulk delete cardholder records

4. Limit System Operator functions and actions, including searching the database

5. Configure client workstation applications and settings

6. Assign System Operator passwords, log on credentials and permissions and provide operator history

C. The SMS shall provide support for single sign-on capability, whereby System Administrators or System Operators may authenticate into SMS applications using their Windows domain account.

D. System Administrative tasks including defining client workstation and Operator permissions, access groups, time zones, reports, and maps shall be available from any client workstation on the network.

E. Graphical Features

1. The SMS shall display a graphical representation of configured field hardware (including ISCs, fire panels, intrusion detection devices, personal safety devices, intercom systems, and Central Station alarm receivers), digital video hardware, access levels, time zones, access groups, holidays, and card formats.

2. System Administrators shall be able to modify a device that is depicted on the graphical system overview tree or see its properties by double-clicking on the related icon, causing the SMS to bring them to the appropriate form.

F. The SMS shall provide context-sensitive help files to guide System Administrators and System Operators in configuration and operation.

G. Logging - The SMS shall provide full System Operator activity tracking/logging of critical keyboard functions to include date/time, Operator, activity program, function, and database changes.

1. System Operator functions to log shall include System Operator login and System Operator logout; Additions, Changes, and Deletions to Cardholder Management; New Badge, Print Badge, and Update Badge.

2. Configuration changes to log shall include all functional modules within the SMS.

3. The SMS shall log activity of System Operators performing SMS alarm monitoring including alarms acknowledged, alarms cleared, output control activity, trace, and other functions.

H. Reporting – The SMS shall have a rich reporting function, storing its reports in the database and viewable from any client workstation with permissions.

I. Reporting Output -- The SMS reporting output options shall include:

1. Access Denials and Grants by Reader Report

2. Access Denials, Grants, and Other Badge Events Report

3. Access Denied Event Report

4. Access Denied Events, by Reader

5. Access Granted Events Report

6. Access Granted Events by Reader Report

7. Access Groups Report

8. Access Groups with Levels Report

9. Access Level Assignments to Cardholders Report

10. Access Levels Assignment to Cardholders, By Segment Report

11. Access Levels Report

12. Access Panels Report

13. Active Visits by Cardholder Name Report

14. Active Visits by Host Name Report

15. Active Visits by Visitor Name Report

16. Alarm Acknowledgments Report

17. Alarm Acknowledgements by Definition Report

18. Alarm Acknowledgments by System Operator Report

19. Alarm Acknowledgements by Panel Report
20. Alarm Configuration Report
21. Alarm Input Events Report
22. Alarm Panel Inputs Report
23. Alarm Panel Local Linkage Report
24. Alarm Panel Outputs Report
25. Alarm Panels Report
26. All Cardholders with Logical Access Report
27. All Events Over Time Report
28. All Events Over Time with Local Panel Time Report
29. All Events Over Time with Unique Alarm ID Report
30. Anti-Passback Events Report
31. Area Anti-Passback Configuration Report
32. Area Configuration Report
33. Area Entrance History Report
34. Asset Classes Report
35. Asset Events Report
36. Asset Groups Report
37. Asset Types Report
38. Assets by Scan ID Report
39. Assets by Type Report
40. Assigned Assets by Cardholder Report
41. Assigned Assets by Scan ID Report
42. Assigned Assets by Type, Scan ID Report
43. Audio Notifications and Instructions Report
44. Badge Type Configuration
45. Badges by Deactivation Date Report
46. Badges Without Access Levels Report

47. Card Formats Report
48. Cardholders Access to Readers Report
49. Cardholder Exit or Entry Report
50. Cardholder Photo Gallery Report
51. Cardholder Time and Attendance Report
52. Cardholders by Badge Type Report
53. Cardholders by Last Name Report
54. Cardholders Located in Each APB Area by Date Report
55. Cardholders Located in Each APB Area by Name Report
56. Cardholders with Access, by Badge Type Report
57. Cardholders with Access by Last Name Report
58. CCTV Instructions Report
59. Continuous Video Report
60. Current Visits Report
61. Destination Assurance Configuration Report
62. Destination Assurance Exempt Cardholders Report
63. Device Status Events Report
64. Dialup Events by Panel Report
65. Dialup Last Connect Time Report
66. Elevator Access Denials and Grants Report
67. Elevator Dispatching Devices and Terminals Report
68. Emergency Events Report
69. Event Codes Report
70. Event Count by Panel Report
71. Fire Device Input or Output Report
72. Global APB or MobileVerify Occupancy by Date Report
73. Global APB or MobileVerify Occupancy by Name Report
74. Global I/O Linkages Report

75. Guard Tour Configuration Report
76. Guard Tour History Report
77. Hardware Panels Report
78. Holidays Report:
79. The Holidays Report shall provide information on all system holiday definitions.
80. ILS Lock Authorizations by Cardholder Report
81. ILS Lock Authorizations by Level Report:
82. ILS Lock Battery Status by Status:
83. ILS Lock Characteristics Report:
84. ILS Lock Communications Report
85. ILS Lock Ownership Report
86. Intercom Functions Report
87. Intercom Stations Report
88. Intrusion Command Authority – Advanced Report
89. Intrusion Command Authority – Global Report
90. Intrusion Command Events Report
91. Intrusion Detection Areas Report
92. Intrusion Detection Devices Report
93. Intrusion Panel User Groups Report
94. Last Location of Cardholders Report
95. Locked Video Events Report
96. Maps Report
97. Mobile Verify User Transaction Log Report
98. Mobile Verify User Transaction Log by Operation Report
99. Mobile Verify User Transaction Log by User ID Report
100. Module Details Report
101. Module Summary Report
102. Monitor Stations Report

103. Monitor Zones Report

104. Panels Report

105. Overdue Visits Report:

106. Overstayed Visits Report:

107. Permission Profiles Report:

108. Personal Safety Transmitter Assignments Report:

109. Personal Safety Transmitters Report:

110. Personnel in the Database Report:

111. Personnel Without an Active Badge Report:

112. Personnel with Organizational Details Report:

113. Personnel with Personal Details Report:

114. Point of Sale Registers Report:

115. Precision Access Groups Report:

116. Reader Assignment to Cardholders Report:

117. Reader Command Programming Configuration Report:

118. Reader Status Events Report:

119. Reader Time Zone Schedules Report:

120. Readers Report:

121. Receiver Account Alarm Activity Report:

122. Receiver Account Areas Report:

123. Receiver Account Groups Report:

124. Receiver Account Zones Report:

125. Receiver Accounts Report:

126. Receiver Accounts that Failed to Report:

127. Receiver and Receiver Account Events Report:

128. Segment Badge Download Summary Report:

129. Segments Report:

130. SNMP Agents Report:

131. SNMP Management Information Base Configuration:

132. System Servers Report:

133. Text Instructions Report:

134. Time Zones Report:

135. User Permissions Report:

136. User Transaction Log Report:

137. User Transaction Log by User ID Report:

138. Users with Area Access Levels to Manage Report:

139. Video Cameras Device Links Report:

140. Video Cameras Report:

141. Video Events Report:

142. Video Servers Report:

143. Visits History Report:

144. Visitors Report:

145. Windows Event Log Errors Report:

J. The SMS shall provide an ad hoc customized report generator, allowing the creation of reports using the relational database structure.

K. The SMS shall support an industry standard, off the shelf, custom report writer.

L. Archiving - The SMS shall allow System Administrators to archive offline history files. Offline files shall include access events and System Operator transactions that have been purged from the reportable database.

2.07 HARDWARE REQUIREMENTS

A. The Manufacturer shall publish a summary of recommended server hardware to accommodate the performance requirements of the SMS server software.

B. The SMS server software shall be capable of running in a virtual or cloud environment. Upgrading current server software not in this RTC scope.

PART 3 EXECUTION

3.01 INSTALLERS

A. Contractor installation personnel shall be trained and certified by the SMS manufacturer and have a valid, current certification at the time of installation. With as minimum of two (2) locally dispatchable and trained technicians.

B. Contractor installation personnel shall comply with all applicable state and local licensing requirements.

3.02 PREPARATION

A. The network design and configuration shall be verified for compatibility and performance with the SMS.

B. The network configuration shall be tested and qualified by the Contractor prior to system installation.

C. Server performance parameters shall be compared with Manufacturer requirements for the SMS.

3.03 INSTALLATION

A. Contractor shall follow manufacturer published installation and configuration instructions and guidelines.

B. System shall be configured in accordance with manufacturer-supplied hardening guide. SMS systems for which the manufacturer does not provide a hardening guide shall not be acceptable.

3.04 STORAGE

A. Server and system hardware devices and components shall be stored in an environment where temperature and humidity are in the range specified by the Manufacturer.

SECTION 281500 - ELECTRONIC SYSTEMS AND COMPONENTS

PART 1 GENERAL

1.01 RELATED DOCUMENTS

A. Drawings and general provisions of the Contract, including General and Supplementary Conditions and other specifications, apply to this Section.

1.02 SUMMARY

A. Related Sections:

1. 280500 Electronic Systems General Requirements
2. 280513 Conductors and Cables
3. 280514 Fiber Optics
4. 281300 Access Control System
5. 281500 Electronic Components
6. 282300 Video Surveillance (CCTV) System

B. Section Includes

1. Door/Gate Monitoring and Control
2. Power Supplies (24 VDC, UPS)
3. Uninterruptible Power Supply (UPS)
4. Terminal Blocks, Fuses, and Snubbers
5. Relays
6. Security Screws
7. Tone Generators
8. Call Made Light
9. Intercom Pedestal
10. Camera Pedestal

1.03 SYSTEM DESCRIPTION

A. Door/Gate Position Alarm Monitoring

1. Provide low voltage power to door/gate position and latch monitoring switches as indicated on the Drawings. All door position and bolt monitoring switches at each door are to be connected in series such that an open at any one (1) of the switch contacts

shall break the circuit to the control electronics and provide an unsecured door indication on the designated operator interface. Losing the indicating signal power by cutting the circuit (circuit failure) shall also initiate an unsecured door.

B. Door/Gate Remote Control

1. Provide remotely controlled operating power to all electric locks, deadbolt locks, electro-mechanical locks, electric deadbolts and door/gate operating devices as indicated on the Drawings.

C. Power Supplies

1. Provide power supplies as required for each system.

2. Low voltage systems shall operate on 24 VDC or 24 VAC or as determined by each section. Size all power supplies to maintain Class 2 ratings and operation of each system at 150% of the maximum loaded condition.

3. Unless otherwise indicated, 24 volt door hardware including locks, strikes, and latches shall be supplied by external power supplies with over-voltage and short circuit protection.

4. Acceptable products: Power One, Lamda, or approved equal from other manufacturers.

D. Uninterruptible Power Supplies (UPS)

1. Provide UPS back up for all Security Electronics, and computer CPU's where shown on the drawings.

2. Size the security equipment UPS with sufficient capacity to support and maintain all added security equipment and devices for a minimum of 15 minutes after the loss of power. Provide (1) UPS per group per group of racks in the Security Electronics Room.

3. Size the radio equipment UPS with sufficient capacity to support and maintain all devices for a minimum of 2 hours after the loss of power.

4. Submit UPS power calculations indicating power consumption by each major equipment component.

E. Terminal blocks, Fuses and Snubbers

1. Provide DIN mounted terminal blocks for field and miscellaneous wiring.

2. Provide fused terminal blocks for power distribution circuit protection.

3. Provide circuit snubbers at all electric strike door locks for electromagnetic field (EMF) protection.

F. Relays

1. Provide relays for use as interposing relays, timer relays, audio relay, one shots, or other applications as shown on plans.

2. Provide EMF circuit protection diode across all relay coils.

G. Security Screws:

1. Submit various types of security screws for approval.

2. Screws shall be suitable for outdoor locations.

H. Tone Generators

1. Provide 24 VDC solid state piezoelectric alarms.

2. Provide one tone generator for each tone or a multi-tone unit. Provide a tone generator for each tone required at each control panel Refer to the Software Development Section for tone types.

I. Call Made Light

1. Provide an amber light at each intercom pedestal which will illuminate when the loop detector is activated.

J. Intercom Pedestal

1. Provide a pedestal for the card reader and intercom where shown on the drawings.

K. Camera Pedestal

1. Provide a custom pedestal for the license plate reader camera where shown on drawings. Custom pedestals shall be submitted and approved prior to purchase and field installation.

L. Provide all necessary interconnecting wiring and terminations including, but not limited to, junction boxes, terminal strips, lead wires, internal contacts, connectors, etc., from new or existing terminations to the new terminations in the control electronics cabinets.

1.04 SUBMITTALS

A. Comply with Section 280500, General Requirements.

B. Calculations

1. DC power supply sizing.

2. AC power supply sizing.

3. UPS system load and battery sizing.

C. UPS installation drawings: Show UPS size and physical mounting. Design and show power source, and branch circuit and load wiring to/from UPS units.

