Division 28 - Electronic Safety and Security

28 13 00 Access Control – Housing Only

Electronic Access Control Requirement Preamble:

It is the request of George Mason University (GMU) for the Security Integrator to be pre-approved from their preferred vendor list and to have an office and warehouse facility within a seventy-five (75) mile radius of the Fairfax campus of GMU. **No exception will be permitted**. GMU reserves the right to reject any Security Integrator they believe cannot fulfill the Quality Assurance requirements as specified within Section 281300. Cross reference with Section 087100 for proper coordination of this section. Section 281300 is **NOT** part of the Electrical Contractor's package, except where noted.

Any Finish Hardware or Electronic Access Control item provided that does not fulfill the owner's requirements, shall be removed and replaced at the no expense to the owner. All internal corridor doors must be tied into the fire alarm system and "Fail Safe" upon activation of fire alarm system. All exterior doors will fail secure. All access control is also to be tied into the emergency generator for seamless operation in the event of power loss.

1. Related Documents
    - Drawings and general provisions of the Contract, including General and Supplementary Conditions and Division 01 Specification Sections, apply to this Section.
2. Summary
    - Retain items below that are included in this Section, or include others as necessary.
        1) Section includes the following for the integrated access control security and site management system:
        2) Electrified and Integrated Access Control Door Hardware.
        3) Monitoring and Signaling Equipment.
        4) System Network Control Processors.
        5) Reader Controller Interfaces and Modules.
        6) Input Monitor and Output Control Interfaces and Modules.
        7) Card Readers.
        8) Multiplexers and Channel Input and Relay Modules.
        9) Cards and Credentials.
        10) Access Control System Application Software.
        11) Electrified Hardware and Access Control System Power Supplies, Back-Ups and Surge Protection.
    - Related Sections:
        1) Retain Division Sections below related to this Section, or include others as necessary.
        2) Division 08 Section 081100 "Steel Doors and Frames."
        3) Division 08 Section 081400 "Flush Wood Doors."

4) Division 08 Section 084100 "Aluminum-Framed Entrances and Storefronts."

5) Division 08 Section 087100 "Door Hardware".

6) Division 14 Section "Elevators" for security access to elevator floor selection controls.

7) Division 26 Sections (inclusive) for connections to electrical power system and for low-voltage wiring work.

8) Division 27 Section "Communications Horizontal Cabling" for connections to LAN.

9) Division 28 Section "Conductors and Cables for Electronic Safety and Security."

10) Division 28 Section 281600 "Intrusion Detection."

11) Division 28 Section 282300 "Video Surveillance."

12) Division 28 Section 283100 "Fire Detection and Alarm."

- References:

1) ANSI A117.1 (1998) - Accessible and Usable Buildings and Facilities.

2) IBC [2003, 2006] - International Building Code.

3) NFPA 70 (2002) - National Electrical Code.

4) NFPA 80 (1999) - Fire Doors and Windows.

5) NFPA 101 (2006) - Life Safety Code.

6) VUSBC Chapter 10 Means of Egress. To achieve compliance with the VUSBC; the Access/ Security Control Locking Systems (the complete system in its entirety) is to be *UL listed* for the specific application, or submit documentation that demonstrates that each of the components are listed for the intended use and that per the manufacturer's documentation the specific components are compatible with each other.

7) UL 294 - Access Control Systems.

8) UL 1076 - Proprietary Burglar Alarm Units and Systems.

- Products furnished, but not installed, under this Section include the following. Coordinating, purchasing, delivering, and scheduling remain requirements of this Section.

1) Patented and security construction keyed cylinders required for mechanical override access. In new construction, permanent cores are to be installed by the EAC sub contractor or his designee in consultation and direction from owner. Any cut hard keys accompanying the cores will be turned over to owner. In renovated buildings using existing cores, the owner will re install cores.

3. Submittals

- Product Data: Manufacturer's product data sheets including installation details, material descriptions, dimensions of individual components and profiles, operational descriptions and finishes.

- Shop Drawings: Details of electrified integrated locking hardware and access control firmware, indicating the following:

1) Wiring Diagrams: Upon receipt of approved schedules, submit detailed system wiring diagrams for power, signaling, monitoring, communication and control of the access control system electrified hardware and firmware. Differentiate between manufacturer-installed and field-installed wiring. Include the following:

a. Complete (risers, point-to-point) access control system block wiring diagrams.

b. Elevation diagram of each unique access controlled opening showing interconnection of major system components.

c. System Operational Descriptions: Include description of component functions including, but not limited to, the following situations: normal secured/unsecured state of door; authorized access; authorized egress; unauthorized access; unauthorized egress; fire alarm and loss of power conditions, and interfaces with other building control systems.