1.05 QUALITY ASSURANCE

A. Comply with Section 280500, General Requirements.

1.06 EXTRA MATERIALS

A. Deliver the following spare parts:

1.	DC power supply	1 ea. size used.
2.	AC power supply	1 ea size used.
3.	Relays	5 ea type used.
4.	Tone Generators	5 ea type used.

PART 2 PRODUCTS

2.01 ACCEPTABLE PRODUCTS

A. Provide equipment and components including but not limited to the following or approved equal from other manufactures. All products shall have the features described herein. The materials listed below establish the minimum quality and standards that are to be met:

1.	Power Supplies	Altronix, LifeSaftey Power
2.	Uninterruptible Power Supplies	APC, Best
3.	Electrical Relays	IDEC RU Series
4.	Audio Relays	IDEC RY2S Series
5.	Fuses	Phoenix, Entrelec
6.	Snubbers	Square D, Rifa
7.	Terminal Blocks	Phoenix, Entrelec
8.	Tone Generators	Floyd Bell (Columbus, OH)
9.	Call Made	Industrial Traffic Solutions
10.	Pedestal	Talk-A-Phone ETP-PM, Custom

2.02 POWER SUPPLIES

A. DC and AC Power Supplies

1. Power supply outputs to integrated circuit devices shall be regulated to within +/- one percent of the rated voltage output

2. Size as required for each location with a capacity of 150 percent of the intended maximum load.

3. Class 2 power supplies shall be power limited to 100 watts with over-voltage and short circuit protection.

4. Where required provide power supply with battery backup. The power supply shall include battery-charging circuit, power loss switching circuit, low battery, trouble and power loss output contact. Size battery to accommodate calculated load for the specified time period.

2.03 UNINTERRUPTIBLE POWER SUPPLIES (UPS)

A. Provide solid state inverter/charger and static bypass switch with less than 1/4 cycle, static transfer time, and frequency stability of 60 Hz + 1 Hz, voltage regulation of +8%, total harmonic distortion less than 5% and minimum output capacity and voltage as indicated in the drawings.

B. Provide sealed lead/acid type batteries.

C. Acceptable products: TOPAZ, BEST, Exide, or approved equal from other manufacturers.

D. Contractor is to provide battery backup to AC Control Panels, only.

2.04 ELECTRICAL RELAYS

A. Rate relays appropriate for the application or as shown on plans.

B. Provide relay sockets for ease of replacement.

C. Provide mounting hardware (i.e. bracket, DIN rail, etc.) unless otherwise noted.

2.05 AUDIO RELAYS

A. The audio switching relays shall connect intercom stations to intercom amplifiers.

B. Relay switch contacts shall be DTDT bifurcated gold plated contacts, rated for 2 amperes inductive and operate on 24 volts DC.

C. The relays shall be rated for at least 1 million operations.

D. The relays shall be removable socket mounted on DIN rail. All field terminations shall be landed on screw terminals rated to accommodate the required field wires.

E. Provide mounting hardware (i.e. bracket for rack mount, DIN rail, etc.) unless otherwise noted.

2.06 TONE GENERATORS

A. Solid State Piezoelectric

B. Screw or quick connect terminals.

2.07 CALL MADE LIGHTS

A. Provide waterproof polycarbonate housing

B. LED light source.

C. View angle shall not be less than 30 degrees.

D. Operating temperature shall be between 0 deg F to 165 deg F.

E. Provide a custom modified pedestal and faceplate to mount intercom station, camera and card reader where shown on the drawings.

F. Provide 1/4 inch thick steel construction with multi-coat rust inhibiting coating.

G. Color to be selected by Owner.

2.08 SOURCE QUALITY CONTROL

A. Comply with Section 280500, General Requirements.

B. Provide components as required for Shop Testing and Demonstration

PART 3 EXECUTION

3.01 INSTALLATION

A. Comply with Section 280500, General Requirements.

B. Comply with manufacturer's recommendations, procedures, and standards for each product.

C. All Class-1 wiring and their conduits shall only be routed to the designated Class-1 gutter or duct. All Class-2 wiring, unless otherwise noted, and their conduits shall only be routed to the designated Class-2 gutter or duct.

D. Provide sufficient quantity of power supplies of SNEC, Class 2 capacity, to power the associated equipment. Furnish power supplies with over voltage and short circuit protection.

E. Mount individual components to removable rear panels in wall-mounted cabinets using DIN rails, snap track or stand off-mounted PC boards, or properly sized mounting hardware.

F. Fuses: Provide over-current protection for control relay outputs and associated wiring.

3.02 WIRE AND CABLE INSTALLATION:

A. Comply with all specifications.

3.03 WIRE TERMINATION, DRESSING, AND IDENTIFICATION:

A. Comply with all specifications.

3.04 FIELD QUALITY CONTROL

A. Comply with Section 280500, General Requirements

3.05 TRAINING

A. Comply with Section 280500, General Requirements.

END OF SECTION

SECTION 28 23 00 - VIDEO SURVEILLANCE (CCTV) SYSTEM

PART 1 - GENERAL

1.01 DESCRIPTION

A. Provide and install a complete Video Surveillance System, which is identified as the Closed Circuit Television System hereinafter referred to as the CCTV System as specified in this section.

1.02 RELATED WORK/SECTION

A. For firestopping application and use latest code requirements.

B. For connection of high voltage use latest code requirements.

C. For access control, Section 28 13 00, PHYSICAL ACCESS CONTROL SYSTEMS (PACS).

D. For control and operation of all security systems, Section 28 13 00, ACCESS CONTROL SYSTEM AND DATABASE MANAGEMENT.

1.03 QUALITY ASSURANCE

A. The Contractor shall be responsible for providing, installing, integration and the operation of the CCTV System. The Contractor shall also provide certification as required.

B. The security system shall be installed and tested to ensure all components are fully compatible as a system and can be integrated with all associated security subsystems, whether the security system is stand-alone or a part of a complete Information Technology (IT) computer network.

C. The Contractor or security sub-contractor shall be a licensed security Contractor as required within the state or jurisdiction of where the installation work is being conducted.

1.04 SYSTEM DESCRIPTION (CONTRACTOR TO VERIFY SITE DETAILS)

A. Monitoring and Display System

1. Cameras mounted in security enclosures will be placed for general surveillance in critical and common areas, and will be automatically displayed upon motion detection and event call-ups via access controlled doors, door position monitoring alarms and duress alarms within field of view of associated cameras.

2. Cameras will be displayed as directed by the Owner.

3. Camera display functions at the noted locations will be programmable and controlled by software installed by the contractor.

4. System Components:

a. The system shall consist of, but not limited to, color cameras, manual lenses, camera enclosures, housing mounts, color monitors, video switcher, video multiplexers, power supplies, heaters and blowers, fiber receivers/transmitters, network switches, and all necessary interfacing components for a fully functional system.

5. Sequence of Operation:

   a. Indoor Fixed Cameras: Provide high resolution, color cameras with vari- focal, auto-iris lenses for general video surveillance coverage and continuous digital video recording. Cameras will have wide angle view to provide the intended coverage. The cameras and lenses will be installed in security smoked dome housings so that the direction of camera is concealed. Mounting types shall include ceiling, corner and wall as specified on the drawings.

   b. Outdoor Fixed Cameras: Provide low light, high resolution, color cameras with vari-focal, auto-iris lenses for general video surveillance coverage and continuous digital video recording. The cameras and lenses will be installed in environmental, security tinted dome housings. Provide all necessary sun- shields, heaters, blowers and weatherproof accessories for a complete installation.

   c. Alarm/Event Control: Perform camera call up by integrating with other security electronic systems described in the Specifications.

B. Network Video Recording System/Manager

   1. Video Recording Manager/recording equipment, distributed storage, existing system compatible iSCSI disk array will be provided for recording of selective cameras continuously. Based on 80% activity level, the system hard drive(s) shall have the capacity to store on-line full video of all cameras with recording resolution set at minimum 15 frames per second, 192 Kbps, and 4CIF for a minimum of 7 days. A DVD-RW drive will be provided for performing selective video event backup on removable media. Provide system software to playback recorded DVD video on PCs if necessary.

1.05 SUBMITTALS

A. Product Data: For each type of product indicated. Include rated capacities, operating characteristics, and furnished specialties and accessories. Reference each product to a location on Drawings.

B. Shop Drawings: Include plans, elevations, sections, details, and attachments to other work. As Built drawings as directed by the Owner.

C. Provide Samples as directed by the Owner.

D. Operation and Maintenance Data: For security system to include in emergency, operation, and maintenance manuals.

E. Provide certificates of compliance.

F. Provide manufacturer security system product cut-sheets. Submit for approval at least 30 days prior to commencement of formal testing, a Security System Operational Test Plan. Include procedures for operational testing of each component and security subsystem, to include performance of an integrated system test.

G. Submit manufacture’s certification of Underwriters Laboratories, Inc. (UL) listing as specified. Provide all maintenance and operating manuals.

H. Provide storage calculation for cameras and system.

I. Provide riser diagram for cameras and system.

1.06 APPLICABLE PUBLICATIONS

A. The publications listed below (including amendments, addenda, revisions, supplement, and errata) form a part of this specification to the extent referenced. The publications are referenced in the text by the basic designation only.

B. American National Standards Institute (ANSI)/Electronic Industries Alliance (EIA):
330 ..... Electrical Performance Standards for CCTV Cameras
375A ..... Electrical Performance Standards for CCTV Monitors

C. Institute of Electrical and Electronics Engineers (IEEE):
C62.41 ..... IEEE Recommended Practice on Surge Voltages in Low- Voltage AC Power Circuits
802.3af..... Power over Ethernet Standard

D. National Electrical Contractors Association (NECA):
303-2005 ..... Installing Closed Circuit Television (CCTV) Systems

E. National Fire Protection Association (NFPA):
70-05 ..... Article 780-National Electrical Code

F. Federal Information Processing Standard (FIPS):
140-2 ..... Security Requirements for Cryptographic Modules

G. Underwriters Laboratories, Inc. (UL):
983-06 ..... Standard for Surveillance Camera Units
3044-01 ..... Standard for Surveillance Closed Circuit Television Equipment

1.07 WARRANTY/AGREEMENTS/LICENSES

A. Provide as a minimum a 60 month (5 years) parts and labor warranty on all CCTV components and systems installed.

B. Provide operator workstation licenses for this project, contractor shall verify the number of work stations with owner prior to bid. This operator workstation licenses shall be used as identified by the Owner and the licenses shall include five years of renewal at no cost to the Owner and shall be turned over to the Owner prior to Substantial Completion. Provide license costs for these licenses for the 60 month (5 Years) period as noted above. RTC will be provided all OS licenses and the RTC will be performing all upgrades.

1.08 COORDINATION

A. Coordinate with the Owner exact mounting location of all cameras prior to installation.

B. Demonstrate to the Owner camera field of views using variable focal lens at each camera location prior to installation. Select and obtain approval of proper lens size or focal setting at each camera location to provide the required video coverage. If the desired view or coverage is unobtainable due to physical obstructions or limitation of lens, perform minor adjustment of the camera physical location at no additional cost to the Owner.

1.09 QUALITY ASSURANCE

A. SNEC Compliance: Comply with applicable requirements.

1.01 EXTRA MATERIALS

A. Provide to the Owner prior to Substantial Completion the following:

1. Camera…….1 of each type

2. Camera Lens……...1 of each type

3. Camera Heater/Blower……..1 of each type

PART 2 - PRODUCTS

2.01 MANUFACTURERS

A. Subject to compliance with requirements, provide video surveillance system equipment and components including, but not limited to, the following specifications and minimum requirements.

B. All equipment shall be from like manufacturers to provide a complete solution.

2.02 360º PTZ NETWORK CAMERA

A. Full 360º overview with one-click PTZ Control

B. Compatible with other PTZ Network cameras

C. Exchangeable M12 Lenses

D. Flexible camera heads with tilt functionality.

E. Lens

1. Fixed focus, Fixed Iris, F2.0, Focal Length: 1.37mm

2. Horizontal Field of View Default Mode: (4:3): 113º

3. Horizontal Field of View: (16:9) 152º

4. Vertical Field of View: (4:3 and 16:9) 85º

5. Light Sensitivity: Color 0.3 lux, F2.0

6. Shutter Time: 1/45500 s to 4 s

F. Camera Angle Adjustment

1. Pan 4 x 90º

2. Tilt -10º to -75º

3. Pan/Tilt/Zoom: Remote Gatekeeper, One-Click PTZ Control

G. Video Compression

1. H.264 (MPEG-4 Part 10/AVC) Baseline, Main and High Profiles Motion JPEG.

H. Resolution

1. Standard Lenses: 4x1280x720 (HDTV 720p) to 320x180
2. Default: 960x720
3. Quad View: 1920x1440 (4:3) to 320x180
4. Optional Lenses: 4x1920x1080 (HDTV 1080p) to 480x270
5. Default: 960x720

I. Frame Rate

1. Up to 25/30 fps (50/60 Hz) at 720p
2. Up to 12.5/15 fps (50/60 Hz) at 1080p

J. Video Streaming

1. Multiple, individually configurable streams in H.264 and Motion JPEG.
2. Controllable Frame Rate and Bandwidth

K. Image Settings

1. Resolution, compression, color level, brightness, sharpness, contrast, white balance, exposure value, exposure control, automatic backlight compensation, exposure zones, shutter and gain fine tuning of behavior at normal and low light, privacy masks (maximum 4 per channel).

L. Network Security

1. Password protection, IP address filtering, HTTPS encryption, IEE 802.1X network access control, Digest authentication, User Access Log, Centralized Certificate Management.

M. Event Triggers

1. Detectors: Live Stream Accessed, Shock Detection, Tampering.
2. Hardware: Fan, Network, Temperature
3. Input Signal: Manual Trigger, Virtual Input
4. Storage: Disruption, Recording
5. System: System Ready

N. Casing

1. IP66- and NEMA 4x-rated, die casted aluminum, polycarbonate dome.

O. Memory

1. 1 GB RAM, 256 MB Flash

P. Storage

1. Support for SD/SDHC/SDXC Card

2. SD Card Encryption

3. Support for Recording to network-attached storage (NAS).

2.03 HIGH SPEED PTZ WITH INSTANT LASER FOCUS PTZ (P) AND 360 (P)

A. The compact, outdoor ready camera features a built-in laser that provides instant focus in challenging lighting conditions and in complete darkness.

B. Top performance HDTV 1080p Video at 25/30 fps, with 30x optical zoom.

C. Camera

1. 1 / 2.8” Progressive scan CMOS.

2. 4.3-129mm, F1.6-4.7

3. Horizontal Field of View: 66.7º-2.36º

4. Vertical Field of View: 39.5º-1.37º

5. Laser focus, auto-iris.

6. Automatically removable infrared-cut filter.

7. Shutter time: 1/60000s to 2s

8. Minimum Illumination

a. Color 0.15 lux at 30 IRE, F1.6

b. B/W: 0.01 lux at 30 IRE, F1.6

c. Color: 0.2 lux at 50 IRE, F1.6

d. B/W: 0.02 lux at 50 IRE, F1.6

9. Pan/Tilt/Zoom

a. Pan: 360º endless, 0.05º-700º/s b. Tilt: +20 to -90º, 0.05º-500º/s

b. Zoom: 30x optical, 12x digital, total 360x zoom

c. Nair flip, 256 preset positions, tour recording, guard tour, control queue, on- screen directional indicator, set new pan 0º, adjustable zoom speed, speed dry.

D. Video

1. Video Compression

a. H.264 (MPEG-4 Part 10/AVC) Baseline, Main and High Profiles Motion JPEG.

2. Resolution

a. 1920x1080p (HDTV 1080p) to 320x180

3. Frame Rate

a. Up to 25/30 fps (50/60 Hz) in 1080p

b. Up to 50/60 fps (50/60 Hz) in 720p

4. Video Streaming

a. Multiple, Individually configurable streams in H.264 and Motion JPEG.
b. Controllable Frame rate and Bandwidth

5. Image Settings

a. Compression, color, brightness, sharpness, white balance, exposure control, exposure zones, rotation, fine tuning of behavior at low light, electronic image stabilization (EIS), manual shutter time, text and image overlay, image freeze on PTZ contrast, local contrast, automatic backlight compensation, autofocus, WDR – forensic capture, 120 dB. 32 individual 3D privacy masks.

E. Network

1. Security

a. Password Protection, IP Address filtering, HTPS encryption, IEEE 802.1X, network access control, digest authentication, user access log, brute force delay protection.

F. System Integration

1. Event Triggers

a. Detectors: Live Stream Accessed, Motion Detection, Shock Detection, Day/Night Mode.

b. Hardware: Network, Temperature, Fan

c. Input Signal: Manual Trigger, Virtual Inputs.

d. PTZ: Auto-Tracking, Error, Moving, Preset Reached, Ready

e. Storage: Disruption, Recording.

f. System: System Ready

g. Time: Recurrence, Use Schedule.

2. Event Actions

a. Record Video: SD card and Network Share

b. Pre and Post Alarm Video or Image Buffering for Recording or Upload

c. Upload of Images or Video Clips: FTP, SFTP, HTTP, HTPS, Network Share and Email.

d. Notification: Email, HTTP, HTTPS, TCP and SNMP Trap

e. PTZ: PTZ Preset, Guard Tour, Auto-tracking

f. Overlay: Text, Day/Night Mode

g. WDR Mode

3. Data Streaming

a. Event Data

4. Built-In Installation Aids

a. Pixel Counter

G. General

1. Casing

a. IK08, IK10 Housing and Mounting, IP66 and NEMA 4X Rated Re-paintable metal casing (aluminum), hard coated Polycarbonate (PC) clear dome.

2. Sustainability

a. PVC Free

3. Memory

a. 512 MB RAM, 256 MB Flash

4. Power

a. High PoE Midspan

b. Typical 11 W, Maximum 51W

c. IEE 802.3at Type 2 Class 4

5. Connectors

a. RJ45 10BASE-T/100BASE-TX

b. RJ Push-pull connector

6. Storage

a. Support for SD/SDHC/SDXC Card

b. Support for SD Card Encryption

c. Support for Record to Network Attached Storage

7. Operating Conditions

a. With 30W midspan: -4ºF-122ºF

b. With 60W midspan: -67ºF-122ºF

c. Maximum Temperature (intermittent) 140ºF

d. Arctic Temperature Control: -40ºF

e. Humidity 10-100% RH (condensing)

8. Storage

Conditions a. -

40ºF-158ºF

9. Approvals

a. EMC

b. EN 55022 Class A, EN 55024, EN 50121-4, IEC 62236-4

c. EN61000-3-2, EN6100-3-3, EN6100-6-1, EN61000-6-2, FCC Part 15 Subpart B Class A, ICES-003 Class A, VCCI Class A, RCM AS/NZS CISPR22 Class A.

d. KCC KN32 Class A, KN35

e. Safety – IEC/EN/UL 62368-1, IEC/EN/UL 60950-22, Laser Safety Regulations IEC/EN 60825-1 Class 1 ED. 3 (2014)

f. Environment- IEC/EN 62262 IK08, IEC/EN 60529 IP66, NEMA 250 Type 4X, IEC 60068-2-1, IEC 60068-2-2, IEC 60068-2-6, IEC 60068-2-14, IEC 60068- 2-27, IEC 60068-2-30, IEC 60068-2-78, ISO4892-2.

g. Midspan EN 60950-1, GS, UL, cUL, CE, FCC, VCCI, CB, KCC, UL-AR Network.

h. NIST SP500-267

2.04 2.0 OUTDOOR READY, DAY/NIGHT FIXED DOME WITH HDTV 1080P

A. Light Sensitive Fixed Dome Camera providing detailed wide-angle views.

B. Day and Night functionality while maintaining high image quality even in low light conditions.

C. Support multi-view streaming, enabling different areas of a scene to be cropped from the full view and streamed simultaneously for viewing or recording.

D. The camera is vandal-resistant, outdoor ready camera has IP66 and NEMA 4X rating for protection against dust, rain and snow.

E. HDTV 1080p/3MP

F. Camera

1. Image Sensor

a. 1/3.6” (effective) progressive scan RGB CMOS.

2. Lens

a. M12 Mount

b. Fixed Iris

c. IR

Corrected d.

2.0mm,

F2.0

e. Horizontal Field of View: 106º

f. Vertical Field of View: 78º

3. Day and Night

a. Automatically Removable Infrared-Cut filter

4. Light Sensitivity/Minimum Illumination

a. Color: 0.3-20000 lux, F2.0, B/W: 0.06 lux, F2.0

5. Shutter Time

a. 1/30500 s to 2s

6. Camera Angle Adjustment

a. Pan ± 175º, Tilt 70º, Rotation ±180º

G. Video

1. Video Compression

a. H.264 (MPEG-4 Part 10/AVC) Baseline and Main Profile Motion JPEG.

2. Resolution

a. 2048x1536 (3 MP) to 160x120

3. Frame Rate

    a. 2MP (1600x1200) and HDTV 1080P (1920x1080) capture modes

    b. 25/30 fps with power line frequency 50/60 Hz

    c. 3 MP Capture Mode

    d. 16/20 fps with power line frequency 50/60 Hz

4. Video Streaming

    a. Multiple, individually configurable steams in H.264 and Motion JPEG.

    b. Controllable Frame Rate and Bandwidth

    c. VBR/MBR H.264

5. Multi-View Streaming

    a. Up to 8 Individually cropper out view areas.

    b. When streaming 4 view areas and 1 overview in VGA resolution, the frame rate is 16/20 fps per stream with power line frequency 50/60 Hz (3 MP Capture Mode)

6. Pan/Tilt/Zoom

    a. Digital PTZ, Preset Positions, Guard Tour

7. Image Settings

    a. Compression, Color, Brightness, Sharpness, Contrast, White Balance, Exposure Control, Blacklight Compensation, Wide Dynamic Range, dynamic contrast, text and image overlay, mirroring of images, privacy mask.

    b. Rotation: 0º, 90º, 180º, 270º, including corridor format.

    c. Exposure Zones, Fine Tuning of Low Light Behavior.

H. Network

1. Security

    a. Password Protection, IP Address Filtering, HTTPS Encryption, IEEE 802.1X network access control. Digest authentication, User Access Log. Centralized Certificate Manager.

2. Supported Protocols

    a. IPv4/v6, HTTP, HTTPS, SSL/TSL, QoS Layer 3 DiffServ, FTP, CIFS, SMB, SMTP.

I. System Integration

1. Event Triggers

a. Analytics, Edge Storage Events, External Input

2. Event Actions

a. File Upload: FTP, SFTP, HTP, HTTPS, Network Share and Email

b. Notification: email, HTTPS and TCP

c. External Output Activation

d. Video Recording to Edge Storage

e. Pre- and Post- Alarm Video Buffering

f. Go to PTZ Preset, Guard Tour

3. Data Streaming

a. Event Data

J. General

1. Casing

a. IP66- and NEMA 4X-rated, IK10 Impact-Resistant Aluminum casing with transparent, polycarbonate cover and dehumidifying membrane.

b. Encapsulated electronics.

c. Captive screws

d. Color: approved by owner

2. Memory

a. 512MB RAM, 128MB Flash

3. Power

a. Power over Ethernet (PoE) IEEE 802.3af/802.3at Type 1 Class 2 max 4.5 W, typical 3.4W

4. Connectors

a. Male RJ45 10BASE-T/100BASE-TX PoE on 2m network cable.

5. Storage

a. Support for microSD/microSDHC/mircoSDXC card

b. SD Card Encryption

c. Support for recording to network attached storage (NAS)

6. Operating

Conditions a. -

22ºF-122ºF

a. Humidity 10-100% RH (condensing)

2.05 2.4 MULTI-MEGAPIXEL FIXED MINI DOME WITH HDMI AND WIDE VIEW

A. Dome camera that provides up to 4 MP video

B. Ensures visible details both in dark and bright areas.

C. HDMI support enables live streaming to a public viewing monitor.

D. Digital PTZ capability, the camera provides cropped out views.

E. Ultra-compact, vandal and dust resistant.

F. HDMI support enables streaming to a monitor

G. Camera

1. Image Sensor

a. 1/3” Progressive Scan RGB CMO

2. Lens

a. M12 Mount, Fixed Iris, Fixed Focus b. 2.4mm: F2.2

b. Horizontal Field of View: 128º

c. Vertical Field of View: 72º e. 1.8mm: F2.4

d. 4:3 Aspect Ratio: Horizontal Field of View: 132º, vertical field of view 96º

e. 16:9 Aspect Ratio: Horizontal Field of View 152º, vertical field of view 80º

3. Light Sensitivity

a. 2.4mm: 0.3 lux at 50 IRE F2.2

4. Shutter Time

a. 1/32500s to 1/5s

5. Camera Angle Adjustment

a. Pan: ±177º

b. Tilt: ±65º

c. Rotation: ±176º

d. Can be directed in any direction and see the wall/ceiling

H. Video

1. Video Compression
    a. H.264 (MPEG-4 Part 10/AVC) Baseline, Main and High Profiles Motion JPEG.
2. Resolution
    a. 2.4mm: 2688x1520 to 320x240
3. Frame Rate
    a. 25/30 fps with power line frequency 50/60 Hz
4. Video Streaming
    a. Multiple, individually configurable streams in H.264 and Motion JPEG
    b. Controllable Frame Rate and Bandwidth
    c. VBR/MBR H.264
    d. HDMI
5. Multi-view Streaming
    a. Up to 2 individually cropped out view areas in full frame rate.
6. Pan/Tilt/Zoom
    a. Digital PTZ
7. HDMI Output
    a. HDMI 1080p @ 25/30 fps (50/60 Hz) b.
    b. HDMI 1080i @ 50/60 fps (50/60 Hz) c.
    c. HDMI 720p @ 50/60 fps (50/60 Hz) d.
    d. HDMI 720p @ 25/30 fps (50/60 Hz)
8. Image Settings
    a. Compression
    b. Color
    c. Brightness
    d. Sharpness
    e. Contrast
    f. White Balance