- Operating and Maintenance Manuals: Provide manufacturers hardware, software, operating and maintenance manuals for each item comprising the complete access control and site management installation in quantity as required in Division 01, Closeout Submittals. The manual to include the name, address, and telephone number of the supplier/integrator providing the installation and the nearest service representatives for each item of equipment included in the system. The final copies delivered after completion of the installation test to include "as built" modifications made during installation, checkout, and acceptance.

1) As-Built Drawings: During system installation, the Contractor to maintain a separate hard copy set of drawings, elevation diagrams, and wiring diagrams of the access control system to be used for record drawings. This set to be kept up to date by the Contractor with all changes and additions to the access control system accurately recorded.

- Warranties and Maintenance: Special warranties and maintenance agreements specified in this Section.

4. Quality Assurance

- Manufacturers Qualifications: Engage qualified manufacturers with a minimum (5) years of documented experience in providing access control and security systems equipment and software similar to that indicated for this Project and that have a proven record of successful in-service performance.

1) Software and access control systems components to have been previously and thoroughly tested together with proven installations similar in size and functionality to the design requirements indicated for this Project.

- Installer Qualifications: Factory trained and certified Systems Integrators, acceptable by the product manufacturers, with a minimum five (5) years documented experience installing complete integrated access control systems similar in material, design, and scope to that indicated for this Project and whose work has resulted in construction with a proven record of successful in-service performance. Qualifications include, but are not necessarily limited, to the following:

1) References: Provide a minimum of five (5) references for similar projects including contact name, phone number, name, and type of project. Two of the five references provided must be projects that consisting of one hundred (100) or more card readers installed during the base project.

2) Professional Staffing: Firms to have a dedicated access control systems integration department with full time, experienced professionals on staff

experienced in providing on site consulting services for both electrified door hardware and integrated access control systems installations.

3) Factory Training: Installation and service technicians are to be competent factory trained and certified personnel capable of maintaining the system. Vendor must be certified by the software manufacturer and must provide certifications from for Advance Level 2 Training.

4) Service Center: Firms to have a service center capable of providing training, in-stock parts, and emergency maintenance and repairs at the Project site with 24-hour/7-days a week response time, with a maximum of a 4 hour emergency response time on site.

5) Software/Integrator/Technicians/ Programmers must be, at a minimum, 2003 Microsoft Certified Systems Engineers (MCSE). (Not installers of Hardware)

6) Vendor must have an internal Technical Support Department staffed with a minimum of at least (3) technical support specialists whose sole job function is to support GMU on high level software related issues. This staff must be separate from installation and service technicians.

7) The Vendor preferably has previous “on-site” experience of the GMU campus and the existing security system(s).

8) All work must be performed directly by the Vendors own internal employees. No work is to be performed by subcontractors.

9) To ensure quality assurance and best of practice installation methods, Vendor must be UL2050 certified for security systems installation. A current copy of this certification must be provided with bid response.

10) Vendor must provide proof of being in business for at least ten (10) years.

- Supplier Qualifications: Factory authorized Supplier/Dealers, in good standing with the primary product manufacturers, with a minimum (3) years experience supplying integrated access control systems similar in material, design, and scope to that indicated for this Project and whose work has resulted in construction with a proven record of successful in-service performance.
- Supplier Certifications: Security Integrators must provide valid certificates from the specified manufacturers listed in this section in order to be pre-qualified to bid on this project.
- Source Limitations: Obtain each type and variety of electrified door hardware and access control system firmware and software from a single source, qualified supplier unless otherwise indicated.

  1) Provide electrified integrated door hardware from the same manufacturer as mechanical door hardware, unless otherwise indicated. Electrified modifications or enhancements made to a source manufacturer's product line by a secondary or third party source will not be accepted.

- Regulatory Requirements: Comply with NFPA 70, NFPA 80, NFPA 101 and ANSI A117.1 requirements and guidelines as directed in the model building code including, but not limited to, the following:

  1) Comply with NFPA 70 "National Electrical Code", including electrical components, devices, and accessories listed and labeled as defined in Article 100 by a testing agency acceptable to authorities having jurisdiction, and marked for intended use.