g. Exposure Control

h. WDR

i. Text and Image Overlay

j. Mirroring of Images

k. Privacy Mask

l. Rotation: 0º, 90º, 180º, 270º, including Corridor Format

I. Network

1. Security

a. Password Protection

b. IP Address Filtering

c. HTTPS Encryption

d. IEEE 802.1X Network Access Control

e. Digest Authentication

f. User Access Log

g. Centralized Certificate Management

h. Brute Force Delay Protection

2. Supported Protocols

a. IPv4

b. IPv6

c. USGv6

d. HTTP

e. HTTPS

f. SSL/TLS

3. QoS Layer 3 DiffServ

4. FTP

5. SFTP

6. CIFS/SMB

7. SMTP
8. Bonjour
9. SNMPv1/v2c/v3 MIB-II)
10. DNS
11. DynDNS
12. NTP
13. RTSP
14. RTP
15. TCP
16. UDP

J. System Integration

1. Analytics Included
    a. Video Motion Detection
    b. Active Tampering Alarm
2. Analytics Supported
    a. Digital Auto tracking
    b. Fence Guard
    c. Motion Guard
    d. Loitering Guard
    e. People Counter
    f. Queue Monitor
    g. Occupancy Estimator
    h. Direction Detector
    i. Tailgating Detector
    j. Random Selector
3. Event Triggers
    a. Analytics
    b. Edge Storage Events

c. Virtual Inputs

4. Event Actions

a. File Upload: FTP, SFTP, HTTP, HTTPS Network Share and Email

b. Notification: email, HTTP, HTTPS and TCP and SNMP Trap

c. Video Recording to Edge Storage

d. Send Video Clip

e. Pre-and post-alarm video buffering

f. Overlay Text

5. Data Streaming

a. Event Data

K. General

1. Casing

a. IP42 Water-and Dust-Resistant, if installed properly

b. IK09 Impact-Resistant, Polycarbonate/ABS Casing

c. Encapsulated electronics, captive screws.

d. Color: approved by owner

2. Sustainability

a. PVC free.

3. Memory

a. 512MB RAM, 256MB Flash

4. Power

a. Power over Ethernet (PoE) IEE 802.3af/802.3at Type 1 Class 1

b. Typical 2.8W, max 3/2W

5. Connectors

a. RJ45 10BASE-T/100BASE-TX PoE

b. HDMI Type D

6. Storage

a. Support for microSD/microSDHC/mircoSDXC card

b. Support for SD Card Encryption

c. Support for Recording to Network Attached Storage (NAS)

7. Operating Conditions

a. 32ºF to 149ºF

b. Humidity 15-85% RH (Non-Condensing)

8. Storage Conditions

a. -40ºF to 149ºF

2.06 FISHEYE 12MP OUTDOOR READY DOME WITH 360º PANORAMIC VIEW

A. Camera

1. Image Sensor

a. 12 MP (4000x3000) 1/1.7” Progressive Scan RGB CMOS

2. Lens

a. Fixed Iris, Fixed Focus, 1.3mm, F2.2

b. Horizontal Field of View: 181º

c. Vertical Field of View: 181º

3. Day and Night

a. Automatically Removable Infrared-Cut Filter

4. Minimum Illumination

a. Color: 0.19lux at 50 IRE F2.2

b. B/W: 0.04 lux at 50 IRE F2.2

c. O Lux with IR Illumination on

5. Shutter Time

a. 1/22 500 s to 2 s

6. Camera Angle Adjustment

a. Rotation n ±180º

B. Video

1. Video Compression

a. H.264 (MPEG-4 Part 10/AVC) Baseline, Main and High Profiles Motion JPEG

2. Resolution

    a. Overview 2992x2992 to 160x160

    b. Panorama: 3584x1344 to 192x72

    c. Double Panorama: 3584x2688 to 256x144 d.

    d. Quad View: 3584x2688 to 256x144

    e. e. View Area 104, 16:9: 2048x1152 to 256x144, 4:3: 2048x1536 to 320x40

    f. Panorama Corner Left/Right: 3200x1600 to 192x72

    g. Double Panorama Corner: 2880x2880 to 320x240

    h. Corridor: 2560x192 to 256x144

3. Frame Rate

    a. 360º Overview Only, up to 2992x2992 without HDR: 25/30 fps at 50/60Hz

    b. 360º Overview and De-warped views up to 4MP with WDR: up to 20 fps @ 50/60 Hz

    c. 360º overview and de-warped views up to max resolution with WDR: up to 12.5/15 fps @ 50/60Hz

4. Video Streaming

    a. Multiple, Individually configurable streams in H.264 and motion JPEG

    b. Controllable Frame Rate and Bandwidth

    c. VBR/MBR H.264

5. Multi-View Streaming

    a. 360º overview, de-warped panorama, double panorama, corridor and quad views.

    b. Up to 4 individually cropped out and de-warped view areas.

    c. All different views can be streamed simultaneously.

    d. Streaming 4 de-warped view areas and one 360º overview in max resolution up to 12 fps per stream.

6. Multi-View Streaming

    a. HDMI 1080p @ 50/60 fps (50/60 Hz)

7. Image Settings

    a. Compression, color, brightness, sharpness, contrast, local contrast, white balance, exposure control (including automatic gain control), exposure zones, fine tuning of behavior at different light levels, forensic WDR: up to 120 dB depending on scene;

dynamic text and image overlay, privacy masks, mirroring of images, rotation: 0º, 180º, including corridor format.

8. Pan/Tilt/Zoom

    a. Digital PTZ of view areas, digital PT of panorama, corner, corridor and quad views, preset positions, guard tour.

C. Network

1. Security

    a. Password Protection

    b. IP Address Filtering

    c. HTTPS Encryption

    d. IEEE 802.1X Network Access Control

    e. Digest Authentication

    f. User Access Log

    g. Centralized Certificate Management

    h. Brute Force Delay Protection

2. Supported Protocols

    a. IPv4

    b. IPv6

    c. USGv6

    d. HTTP

    e. HTTPS

    f. SSL/TLS

    g. QoS Layer 3 DiffServ

    h. FTP

    i. SFTP

    j. CIFS/SMB

    k. SMTP

    l. Bonjour

    m. SNMPv1/v2c/v3 MIB-II)

n. DNS

o. DynDNS

p. NTP

q. RTSP

r. RTP

s. TCP

t. UDP

D. System Integration

1. Application Programing

a. Open API for Software Integration

2. Analytics Included

a. Active Tampering Alarm

3. Event Triggers

a. Analytics

b. Supervised External Input

c. Virtual Inputs through API

d. Edge Storage Events

e. Open Casing

4. Event Actions

a. Record View: SD Card and Network Share

b. Upload of Images or Video Clips: FTP, SFTP, HTTP, HTTPS,

c. Network Share and email

d. Pre-and post-alarm video or image buffering for recording or upload.

e. Notification: email, HTTP, HTTPS, TCP and SNMP trap

f. PTZ: PTZ preset, start/stop guard tour

g. Overlay text, external output activation

5. Data Streaming

a. Event Data

6. Built-In Installation Aids

    a. Pixel counter, digital PTZ of view areas, digital PT of panorama, corner, corridor and quad views.

E. General

1. Casing

    a. IP66-and NEMA 4X-rated, IK10 impact-resistant casing in polycarbonate and aluminum with hard-coated dome and dehumidifying membrane.

    b. Encapsulated electronics and captive screws.

    c. Color: approved by owner

2. Sustainability

    a. PVC -free

3. Memory

    a. 2GB RAM, 512MB Flash

4. Power

    a. Power over Ethernet (PoE) IEEE 802.3af/802.3at Type 1 Class 3 Typical 7.8W, max 12.95W.

5. Connectors

    a. RJ45 10BASE-1/100BASE-TX PoE

    b. Terminal Block for 1 supervised alarm input and 1 digital output (12V DC output, max, load 25 mA)

    c. HDM type D

6. IR Illumination

    a. Range of reach 49 ft or more depending on scene.

7. Storage

    a. Support for microSD/microSDHC card

    b. Support for SD card encryption

    c. Support for recording to network-attached storage (NAS)

8. Operating Conditions

    a. 40ºF-122ºF

    b. Maximum Temperature (Intermittent): 131ºF

c. Start-up -22ºF-122ºF

d. Humidity 10-100% RH (condensing)

9. Storage Conditions

a. -40ºF-149ºF

10. Approvals

a. EMC

b. EN55032 Class A, EN 50121-4, IEC 62236-4, EN 55024

c. EN6100-6-1, EN 61000-6-2, FCC Part 15 Subpart B Class A

d. ICES-003 Class A, VCCI Class A, RCM AS/NZS CISPR 32 Class A

e. KC KN32 Class A, KC KN35

f. Safety

g. IEC/EN/UL 62368-1, IEC/EN/UL 60950-22, IEC/EN 62471

h. Environment

i. IEC 60068-2-1, IEC 60068-2-2, IEC 60068-2-6, IEC 60068-2-14,

j. IEC 60068-2-27, IEC 60721-3-5 Class 5M3 (vibration and shock), IEC/EN 60529 IP66, IEC/EN 62262 IK10, NEMA 250 Type 4X

k. Network

l. NIST SP500-267

2.07 180º PANORAMIC CAMERA FOR SEAMLESS COVERAGE

A. Fixed Dome Camera with Multiple Sensors, providing an easy, reliable and cost-efficient one-camera installation.

B. Seamlessly Stitched Images

C. 180º horizontal and 90º vertical coverage

D. 8.3MP Resolution at full frame rate

E. Camera

1. Image Sensor

a. 4 x 1/2.9” progressive scan RGB CMOS

2. Lens

a. Fixed 3.2mm, F2.0

b. Horizontal Field of View: 180º

c. Vertical Field of View: 90º

d. M12 mount

3. Day and Night

a. Automatically Removable Infrared-Cut Filter

4. Minimum Illumination

a. Color: 0.17 lux, F2.0 b. B/W: 0.05 lux, F2.0

5. Shutter Time

a. 1/33500 s to 1/10 s

6. Camera Angle Adjustment

a. Pan: ±180º

b. Tilt: 0º, 35º, 45º, 55º

c. Roll ±10º

F. Video

1. Video Compression

a. H.264 (MPEG-4 Part 10/AVC) Baseline

b. Main and High Profiles Motion JPEG

2. Resolution

a. 4320x1920 to 480x270

3. Frame Rate
a. 8.3MP (Client De-Warp): up to 25/30 fps (50/60 Hz) without WDR, up to 12.5/15 fps (50/60 Hz) with WDR

b. 7.5MP (Client De-Warp): up to 12.5/15 fps (50/60 Hz)

4. Video Streaming
a. 8.3MP (Client De-Warp): 1 individually configurable stream in

b. H.264 and Motion JPEG.

c. 7.5MP (Client De-Warp): 2 individually configurable streams in

d. H.264 and Motion JPEG

e. Controllable Frame Rate and Bandwidth

5. Image Settings

    a. Saturation, Contrast, Brightness, Sharpness, Forensic WDR: up to 120 dB depending on scene, white balance, day/night threshold, exposure mode, compression, dynamic text and image overlay, exposure control, noise reduction, fine tuning of behavior at low light, polygon privacy masks.

G. Network

1. Security

    a. Password protection, IP address filtering, HTTPS encryption, IEEE 802.1X network access control, digest authentication, user access log, centralized certificate management.

2. Supported Protocols

    a. IPv4

    b. IPv6

    c. HTTP

    d. HTTPS

    e. SSL/TLS

    f. QoS Layer 3 DiffServ

    g. FTP

    h. SFTP

    i. CIFS/SMB

    j. SMTP

    k. Bonjour

    l. UPnP

    m. SNMPv1/v2c/v3 MIB-II)

    n. DNS

    o. DynDNS

    p. NTP

    q. RTSP

    r. RTP

    s. TCP

t. UDP

u. IGMP

v. RTCP

w. ICMP

x. DHCP

y. ARP

z. SOCKS

aa. SSH

bb. LLDP

H. System Integration

1. Event Triggers

a. Analytics

b. Edge Storage Events

c. Shock Detection

2. Event Actions

a. Day/Night Mode

b. Overlay Text

c. Video Recording to Edge Storage

d. Pre-and Post- Alarm video buffering

e. Send SNMP trap

f. File upload: FTP, SFTP, HTTP, HTTPS network share, email

g. Notification: Email, HTTP, HTTPS, TCP

3. Data Streaming

a. Event data

4. Built-in Installation Aids

a. Pixel Counter, Leveling Guide

I. General

1. Casing
    a. IP66-/IP67- and NEMA 4X-rated
    b. IK10 Rated Impact-Resistant casing with polycarbonate hard coated clear dome, aluminum base and dehumidifying membrane.
2. Mounting
    a. Mounting bracket with junction box holes (double-gang, single-gang, 4” square and 4” octagon).
    b. ¾” (M25) conduit side entries
3. Sustainability
    a. PVC Free
4. Memory
    a. 1024MB RAM, 512MB Flash
5. Power
    a. Power over Ethernet (PoE) IEEE 802.3af/802.3at Type 1 Class 3 Typical 7W, max 12.9W
6. Connectors
    a. Shielded RJ45 10BASE-T/100BASE-TX/1000BASE-T PoE
7. Storage
    a. Support for microSD/microSDHC/microSDXC card
    b. Support for SD card encryption
    c. Support for recording to network-attached storage (NAS)
8. Operating Conditions
    a. -22ºF-122ºF
    b. Maximum Temperature (intermittent): 140ºF
    c. Humidity 10-100% RH (Condensing)
9. Storage Conditions
    a. -40ºF-149ºF
    b. EMC
10. Approvals

a. EN55032 Class A, EN 50121-4, IEC 62236-4, EN 50024

b. EN 61000-6.1, EN 61000-6-2, FCC Part 15 Subpart B Class A

c. ICES-003 Class A, VCCI Class A, RCM AS/NZS CISPR 32 Class A

d. KC KN32 Class A, KC KN35

11. Safety

a. IEC/EN/UL 60950-22, IEC/EN/UL 62368-1

12. Environment

a. IEC 60068-2-1, IEC 60068-2-2, IEC 60068-2-6

b. b. IEC 60068-2-14, IEC 60068-2-27, IEC 60068-2-78

c. IEC/EN 60529 IP66/IP67, IEC/EN 62262 IK10, NEMA 250 Type 4X

2.08 360ºM PTZ NETWORK CAMERA

A. Pan-Tilt-Zoom Camera for Remote Indoor Monitoring

B. Full Frame Rate Video in HDTV 1080p resolution and supports multiple H.264 and motion JPEG video streams.

C. Ceiling Mount Camera that provides flexible coverage over 4300 sf are with ±180º pan, 90º tilt and 5x optical zoom.

D. Protection against dust and dripping water, enabling the camera to operate.

E. HDTV 1080p

F. 5x Optical Zoom and autofocus

G. IP51-rated

H. Power over Ethernet (IEEE 802.3af)

I. Built-in Analytics

J. Camera

K. Image Sensor

1. 1/4.85” Progress Scan RGB CMOS

2. Lens

a. Varifocal, 2.2-11.0mm, F1.4-F2.5

b. Horizontal Field of View: 14º-71º

c. Vertical Field of View: 8º-40º

3. Autofocus

4. Minimum Illumination

a. Color: 1.2 lux at 30 IRE F1.4

5. Shutter Time

a. 1/16000 s to 1 s

6. Pan/Tilt/Zoom

a. Pan: ±179º, 100º/s

b. Tilt: 90º, 100º/s

c. Zoom: 5x optical, 10x digital

d. 25 preset positions, control queue, on-screen directional indicator

L. Video

1. Video Compression

a. H.264 (MPEG-4 10/AVC) Baseline, Main and High Profiles Motion JPEG

2. Resolution

a. 1920x1080 to 320x180 (16:9)

3. Frame Rate

a. Up to 25/30 fps (50/60 Hz) in all resolutions

4. Video Streaming

a. Multiple, individually configurable streams in H.264 and Motion JPEG.

b. Controllable Frame Rate and Bandwidth

c. VBR/MBR H.264

5. Image Settings

a. Resolution, compression, rotation: 0º, 180º, text and image overlay, color, brightness, sharpness, white balance, wide dynamic range, exposure control, exposure time, gain, exposure zones, exposure priority, image freeze on PTZ, privacy masks.

M. Audio

1. Audio Streaming

a. One-Way

2. Audio Compression

a. AAC-LC 8/16 kHz, G.711 PCM 8kHz, G.726 ADPCM 8 kHz

b. Configurable bit rate

3. Audio Input

a. Built-in Microphone

N. Network

1. Security

a. Password Protection, IP Address Filtering, HTTPS encryption, IEEE 802.1X network access control, digest authentication, user access log, centralized certificate management.

2. Supported Protocols

a. IPv4/v6

b. HTTP

c. HTTPS

d. SSL/TLS

e. QoS Layer 3 DiffServ

f. FTP

g. SFTP

h. CIFS/SMB

i. SMTP

j. Bonjour

k. UPnP

l. SNMPv1/v2c/v3 (MIB-II)

m. DNS

n. DynDNS

o. NTP

p. RTSP

q. RTP

r. TCP

s. UDP

t. IGMP

u. RTCP

v. ICMP

w. DHCP

x. ARP

y. SOCKS

z. SSH

O. System Integration

1. Analytics Included

a. Video Motion Detection

b. Audio Volume Detection

c. Scream Detection

d. Removed Object Detection

2. Event Triggers

a. Detectors: Live Steam Accessed

b. Hardware: Network

c. Input Signal: Manual Trigger, Virtual Inputs

d. PTZ: Moving, preset reached, ready

e. Storage: Disruption, recording

f. System: System Ready

g. Time: Recurrence, use schedule

3. Event Activities

P. General

1. Record video: SD Card, Network Share

2. Upload of Images or video clips: FTP, SFTP, HTTP, HTTPS Network share, email.
3. PTZ Control: preset Position
4. Notification: email, HTTP, HTTPS, TCP and SNMP
5. Overlay Text
6. Status LED
7. Data Streaming: Event Data
8. Casing
    a. IP51-rated plastic casing, clear dome
9. Sustainability
    a. PVC Free
10. Memory
    a. 512MB RAM, 256MB Flash
11. Power
    a. Power over Ethernet (PoE) 802.3af/802.3at Type 1 Class 3
    b. Typical 4.3W, max 7.8W
12. Connectors
    a. RJ45 10BASE-T/100BASE-TX PoE
13. Storage
    a. Support for microSD/microSDHC/microSDXC card
    b. Support for SD Card Encryption
    c. Support for recording to network attached storage (NAS)
14. Operating Conditions
    a. 32ºF to 113ºF
    b. Humidity 10-90% RH (non-condensing)
15. Storage Conditions
    a. -22ºF to 140ºF
16. Approvals

a. EMC

b. EN 55032 Class A, EN 55024, EN 61000-6-1, EN 61000-6-2

c. FCC Part 15 Supart B Class A, ICES-003 Class A, VCCI Class A, RCM AS/NZS CISPR 32 Class A, KCC KN32 Class A, KN-35 Safety

d. IEC/EN/UL 62368-1

e. Environment

f. IEC/EN 60529 IP51

2.09 4-PORT INDUSTRIAL POE SWITCH

A. 60W per port, 240W power budget

B. Compliant with High PoE 60W

C. Dual DC Power Redundancy

D. NEMA TS-2 Compliant

E. Switch is equipped with two RJ45 and two SFP data ports that allow extra devices to be connected.

F. Switch to be ruggedized for the availability to be mounted inside a surveillance cabinet.

G. Designed to withstand shock, vibrations and temperatures from -40ºF-167ºF.

H. Network

1. Security

a. Password Protection

b. HTTPS Encryption

c. VLAN

2. Supported Protocols

b. IPv4, IPv6v

c. HTTP

d. HTTPS

e. SMTP

f. Bonjour

g. UPnP

h. SNMP v1/v2c/v3

i. DNS

j. NTP

k. RTSP

l. TCP

m. UDP

n. IGMP

o. ICMP

p. DHCP

q. ARP

r. SSH

s. Radius

t. TACACS+

u. Syslog

v. IEEE 802.1X

w. IEEE 802.1Q (VLAN)

x. LLDP

y. LLP-Med

z. STP

aa. MSTP

bb. RSTP

cc. LACP

dd. RRPP

ee. 11.9 Mpps

ff. 16 Gbps

gg. 8K

hh. 9216 Bytes

l. General

1. Aluminum
2. Throughput
3. Switching Capacity
4. MAC Table
5. Jumbo Frames

J. Casing

1. Color: To Be Approved by Owner

K. Sustainability

1. PVC Free
2. Indoor

L. Environment

M. Dimensions

1. 5.3x5.1x2.4 inches
2. PoE Class
    a. Power over Ethernet Plus (PoE+) IEEE 802.3at Type 2 Class 4
3. PoE Output
    a. Up to 60W per port
    b. Power Budget 240W
4. Pin Assignment
    a. Power Over Pairs
    b. Port 1-4: 1/2, 3/6, 4/5 and 7/8
5. Connectors
    a. PoE Ports
    b. RJ45 10BASE-T/100BASE-TX/1000BASE-T Mbps (4x)
    c. Data Ports/Uplink
    d. RJ45 10BASE-T/100BASE-TX/1000BASE-T Mbps (2x)
    e. SFP Port (2x)

f. Power

g. Power Connector Port (2x for power redundancy)

h. Console

i. RJ45 (1x)

6. Surge Protection

a. 6kV on all network ports

7. Operating Conditions

a. -40ºF to 167ºF

b. Humidity 5-95% RH (non-condensing)

8. Storage Conditions

a. -40ºF to 185ºF

b. EMC

9. Approvals

a. EN 55032 Class A

b. c. EN 55024

c. FCC part 15 Subpart 32 Class A

d. ICES-003 Class A

e. VCCI Class A

f. RCM AS/NZS CISPR 32 Class A h. EN 50121-4

g. EN 61000-3-2, EN 61000-3-3, EN 61000-6-1, EN 61000-6-2

h. EN 61000-6-3, EN 61000-6-4

i. IEC 62236-4

10. Safety

a. IEC/EN/UL 60950-1

11. Environment

a. IEC 60068-2-6, IEC 60068-2-27

b. 60068-2-31 (Free Fall – Procedure 1)

c. NEMA TS-2-2003 v02.06, subsection 2.2.8 and 2.2.9

2.10 CORNER MOUNT

A. Corner Bracket is an aluminum bracket for mounting network cameras on external corners. Contractor to confirm complete installation of cameras with this mount.

B. Robust and Safe Installation

C. Indoor or Outdoor use

2.11 MEDIA CABINETS

A. Media Converter Cabinet designed for PTZ dome cameras with pendant kit.

B. Pre-configured Cabinet

C. Indoor/Outdoor ready cabinet

D. Offers pre-configured components for usage together with fiber installations.

E. Robust and Safe Installation

F. Power

1. Input (120V AC): 90-175 V AC, Max. 4A

2. Input (230V AC): 90-264 VAC, Max 4A

3. Output: Input Voltage, Max 4A

G. Connectors

1. 2x RJ45 connectors (10/100 Mbps)

2. 2x SFP connectors (100/1000 Mbps) for SFP fiber optic modules or SFP to copper modules

H. Operating Conditions

1. -40ºF to 149ºF

2. Humidity 10-100% RH (condensing)

I. Approvals

1. EN 50121-4, IEC 6223604, EN 50581, IEC/EN 60529, IP66, NEMA 250 Type 4X, IEC/EN 62262 Ik10, REACH, WEEE, CE, IEC 60068-2-27 4M3, IEC/EN/UL 60950-22, UL 50, UL 50E 120V AC, FCC Part 15

2. Subpart B Class A, VCCI Class A, ICES-003 Class A, C-tick, AS/NZS CISPR 22 Class A 230 V AC, EN 55022 Class A, EN 61000-3-2, EN 61000-3-3, EN 61000-6-1, EN 61000-6.2, EN 55024, C-Tick AS/NZS

3. CISPR 22 Class A

2.12 WALL AND POLE MOUNT ARM

A. Designed for PTZ and Multi-Sensor Cameras.

B. Wall and Pole Mount accommodates and safely protects the accessories inside the mount.

C. Mount includes power and data connection via pre-mounted Ethernet cable.

D. Impact Resistant and Outdoor Proven material.

E. Mount suits all environments both indoor and outdoors.

F. Mount can be installed on poles and corners with accessories to be included as required.

G. Room for connectivity devices, midspans and service loop.

H. Protection against impacts, water, dust and corrosion

I. Pre-mounted RJ45 connector

2.13 OUTDOOR 24V POWER SUPPLY

A. UL Certified Power Supply Provides 24V DC.

B. Operating Temperature -40ºF to 158º

C. Provides power to network cameras, media converters, etc. even in harsh environments

D. Rated Input Voltage: 100-240V AC

E. Input Voltage: 90-264V AC/120-375V DC

F. Output Voltage: 24V DC (adjustable from 24 to 28 V DC)

G. Output Current 4.2A

H. Output Power: 100W

I. Operating Conditions: -40ºF to 158ºF

J. Storage Conditions: -40ºF to 185ºF

K. Approvals: CE, cULus, cURus, CCC, RCM, EAC

L. Standards: EMC, IEC/EN 55024, IEC/EN 55022 Class B

M. Standards Safety: UL 508, UL 60950-1, CAS/CSA C22.2 No. 107.1, CAN/CSA C22.2 No. 60950

2.14 SFP MODULE 1000BASE-T COPPER

A. Ethernet Module for Expansion of Network Ports

B. Small Form-Factor Pluggable (SFP) transceiver that supplies network devices

C. Industrial Grade

D. Provides link-loss that enable network redundancy.

E. 1.25 Gbps over 4-pair category 5 UTP cable with up to 100m link length

F. Module uses an integrated RJ-45 connector and is to be tested and verified.

G. IEEE 802.3: 2002 compliant

H. 1000BASE-X and 1000BASE-T auto negotiation compliant

I. SFP Multi-source agreement.

J. Operating Conditions: -40ºF to 185º F

K. Operating Conditions Humidity 10-90% RH (non-condensing)

L. Storage Conditions -40ºF to 185º

M. Storage Conditions Humidity 5-95% RH (non-condensing)

N. Approvals: EN 55022 Class B, EN 6100-3-2, EN 61000-3-3, EN 55024, FCC Part 15 Subpart B Class B, IEC/EN/UL 60950-1, RoHS, REACH, WEEE