2) Where indicated to comply with accessibility requirements, comply with Americans with Disabilities Act (ADA), "Accessibility Guidelines for Buildings and Facilities (ADAAG)," ANSI A117.1.

3) Comply with NFPA 80 "Fire Doors and Windows" for fire labeled opening assemblies.

4) Comply with Virginia Uniform Statewide Building Code.

5) The installed access control system shall conform to all local jurisdiction requirements.

- Pre-Installation Conference: Conduct conference in compliance with requirements in Division 01 Section "Project Meetings" with attendance by representatives of Supplier/Dealer, Systems Integrator, and Contractor to review proper installation methods and the procedures for receiving and handling the access control system hardware. At completion of installation, provide written documentation that components were applied to manufacturer's instructions and recommendations and according to approved schedules.

  1) Inspect and discuss Division 26 electrical roughing-in and similar preparatory work performed by other trades.

  2) Review and verify sequence of operation descriptions for each unique access controlled opening.

  3) Review and finalize construction schedule and verify availability of materials.

  4) Review the required inspecting, testing, commissioning, and demonstration procedures.

5. Delivery, Storage, And Handling

- Do not store electronic access control hardware, software, or accessories at Project site without prior authorization.

  1) Access control firmware and software: Where approved and directed, inventory upon receipt and store electronic access control equipment in a secure, temperature and humidity controlled environment in original manufacturer's sealed containers.

- Tag each item or package separately with identification related to the final Access Control Door Schedule, and include basic installation instructions with each item or package.

- Deliver permanent keys, cores, access control credentials, software, and related accessories directly to Owner via registered mail or overnight package service. Instructions for delivery to the Owner established at the “Pre-Installation Conference".

6. Coordination

- Coordinate quantity and arrangement of assemblies with ceiling space configuration and with components occupying ceiling space, including structural members, pipes, air-distribution components, raceways, cable trays, recessed lighting fixtures, and other items.

- Access Control System: Coordinate with the appropriate trades the layout and installation of scheduled electrified door hardware and access control equipment with required connections to source power junction boxes, power supplies, sealing of fire penetrations, detection and monitoring hardware and fire alarm system.

- Templates: Obtain and distribute to the parties involved templates for doors, frames, and other work specified to be factory prepared for installing electrified door hardware and access control system components. Check Shop Drawings of other work to confirm that adequate provisions are made for locating and installing access control system hardware to comply with indicated requirements.
- Door and Frame Preparation (New Doors/Frames only): Related Division 08 Sections (Steel, Aluminum and Wood) doors and corresponding frames are to be prepared, reinforced and pre-wired (if applicable) to receive the installation of the specified electrified, monitoring, signaling and access control system hardware without additional in-field modifications.

7. Warranty

- General Warranty: Reference Division 01, General Requirements. Special warranties specified in this Article will not deprive Owner of other rights Owner may have under other provisions of the Contract Documents and are in addition to, and run concurrent with, other warranties made by Contractor under requirements of the Contract Documents.
- Warranty Period: Written warranty agreeing to repair or replace components of the installed access control system hardware and software that fail in materials or workmanship, including all related parts and labor, for a minimum period of (24) months after final testing and acceptance by the Owner. Failures include, but are not limited to, the following:

  1) Structural failures including excessive deflection, cracking, or breakage.

  2) Faulty operation of the hardware.

  3) Deterioration of metals, metal finishes, and other materials beyond normal weathering.

  4) Electrical component defects and failures within the systems operation.

- Special Warranty Periods (Electrified Access Control Door Hardware):

  1) Two years for Electrified, Wiegand Output, and IP-Enabled Access Control Door Hardware.

- Support and Extended Service Agreement: Submit for Owner’s consideration an optional extended service agreement for the installed access control system, including support for software related issues. The extended service agreement is considered elective without a manufacturer's requirement stipulating mandatory annual agreements covering owner and/or vendor system support.

  1) A published copy of this agreement to be included with the submittal package

  2) Support for the installed access control system components is provided through the vendor under a 24 hour technical assistance program.

  3) Access control and management system components are to be available on a one-day turnaround time frame from the manufacturer.

  4) Primary systems manufacturer to offer and provide remote modem or internet access for direct factory support to the vendor. The factory level support to include diagnostics and troubleshooting support on systems related issues at no additional cost to the owner.

- Access Control Software Upgrades: Version upgrades and "fix" releases to the access control system software are available at no extra charge as long as the

version of software provided under this specification remains the current manufacturer's version or for up to (2) years after a new version release.

1) Major access control software revisions that provide new functionality to the product provided free of charge for up to one (1) year from the date of substantial completion.

2) Access control system software is to be upgradable as may be required or as necessary, to expand, and manage the owner's site or sites. Upgrades are to be offered at a published flat fee for the primary system software, with single license modules included in the primary fee structure. System upgrades offered at a costing structure based upon the original number of licensed modules issued, or on those to be purchased at a future date, are not allowed.

3) As part of the submittal package, provide a list of available software upgrades and/or expansions modules. List to identify related costs for upgrades, or expansions to the original system, up to the next qualifying operational level.

8. Maintenance Service

- Maintenance Tools and Instructions: Furnish a complete set of specialized tools and maintenance instructions as needed for Owner's continued adjustment, maintenance, and removal and replacement of the installed access control system hardware and components.

- Maintenance Service: Beginning at Substantial Completion, provide continuous (6) months full maintenance by skilled employees of the Systems Integrator. Include preventive maintenance, repair, or replacement of worn or defective components, lubrication, cleaning, and adjusting as required for proper door opening operation. Provide parts and supplies as used in the manufacture and installation of original products.

9. Scope of Work

- Furnish and install at the indicated locations the specified electrified and integrated door hardware and access control firmware and software for a completely operational access control and security site management system. The proposed system MUST be able to fully and seamlessly integrate into GMU Housing's current access control system**. Please note that ALL doors (with a few exceptions noted by owner) WILL have some form of electronic access control installed. With very few exceptions, exterior doors will be hard wired, online lock with readers, while interior doors will be wireless, online locks.**

- Installation requirements:

1) Security Contractor: All Access Control components as specified within Section 281300 will be furnished and installed as a turnkey system by an Single Security Contractor; including but not limited to the following items: Access Control Software, licensing, Access Control Panels, Input/Output Panels, Card Readers, Electrified Locking Hardware, Power Supplies, Door Contacts, Request-to-exit Devices and all low voltage wiring, including final terminations of all security devices at both ends as well as door operators, if applicable. In addition, the Security Contractor must include any and all licensing as required to fully operate the system.

- System includes, but is not necessarily limited, to the following:

1) Electrified integrated card reader locks and exit hardware, override cylinders, network control processors, reader controller panels, I/O monitor/control

interfaces, door position switches, remote card readers and display terminals, access cards and credentials, system application software, special tools, operating manuals, and required cabling and accessories as detailed below and listed in the Access Control Hardware Sets at the end of Part 3.

a. Provide the appropriate number of reader controller panels and I/O monitoring/control expansion interfaces as needed to handle the number of card readers, locking devices, door status devices, and identified alarm inputs specified in this section, and as shown on the security drawings.

b. Provide manufacturer approved integrated card reader locks, exit hardware, and remote mounted card readers [mullion, jamb, wall mounted] that are functionally compatible with the specified access control equipment interfaces.

c. All doors with card readers shall permit free egress at all times to comply with the Virginia Uniform Building Code and BOCA.

d. All doors specified to receive electrified locking hardware shall have the function of either a night latch or storeroom; if a key override is used the electrified locking hardware will remain in a locked state.

e. All doors specified to receive electrified locking hardware shall be provided with an electric hinge. Armored door loops will not be accepted by the owner.

f. All doors specified to receive card readers shall also have door contacts to monitor the door position and request-to-exit devices to shunt the door contact upon exit. Request-to-exit devices shall be integrated into the electrified locking hardware. Wall mounted passive infrared request-to-exit devices can only be used if they cannot be integrated into the electrified locking hardware.

g. Magnetic locks are not an acceptable electrified locking method unless they are required to satisfy Building Codes.

- Access control system equipment to be installed in an enclosure box compatible with the specified components. This enclosure to include, but is not necessarily limited to, the network control processor, I/O monitor/control interface panels, power supplies, terminal strips, wire ducts, keyed lock cylinder, integrated outlet for A/C power, and standoffs.

  1) Enclosure box to be located in a designated Housing Server room(s) with connection to the campus wide local area network for communication back to the central server host.

- Owner to provide necessary computer hardware and network consisting of:

  1) Central Server Host Computer

  2) Client Workstations

  3) Owner will be responsible for ensuring that each computer hardware component includes the required interfaces, expansion boards, and peripherals that will be necessary to allow the system to operate as described within this specification and as indicated on the drawings.