2.15 SFP MODULE SINGLE-MODE

A. Form Factor Pluggable SFP Transceiver that supplies network devices with a fiber optic network connection.

B. Includes Link-Loss that Enable Network Redundancy.

C. Long Wavelength FP laser diodes enable data transmission up to 10km on a single mode 9/125 µm optical fiber.

D. Switching capacity 1.25 Gbsp

E. Transceiver Type: Single-mode

F. Hot Pluggability

G. Wavelength 1310 nm

H. 1.0625 Gbps Fiber Channel FC-P1 100-SM-LC-L Compliant

I. Connectors LC Duplex Receptacle

J. Operating Conditions: -40ºF to 185ºF, Humidity 10-90% RH (non-condensing)

K. Storage Conditions: -40ºF to 185ºF, Humidity 5-95% RH (non-condensing)

L. Approvals: EN 55022 Class B, EN 6100-3-2, EN 61000-3-3, EN 55024, FCC Part 15

M. Subpart B Class B, IEC/EN/UL 60950-1, EN 60825-1 Class 1, FDA 21 CFR 1040, RoHS, REACH, WEEE.

2.16 SFP MODULE MULTIMODE FIBER

A. Up to 550m Transmission Range

B. Form Factor Pluggable SFP Transceiver that supplies network devices with a fiber optic network connection.

C. Short wavelength VCSEL laser diodes enable data transmission up to 500m on a multimode 50/125 µm optical fiber.

D. Up to 550m range

E. Multimode fiber

F. Link-Loss Feature

G. Hot Pluggability

H. Wavelength 850nm

I. 1.0625 Gbps fiber channel FC-PI 100-M5-SN-I Compliant

J. 1.0625 Gbps fiber channel FC-PI 100-M6-SN-I Compliant

K. 1.25 Gbps IEEE 802.3z 1000BASE-SX compliant

L. 1.25 Gbps IEEE 802.3ah 1000BASE-SC compliant

M. Connectors LC Duplex Receptacle

N. Operating Conditions: -40ºF to 185ºF, Humidity 10-90% RH (non-condensing)

O. Storage Conditions: -40ºF to 185ºF, Humidity 5-95% RH (non-condensing)

P. Approvals: EN 55022 Class B, EN 6100-3-2, EN 61000-3-3, EN 55024, FCC Part 15

Q. Subpart B Class B, IEC/EN/UL 60950-1, EN 60825-1 Class 1, FDA 21 CFR 1040, RoHS, REACH, WEEE.

2.17 SINGLE PORT 60W INDUSTRIAL MIDSPAN (OPTIONAL)

A. 60W Power over Ethernet

B. Operating Temperature Range: -40ºF to 167ºF

C. Dual DC Input: 20-60 V DC

D. Plug and Play

E. Data and power are fed to a network video product through an Ethernet cable.

F. Use together with a PoE splitter for a network video product without built-in PoE support

G. Data Rate: 10/100/1000 Mbps

H. Installation and Management: Automatically detects PoE and High PoE-enabled devices and supplies inline power

I. Local LED management display

J. High Power over Ethernet

K. Power Max 72W

L. Power Consumption:

1. No remote device connected 2W

2. 30W remote device connected 36W

3. 60W remote device connected 72W

M. Connectors: Shielded, RJ45, ANSI TIA 568A and 568B, 6-pin DC power and alarm terminal connector

N. Wiring: Data provided over pairs 1/2 and 3/6 for 10/100 Ethernet, over all foru pairs for Gigabit Ethernet.

O. Operating Conditions: -40ºF to 167ºF, humidity max 95% RH (non-condensing)

P. Storage Conditions: -40ºF to 185ºF

Q. Approvals: Safety – IEC/EN/UL 62368-1, UL 508, EMC, EN 55024, EN 55032 Class A, FCC Part 15 Subpart B Class A, VCCI Class A, RCM AS/NZS CISPR32 Class A, ICES- 003 Class A, EAC.

2.18 128 GB HIGH ENDURANCE CARD (OPTIONAL)

A. High Performing Edge Storage optimized for video surveillance

B. Edge Storage enables flexible storage solutions such as de-centralized video recording.

C. In applications with bandwidth limitations, live video can be viewed in low resolution, while high resolution video is recorded locally.

D. Optimized for surveillance cameras

E. Health monitoring ready

F. SD Card Adapter included

2.19 INDOOR WITH POWER OVER ETHERNET EXTENDER (OPTIONAL)

A. More than 100m Ethernet and PoE connection

B. Compatible with IEEE 802.3af and IEEE 802.3at

C. Full-rate network throughout the whole extender distance.

2.20 24V POWER OVER ETHERNET MIDSPAN 60W (OPTIONAL)

A. Midspan injects power and data to the network device with built-in PoE support.

B. Provide 60W (two times IEEE 802.3at)

C. IEEE 802.3at

D. 24V AC

E. Support for PTZ Dome Cameras

F. Plug and plan

G. To be used together with PoE splitter for a network video product without built-in PoE support

H. Data Rate: 10/100/1000 Mbps

2.21 60W 120 VAC SFP MIDSPAN (OPTIONAL)

A. SFP slot for fiber compact plug and play media converter with PoE.

B. Integrated midspan

C. High PoE 60W

D. Data and power are fed to a network video product through an Ethernet cable

E. Use together with a PoE splitter for a network video product without built-in PoE support

F. Data rate: 10/100/1000 Mbps

G. High Power over Ethernet, Max 60W

H. AC Input Voltage: 100 to 240 V AC

I. AC Frequency: 50-60 Hz

J. Maximum Output Power: 56V DC (max 60 W)

K. Connectors: Shielded RJ45 ANSI TIA 568A and 568B

L. Data provided over pairs 1/2 and 3/6 for 10/100 Ethernet, over all four pairs for Gigabit Ethernet

M. Port Interfaces are located on the front panel

N. PoE LED

O. Power LED

P. Wall, shelf or DIN rail

Q. Operating Conditions: Up to 30W: 14ºF to 131ºF

R. Operating Conditions: Up to 60W 14ºF to 113ºF

S. Humidity max 90% RH (non-condensing)

T. Storage Conditions: -4ºF to 158ºF, humidity max 95% RH (non-condensing)

2.22 OUTDOOR RATED 60W POE EXTENDER (OPTIONAL)

A. Extends Ethernet and PoE connections beyond 100m limit

B. Compatible with IEEE 802.3af, IEEE 802.2at and high PoE 60W

C. Rugged, IP66/IP67- rated enclosure

D. No additional power supply is required

E. Full-rate network throughout the whole extender distance.

F. 10/100 Mbps half/full duplex

G. The maximum distance depends on the connected product, power source and operating conditions.

H. Max 200m for IEEE 802.3at

I. Max 300m for IEEE 802.3af

J. Connectors: Shielded or unshielded RJ45, ANSI TIA 568A and 568B

K. Network Cables: Shielded or unshielded category 5 (or higher)

PART 3 - EXECUTION

3.01 INSTALLATION

A. System installation shall be in accordance with NECA 303, manufacturer and related documents and references, for each type of security subsystem designed, engineered and installed.

B. Components shall be configured with appropriate “service points” to pinpoint system trouble in less than 30 minutes.

C. The Contractor shall install all system components including Government furnished equipment, and appurtenances in accordance with the manufacturer's instructions and shall furnish all necessary connectors, terminators, interconnections, services, and adjustments required for a complete and operable system.

D. Integration with these security subsystems shall be achieved by computer programming or the direct hardwiring of the systems.

E. For programming purposes refer to the manufacturers requirements for correct system operations. Ensure computers being utilized for system integration meet or exceed the minimum system requirements outlined on the systems software packages.

F. A complete CCTV System shall be comprised of, but not limited to, the following components:

1. Cameras

2. Lenses

3. Video Display Equipment

4. Camera Housings and Mounts

5. Controlling Equipment

6. Recording Devices

7. Wiring and Cables

G. The Contractor shall visit the site and verify that site conditions are in agreement/compliance with the design package. The Contractor shall report all changes to the site or conditions that will affect performance of the system to the Contracting Officer in the form of a report. The Contractor shall not take any corrective action without written permission received from the Contracting Officer.

H. Enclosure Penetrations: All enclosure penetrations shall be from the bottom of the enclosure unless the system design requires penetrations from other directions. Penetrations of interior enclosures involving transitions of conduit from interior to exterior, and all penetrations on exterior enclosures shall be sealed with rubber silicone sealant to preclude the entry of water. The conduit riser shall terminate in a hot-dipped galvanized metal cable terminator. The terminator shall be filled with an approved sealant as recommended by the cable manufacturer and in such a manner that the cable is not damaged.

I. Cold Galvanizing: All field welds and brazing on factory galvanized boxes, enclosures, and conduits shall be coated with a cold galvanized paint containing at least 95 percent zinc by weight.

J. Interconnection of Console Video Equipment: The Contractor shall connect signal paths between video equipment as specified by the OEM. Cables shall be as short as practicable for each signal path without causing strain at the connectors. Rack mounted equipment on slide mounts shall have cables of sufficient length to allow full extension of the slide rails from the rack.

K. Cameras:

1. Install the cameras with the focal length lens as indicated for each zone.

2. Connect power and signal lines to the camera.

3. Set cameras with fixed iris lenses to the f-stop to give full video level.

4. Aim camera to give field of view as needed to cover the alarm zone.

5. Aim fixed mounted cameras installed outdoors facing the rising or setting sun sufficiently below the horizon to preclude the camera looking directly at the sun.

6. Focus the lens to give a sharp picture (to include checking for day and night focus and image quality) over the entire field of view; and synchronize all cameras so the picture does not roll on the monitor when cameras are selected. Dome cameras shall have all preset positions defined and installed.

L. Monitors:

1. Install the monitors as shown and specified in design and construction documents.

2. Connect all signal inputs and outputs as shown/specified.

3. Terminate video input signals as required.

4. Connect the monitor to AC power.

M. Video Recording Equipment:

1. Install the video recording equipment as shown in the design and construction documents, and as specified by the OEM.

2. Connect video signal inputs and outputs as shown/specified.

3. Connect alarm signal inputs and outputs as shown/specified.

4. Connect video recording equipment to AC power.

N. Video Signal Equipment:

1. Install the video signal equipment as noted construction documents, and as specified by the OEM.

2. Connect video or signal inputs and outputs as shown/specified.

3. Terminate video inputs as required.

4. Connect alarm signal inputs and outputs as required.

5. Connect control signal inputs and outputs as required

6. Connect electrically powered equipment to AC power.

O. Camera Housings, Mounts, and Poles:

1. Install the camera housings and mounts as specified by the manufacturer, provide mounting hardware sized appropriately to secure each camera, housing and mount with maximum wind and ice loading encountered at the site.

2. Provide a foundation for each camera pole as specified.

3. Provide a ground rod for each camera pole and connect the camera pole to the ground rod.

4. Provide electrical and signal transmission cabling to the mount location via a hardened carrier system from the Access Control System and Database Management to the device.

5. Connect signal lines and AC power to the housing interfaces.

6. Connect pole wiring harness to camera.

P. System Start-Up

1. The Contractor shall not apply power to the CCTV System until the following items have been completed:

   a. CCTV System equipment items and have been set up in accordance with manufacturer's instructions.

   b. A visual inspection of the CCTV System has been conducted to ensure that defective equipment items have not been installed and that there are no loose connections.

   c. System wiring has been tested and verified as correctly connected as indicated.

   d. All system grounding and transient protection systems have been verified as installed and connected as indicated.

   e. Power supplies to be connected to the CCTV System have been verified as the correct voltage, phasing, and frequency as indicated.

2. Satisfaction of the above requirements shall not relieve the Contractor of responsibility for incorrect installation, defective equipment items, or collateral damage as a result of Contractor work efforts.

Q. Supplemental Contractor Quality Control

1. The Contractor shall provide the services of technical representatives who are familiar with all components and installation procedures of the installed CCTV System; and are approved by the Consultant.

2. The Contractor will be present on the job site during the preparatory and initial phases of quality control to provide technical assistance.

3. The Contractor shall also be available on an as needed basis to provide assistance with follow-up phases of quality control.

4. The Contractor shall participate in the testing and validation of the system and shall provide certification that the system installed is fully operational as all construction document requirements have been fulfilled.

3.02 TESTING AND TRAINING

A. All testing and training shall be performed by a factory-authorized representative and this training shall be videotaped and shall accommodate no less than 8 attendees and all training shall be on-site. The time, date and location of this training shall be identified by the Owner.

B. All training shall include demonstrations of the key elements and components of the CCTV system, including videotaping and all related features.

C. The Contractor shall submit, for review and approval a listing of all demonstration and training that is to take place. This listing shall include subject matter and time frames for each of the recommended subjects. This training shall be compliant with the General Requirements.

END OFSECTION

SECTION 283111 – DIGITAL, ADDRESSABLE FIRE-ALARM SYSTEM

1 - GENERAL

1.01 RELATED DOCUMENTS

A. Drawings and general provisions of the Contract, including General and Supplementary Conditions and Division 01 Specification Sections, apply to this Section.

B. 2018 International Building Code with Clark County amendments (SNBC).

C. 2018 International Fire Code (IFC) with Clark County amendments (SNFC).

D. 2017 National Electrical Code with Clark County amendments.

E. 2016 Edition of NFPA 72, National Fire Alarm and Signaling Code with Clark County amendments.

1.02 SUMMARY

A. Section Includes:

1. Fire-alarm control units.

2. Notification appliances.

3. Remote annunciator.

1.03 DEFINITIONS

A. AHJ: Authority Having Jurisdiction.

B. LED: Light-emitting diode.

C. NICET: National Institute for Certification in Engineering Technologies.

D. NRTL: Nationally Recognized Testing Laboratory.

1.04 SYSTEM DESCRIPTION

A. Noncoded, UL-listed addressable system, with multiplexed signal transmission, dedicated to fire-alarm service only. The system shall also control and monitor the smoke control system components and be UL-listed for smoke control system equipment (UUKL).

B. The contractor shall furnish all labor, services and materials necessary to furnish and install a complete, fully functional fire alarm and detection system. The system shall comply in respects with all pertinent codes, rules, regulations and laws of the Authority and local jurisdiction. The system shall comply in all respects with the requirements of the specifications, manufacturer’s recommendations and Underwriters Laboratories, Inc. (ULI).

1.05 PERFORMANCE REQUIREMENTS

A. Seismic Performance: Fire-alarm control unit and raceways shall withstand the effects of earthquake motions determined according to ASCE/SEI 7.

1. The term "withstand" means "the unit will remain in place without separation of any parts from the device when subjected to the seismic forces specified and the unit will be fully operational after the seismic event."

1.06 SUBMITTALS

A. General Submittal Requirements:

1. Submittals shall be reviewed by the Engineer prior to submitting them to the AHJ.

2. Shop drawings for fire alarm systems shall be submitted for review and approval prior to system installation.

3. Shop Drawings shall be prepared by persons with the following qualifications:

a. Trained and certified by manufacturer in fire-alarm system design.

b. Licensed or certified by authorities having jurisdiction.

4. Shop drawings shall be reviewed and signed off by an individual having a minimum of a NICET Level II certification in fire protection engineering technology, subfield of fire alarm systems.

B. Product Data: For each type of product indicated. All submitted product data model/catalog numbers must be clearly identified by means of arrows, highlights, or other suitable means.

C. Shop Drawings: For fire-alarm system. Include plans, elevations, sections, details, and attachments to other work as required by NFPA 72 and SNFC Section 907.1.2. Drawings to include the following as a minimum:

1. Comply with recommendations in the "Documentation" Section of the "Fundamentals of Fire Alarm Systems" Chapter in NFPA 72.

2. Include voltage drop calculations for notification appliance circuits.

3. Include battery-size calculations.

4. Control panel wiring and interconnection schematics.

5. Complete point to point wiring diagrams.

6. Riser diagrams.

7. Complete floor plan drawings locating all system devices and 1/8” = 1’-0” scale plan and elevation of all equipment. Including showing the placement of each individual item of fire alarm as well as raceway size and routing, junction boxes, and conductor size, quantity, and color in each raceway. Floor plans shall also include labeling for all addressable devices, notification appliances, relay circuits and electrical circuits serving fire alarm panels.

8. Detailed system of operation input/output matrix similar to Figure A.14.6.2.4 of NFPA 72.

9. Class/style designation of all initiating device circuits (IDC), signaling line circuits (SLC), notification appliance circuits (NAC) and network circuits.

10. Device mounting heights.

11. Catalog/model number for all items proposed to meet the system performance detailed in this specification.

D. Qualification Data: For qualified Installer.

E. Seismic Qualification Certificates: For fire-alarm control unit, accessories, and components, from manufacturer.

1. Basis for Certification: Indicate whether withstand certification is based on actual test of assembled components or on calculation.

2. Dimensioned Outline Drawings of Equipment Unit: Identify center of gravity and locate and describe mounting and anchorage provisions.

3. Detailed description of equipment anchorage devices on which the certification is based and their installation requirements.

F. Field quality-control reports.

G. Operation and Maintenance Data: For fire-alarm systems and components to include in emergency, operation, and maintenance manuals. In addition to items specified in Division 01 Section "Operation and Maintenance Data," include the following:

1. Comply with the "Records" Section of the "Inspection, Testing and Maintenance" Chapter in NFPA 72.

2. Provide "Notification Appliance Power Panel Supplementary Record of Completion" and/or “Interconnected Systems Supplementary Record of Completion” documents, as necessary, according to NFPA 72 article "Permanent Records" in the "Records" Section of the "Inspection, Testing and Maintenance" Chapter.

3. Provide "Maintenance, Inspection and Testing Records" according to NFPA 72 article of the same name and include the following:

a. Frequency of testing of installed components.

b. Frequency of inspection of installed components.

c. Requirements and recommendations related to results of maintenance.

d. Manufacturer's user training manuals.

4. Manufacturer's required maintenance related to system warranty requirements.

5. Abbreviated operating instructions for mounting at fire-alarm control unit.

6. Copy of NFPA 72.

7. Warranty letter.

8. Provide the name, address and telephone number (including 24-hour support numbers) of the authorized factory representative.

9. Small scale (11-inches by 17-inches) fire alarm shop drawings of the system.

10. Manufacturer's equipment data sheets and installation instructions for all equipment supplied.

11. Detailed narrative description of the system architecture, inputs, notification signaling, auxiliary functions, annunciation, sequence of operations, expansion capability, application considerations and limitations.

H. Software and Firmware Operational Documentation:

1. Software operating and upgrade manuals.

2. Program Software Backup: On magnetic media or compact disk, complete with data files.

3. Device address list.

4. Printout of software application and graphic screens.

1.07 CLOSE OUT DOCUMENTATION

A. Two copies of the following documents shall be delivered to the building Owner's representative at the time of system acceptance. The close out submittals shall include:

1. Operation and maintenance manual as described in Section 1.6.H.

2. The application program listing for the system as installed and tested at the time of acceptance by the building Owner and/or local AHJ (disk, hard copy printout and all required passwords).

3. As-built shop drawings as described in Section 1.6.C.

4. A filled out Fire Alarm System Record of Completion form identical to NFPA 72 Figure 7.8.2(a).

1.08 QUALITY ASSURANCE

A. Manufacturer: The manufacturer shall be a company specializing in fire alarm and detection systems with a minimum of five years documented experience in systems of this complexity.

B. Installer Qualifications: Personnel shall be trained and certified by the manufacturer for installation of units required for this Project. Installation personnel shall be supervised by persons who are qualified and experienced in the installation, inspection and testing of fire alarm systems. The installation supervisor must be licensed or certified by the state and have a minimum of a NICET Level II certification in fire protection engineering technology, subfield of fire alarm systems.

C. Source Limitations for Fire-Alarm System and Components: Obtain fire-alarm system from single source from single manufacturer. Components shall be compatible with, and operate as, an extension of existing system.

D. Electrical Components, Devices, and Accessories: Listed and labeled as defined in NFPA 70, by a qualified testing agency, and marked for intended location and application.

1.09 PROJECT CONDITIONS

A. Interruption of Existing Fire-Alarm Service: Do not interrupt fire-alarm service to facilities occupied by Owner or others unless permitted under the following conditions and then only after arranging to provide temporary guard service according to requirements indicated:

1. Notify the Owner no fewer than two days in advance of proposed interruption of fire-alarm service.

2. Do not proceed with interruption of fire-alarm service without Owner's written permission

1.10 SEQUENCING AND SCHEDULING

A. Existing Fire-Alarm Equipment: Maintain existing equipment fully operational until new equipment has been tested and accepted. As new equipment is installed, label it "NOT IN SERVICE" until it is accepted. Remove labels from new equipment when put into service and label existing fire-alarm equipment "NOT IN SERVICE" until removed from the building.

B. Equipment Removal: After acceptance of new fire-alarm system, remove existing disconnected fire-alarm equipment and wiring.

1.11 SOFTWARE SERVICE AGREEMENT

A. Comply with UL 864.

B. Technical Support: Beginning with Substantial Completion, provide software support for one year.

C. Upgrade Service: Update software to latest version at Project completion. Install and program software upgrades that become available within two years from date of Substantial Completion. Upgrading software shall include operating system. Upgrade shall include new or revised licenses for use of software.

1. Provide 30 days' notice to Owner to allow scheduling and access to system and to allow Owner to upgrade computer equipment if necessary.

1.12 TRAINING

A. The system supplier shall include and present a minimum of 16-hours of documented formalized instruction for the building Owner, detailing the proper operation of the installed system.

B. The instruction shall be presented in an organized and professional manner by a person factory trained in the operation and maintenance of the equipment and who is also thoroughly familiar with the installation.

C. The instruction shall cover the schedule of maintenance required by NFPA 72 and any additional maintenance required by the system manufacturer.

D. Instruction shall be made available to the AHJ if requested.

1.13 WARRANTY AND MAINTENANCE

A. The contractor shall warranty all materials, installation and workmanship for one (1) year from date of acceptance, unless otherwise specified. A copy of the manufacturer’s warranty shall be provided with close-out documentation and included with the operations and maintenance manuals.

B. The system supplier shall maintain a service organization with adequate spare parts stock with 75-miles of installation. Any defects that render the system inoperative shall be repaired within 24-hours of the Owner notifying the contractor.

1.14 DELIVERY, STORAGE AND HANDLING

A. The contractor shall be responsible for all receiving, handling and storage of his material at the job site. Use of loading dock, service driveways and freight elevators shall be coordinated with the Owner and general contractor.

B. The contractor shall be responsible for providing proper storage spaces/containers during this project. The contractor shall be responsible for security of this space.

1.15 EXTRA MATERIALS

A. Furnish extra materials that match products installed and that are packaged with protective covering for storage and identified with labels describing contents.

1. Lamps for Remote Indicating Lamp Units: Quantity equal to 10 percent of amount installed, but no fewer than 1 unit.

2. Lamps for Strobe Units: Quantity equal to 10 percent of amount installed, but no fewer than 1 unit.

3. Keys and Tools: One extra set for access to locked and tamperproofed components.

4. Audible and Visual Notification Appliances: One of each type installed.

5. Fuses: Two of each type installed in the system

2 - PRODUCTS

2.01 MANUFACTURERS

A. All system components shall be cataloged products of a single supplier. All products shall be listed by the manufacturer for their intended purpose.

B. All control panel assemblies and connected field appliances shall be both designed and manufactured by the same company and shall be tested and cross-listed as to ensure that a fully functioning system is designed and installed. The system supplied under this specification shall be a microprocessor-based direct wired system. The system shall utilize independently addressed, microprocessor-based detectors and modules as described in this specification.

C. In order to establish a quality standard, the following manufacturer’s products shall be acceptable in the project base bid:

1. Fire Control Instruments, Inc.; a Honeywell company.

2. Gamewell; a Honeywell company.

3. GE Infrastructure; a unit of General Electric Company.

4. NOTIFIER; a Honeywell company.

5. Siemens Building Technologies, Inc.; Fire Safety Division.

6. SimplexGrinnell LP; a Tyco International company.

2.02 SYSTEMS OPERATIONAL DESCRIPTION

A. Fire-alarm signal from the existing system shall initiate the following actions:

1. Continuously operate alarm notification appliances.

2. Identify alarm at fire-alarm control unit and remote annunciator(s).

3. Transmit an alarm signal to the remote alarm receiving station.

4. Transmit a waterflow switch signal to the remote alarm receiving station (sprinkler waterflow switch only).

5. Unlock electric door locks in designated egress paths.

6. Release fire and smoke doors held open by magnetic door holders.

7. Activate visual notification appliances. Visual notification appliances shall continue to flash until the system has been reset.

8. Activate emergency shutoffs for gas and fuel supplies.

9. Record events in the system memory.

10. Record events by the system printer.

B. System trouble signal initiation shall be by one or more of the following devices and actions:

1. Open circuits, shorts, and grounds in designated circuits.

2. Opening, tampering with, or removing alarm-initiating and supervisory signal-initiating devices.

3. Loss of primary power at fire-alarm control unit.

4. Ground or a single break in fire-alarm control unit internal circuits.

5. Abnormal ac voltage at fire-alarm control unit.

6. Break in standby battery circuitry.

7. Failure of battery charging.

8. Abnormal position of any switch at fire-alarm control unit or annunciator.

9. Fire-pump power failure, including a dead-phase or phase-reversal condition.

10. Low-air-pressure switch operation on a dry-pipe or preaction sprinkler system.

C. System trouble and supervisory signal actions shall initiate the following actions:

1. Identify trouble or supervisory at fire-alarm control unit and remote annunciators.

2. Transmit a valve tamper alarm signal to the remote alarm receiving station (valve supervisory switch only).

3. Transmit a trouble signal to the remote alarm receiving station.

4. Record events in the system memory.

5. Record events by the system printer.

2.03 FIRE-ALARM CONTROL UNIT

A. General Requirements for Fire-Alarm Control Unit:

1. Field-programmable, microprocessor-based, modular, power-limited design with electronic modules, complying with UL 864 and listed and labeled by an NRTL.

a. System software and programs shall be held in flash electrically erasable programmable read-only memory (EEPROM), retaining the information through failure of primary and secondary power supplies.

b. Include a real-time clock for time annotation of events on the event recorder and printer.

2. Addressable initiation devices that communicate device identity and status.

a. Smoke sensors shall additionally communicate sensitivity setting and allow for adjustment of sensitivity at fire-alarm control unit.

b. Temperature sensors shall additionally test for and communicate the sensitivity range of the device.

3. Addressable control circuits for operation of mechanical equipment.

B. Alphanumeric Display and System Controls: Arranged for interface between human operator at fire-alarm control unit and addressable system components including annunciation and supervision. Display alarm, supervisory, and component status messages and the programming and control menu.

1. Annunciator and Display: Liquid-crystal type, 3 lines of 40 characters, minimum.

2. Keypad: Arranged to permit entry and execution of programming, display, and control commands and to indicate control commands to be entered into the system for control of smoke-detector sensitivity and other parameters.

C. Circuits:

1. Initiating Device, Notification Appliance, Signaling Line and Network Circuits:

a. Initiating Device Circuits: Style B, Class B.

b. Notification Appliance Circuits: Style Y, Class B.

c. Signaling Line Circuits: Style 4, Class B.

d. Network Circuits: Class A. Network circuits may be either copper of fiber optic cable.

2. Serial Interfaces: Two RS-232 ports for printer.

D. Door Controls: Door hold-open devices that are controlled by smoke detectors at doors in smoke barrier walls shall be connected to fire-alarm system.

E. Voice/Alarm Signaling Service: Central emergency communication system with redundant microphones, preamplifiers, amplifiers, and tone generators provided as a special module that is part of fire-alarm control unit. The system shall be a minimum dual channel system.

1. Indicated number of alarm channels for automatic, simultaneous transmission of different announcements to different zones or for manual transmission of announcements by use of the central-control microphone. Amplifiers shall comply with UL 1711 and be listed by an NRTL.

a. Allow the application of and evacuation signal to indicated number of zones and, at same time, allow voice paging to the other zones selectively or in any combination.

b. Programmable tone and message sequence selection.

c. Standard digitally recorded messages for "Evacuation" and "All Clear."

d. Generate tones to be sequenced with audio messages of type recommended by NFPA 72 and that are compatible with tone patterns of notification appliance circuits of fire-alarm control unit.

2. Status Annunciator: Indicate the status of various voice/alarm speaker zones and the status of firefighters' two-way telephone communication zones.

3. Preamplifiers, amplifiers, and tone generators shall automatically transfer to backup units, on primary equipment failure.

F. Printout of Events: On receipt of signal, print alarm, supervisory, and trouble events. Identify zone, device, and function. Include type of signal (alarm, supervisory, or trouble) and date and time of occurrence. Differentiate alarm signals from all other printed indications. Also print system reset event, including same information for device, location, date, and time. Commands initiate the printing of a list of existing alarm, supervisory, and trouble conditions in the system and a historical log of events.

G. Primary Power: 24-V dc obtained from 120-V ac service and a power-supply module. Initiating devices, notification appliances, signaling lines, trouble signals, supervisory signals shall be powered by 24-V dc source.

1. Alarm current draw of entire fire-alarm system shall not exceed 80 percent of the power-supply module rating.

H. Secondary Power: 24-V dc supply system with batteries, automatic battery charger, and automatic transfer switch.

1. Batteries: Sealed lead calcium.

2. The secondary power supply shall have the capacity to operate the system under maximum supervisory load for 4 hours and be capable of operating the system for 15 minutes of evacuation alarm on all required devices, operating at maximum load.

I. Instructions: Computer printout or typewritten instruction card mounted behind a plastic or glass cover in a stainless-steel or aluminum frame. Include interpretation and describe appropriate response for displays and signals. Briefly describe the functional operation of the system under normal, alarm, and trouble conditions.

2.04 NOTIFICATION APPLIANCES

A. General Requirements for Notification Appliances: Connected to notification appliance signal circuits, zoned as indicated, equipped for mounting as indicated and with screw terminals for system connections.

1. Combination Devices: Factory-integrated audible and visible devices in a single-mounting assembly, equipped for mounting as indicated and with screw terminals for system connections.

B. Horns: Electric-vibrating-polarized type, 24-V dc; with provision for housing the operating mechanism behind a grille. Comply with UL 464. Horns shall produce a sound-pressure level of 90 dBA, measured 10 feet (3 m) from the horn, using the coded signal prescribed in UL 464 test protocol.

C. Visible Notification Appliances: Xenon strobe lights comply with UL 1971, with clear or nominal white polycarbonate lens mounted on an aluminum faceplate. The word "FIRE" is provided in minimum 1-inch high letters on the cover.

1. Rated Light Output:

a. 15/30/75/110 cd, selectable in the field.

2. Mounting: Wall or ceiling mounted as indicated on the contract drawings.

3. For units with guards to prevent physical damage, light output ratings shall be determined with guards in place.

4. Flashing shall be in a temporal pattern, synchronized with other units.

5. Strobe Leads: Factory connected to screw terminals.

6. Mounting Faceplate: Factory finished, white.

D. Voice/Tone Notification Appliances:

1. Appliances shall comply with UL 1480 and shall be listed and labeled by an NRTL.

2. High-Range Units: Rated 2 to 15 W.

3. Low-Range Units: Rated 1/4 to 2 W.

4. Mounting: Wall or ceiling as indicated on the contract drawings and flush or surface mounted and bidirectional.

5. Matching Transformers: Tap range matched to acoustical environment of speaker location.

2.05 REMOTE ANNUNCIATOR

A. Description: Annunciator functions shall match those of fire-alarm control unit for alarm, supervisory, and trouble indications. Manual switching functions shall match those of fire-alarm control unit, including acknowledging, silencing, resetting, and testing.

1. Mounting: Flush or Surface cabinet, NEMA 250, Type 1.

B. Display Type and Functional Performance: Alphanumeric display and LED indicating lights shall match those of fire-alarm control unit. Provide controls to acknowledge, silence, reset, and test functions for alarm, supervisory, and trouble signals.

2.06 ADDRESSABLE INTERFACE DEVICE

A. Description: Microelectronic monitor module, NRTL listed for use in providing a system address for alarm-initiating devices for wired applications with normally open contacts.

B. Integral Relay: Capable of providing a direct signal to the associated function (e.g. elevator controller to initiate elevator recall, fan control, etc.).

2.07 DEVICE GUARDS

A. Description: Welded wire mesh of size and shape for the manual station, smoke detector, gong, or other device requiring protection.

1. Factory fabricated and furnished by manufacturer of device.

2. Finish: Paint of color to match the protected device.

3 - EXECUTION

3.01 EQUIPMENT INSTALLATION

A. Comply with NFPA 72 for installation of fire-alarm equipment.

B. All equipment shall be attached to walls and ceiling/floor assemblies and shall be mounted firmly in place. Detectors shall not be supported solely by suspended ceilings. Fasteners and supports shall be sized to support the required load.

C. Connecting to Existing Equipment: Verify that existing fire-alarm system is operational before making changes or connections.

1. Connect new equipment to existing control panel in existing part of the building.

2. Connect new equipment to existing monitoring equipment at the supervising station.

3. Expand, modify, and supplement existing control and monitoring equipment as necessary to extend existing control and monitoring functions to the new points. New components shall be capable of merging with existing configuration without degrading the performance of either system.

D. Audible Alarm-Indicating Devices: Comply with NFPA 72 Section 18.4.

E. Visible Alarm-Indicating Devices: Comply with NFPA 72 Section 18.5.

F. Fire-Alarm Control Unit: Surface mounted, with tops of cabinets not more than 72 inches above the finished floor.

G. Annunciator: Install with top of panel not more than 72 inches above the finished floor.

3.02 CONDUCTORS

A. All conductors shall be installed in conduit or enclosed raceway.

B. The conductors shall be of type recommended by the fire alarm manufacturer and comply with the SNEC.

3.03 CONDUIT RACEWAY

A. All systems and system components listed to UL864 Control Units for Fire Protection Signaling Systems may be installed within a common conduit raceway system, in accordance with the manufacturer's recommendations. Systems or system components not listed to UL864 standard shall utilize a separate conduit raceway system for each of the sub-systems.

B. The requirements of this section apply to all system conduits, raceways, electrical enclosures, junction boxes, pull boxes and device back boxes.

C. All system conduits shall be of sizes and types specified.

D. All system components shall be EMT, ¾-inch minimum, except for flexible metallic conduit used for whips to devices only, with a maximum length of 6-feet and ¾-inch diameter, minimum. Metal clad (MC) type cable is permitted and is to be installed in accordance with the SNEC.

E. All system conduits, which are installed in areas, which may be subject to physical damage or weather, shall be IMC or rigid steel, ¾-inch minimum.

F. Conduits shall be sized according to the conductors contained therein. Cross sectional area percentage fill for conduits shall not exceed 40%.

G. All fire alarm conduit systems shall be routed and installed to minimize the potential for physical, mechanical or by fire damage and so not to interfere with existing building systems, facilities or equipment and to facilitate service and minimize maintenance.

H. All conduits, except flexible conduit whips to devices, shall be solely attached to building structural members, ceiling slabs or permanent walls. Conduits shall not be attached to duct work, cable trays, other ceiling equipment, drop ceiling hangers/grids or partition walls, except where necessary to connect to initiating, notification, or auxiliary functions.

I. All system conduits, junction boxes, pull boxes, terminal cabinets, electrical enclosures and device back boxes shall be readily accessible for inspection, testing, service and maintenance.

3.04 IDENTIFICATION

A. Identify system components, wiring, cabling, and terminals. Comply with requirements for identification specified in Section 270553 "Identification for Communications Systems."

B. Install framed instructions in a location visible from fire-alarm control unit.

3.05 GROUNDING

A. Ground fire-alarm control unit and associated circuits; comply with IEEE 1100. Install a ground wire from main service ground to fire-alarm control unit.

3.06 FIELD QUALITY CONTROL

A. Field tests shall be witnessed by the AHJ and/or third party special inspector.

B. Manufacturer's Field Service: Engage a factory-authorized service representative to inspect, test, and adjust components, assemblies, and equipment installations, including connections.

C. Perform tests and inspections.

1. Manufacturer's Field Service: Engage a factory-authorized service representative to inspect components, assemblies, and equipment installations, including connections, and to assist in testing.

D. Tests and Inspections:

1. Visual Inspection: Conduct visual inspection prior to testing.

   a. Inspection shall be based on completed Record Drawings and system documentation that is required by NFPA 72 in its "Completion Documents, Preparation" Table in the "Documentation" Section of the "Fundamentals of Fire Alarm Systems" Chapter.

   b. Comply with "Visual Inspection Frequencies" Table in the "Inspection" Section of the "Inspection, Testing and Maintenance" Chapter in NFPA 72; retain the "Initial/Reacceptance" column and list only the installed components.

2. System Testing: Comply with "Test Methods" Table in the "Testing" Section of the "Inspection, Testing and Maintenance" Chapter in NFPA 72.

3. Test audible appliances for the public operating mode according to manufacturer's written instructions. Perform the test using a portable sound-level meter complying with Type 2 requirements in ANSI S1.4.

4. Test visible appliances for the public operating mode according to manufacturer's written instructions.

5. All intelligent addressable devices shall be tested for current address, sensitivity and user defined message.

6. Factory-authorized service representative shall prepare the "Fire Alarm System Record of Completion" in the "Documentation" Section of the "Fundamentals of Fire Alarm