  4) Network Control Processor Connections

- Power Supplies, including battery backup and separately fused surge protection, required for the electrified door hardware and access control equipment.

- Installation, final configuration, and commissioning of electrified door and access control system hardware, communication firmware, power supplies, and related accessories.
- System application software including installation, programming, and end user training of the access control system demonstrating operating, repair and maintenance procedures. Include no fewer than 8 hours of on-site central server training for designated personnel (facilities maintenance, security, IT, administration) by a factory certified representative.

  1) Include minimum of 4 hours of Client Software Application (client workstation) training at each of the remote installed facilities for local administrative staff.

- Provide manufacturer required power controllers, interface boards, and programming that may be required for approved electric latch retraction exit devices supplied under this Section.
- Electrical contractor (Division 26) to provide the following for New Construction:

  1) Source power wiring (120VAC) as required for the electrified locking and access control hardware, equipment, accessories, and power supplies. This includes quad outlets as required on a dedicated circuit in the designated HOUSING server room (separate room from the GMU/ITU Telecom room) and the related conduit, stub-in, junction and back boxes, pull strings and connectors required for the source power delivery and connections.

  2) Provide required conduit, stub-in, junction and back boxes, pull strings and connectors for both the electrified locking hardware and access control equipment at each of the access controlled or monitored openings per plan drawings and specs. Supply and install conduit between each of the aforementioned devices and between the electrical junction boxes, power supplies, and access control equipment located on or above the door opening.

     a. At wall mounted remote readers, provide conduit on the secured side of the door, 36" from the finish floor and 6" from the edge of the frame, to the related power supplies and access control equipment.

     b. At electrical hardware power transfers provide conduit on the secured side of the opening from the power transfer, thru-wire hinge, or serviceable panel location on the frame jamb to the related power supplies and access control equipment.

  3) Electrical Contractor to provide all 120VAC cabling connections and terminations from the electrical junction boxes to these electrical devices.

  4) All electronic access control 120VAC power shall be tied into the Emergency Power circuit by the Electrical Contractor.

- Access Control System Integrator to provide the following:

  1) Low voltage wiring (12/24VDC) and communication cabling (RS-232/RS-485) from network control processors to reader controllers, I/O monitor/control interface panels, electrified and integrated locking hardware, remote card readers, keypads, or display terminals, monitoring and signaling switches, and power supplies. Work includes related connectors, final terminations, and hook-ups required for a complete and functional access controlled opening in accordance with applicable codes and specified system operational narratives.

- Elevator Contractor to provide the following:

  1) Interface or landing of interface cable onto the elevator call button will be performed by a certified elevator contractor.

2) Coordinate with access control systems integrator provisions for a card reader with output allowing the elevator call button to be activated. A validated card read will be required for activation.

- Final connections to fire alarm system, if required, by electrical and fire alarm system contractors.
- Provide permits, submittals, and approvals required by the authority having jurisdiction, prior to commencing with work.

10. System Architecture - Access Control and Site Management System (Acsms)

- General: The ACSMS must utilize the existing system in place at George Mason University. The ACSMS is a modular and networked based system providing physical access control security to a Wide Area campus enterprise. The system to be capable of controlling and integrating multiple security functions including the configuration, management and monitoring of cardholder access, locking hardware units, events, alarms, visitors, and real-time tracking and reporting. The ACSMS is to be alterable at any time depending on the facility requirements and will allow for easy upgradeability or modification of network processors, controller, interface modules, card data, inputs, outputs, and remote work stations. The ACSMS to include, but is not be limited to, the following features and functions:

1) An "Enterprise" class access control software application.

2) Client/Server model operating central server host software modules and client workstation software applications in a multi-user and a multi-tasking environment.

a. The ACSMS to permit multiple instances of client software applications to run simultaneously on the network. The base system to include 3 single client and 3 web client software application licenses.

3) Partitioning: The system to support security partitioning enabling system administrator to segment the configuration database and group multiple entities within the security partition.

a. Security partitions limit what users can view in the configuration database. Administrators, who have all rights and privileges, can segment a database into multiple security partitions. A user who is given access to a specific partition will only be able to view entities (components) within the partition they have been assigned.

4) Encryption: The system to support encrypted communication between the central server software and client software applications (sever-to-server and client-to-server) using a 128-bit AES encryption algorithm (at a minimum). Systems that do not provide encrypted communication will NOT be considered.

a. Communication between the central server host software module and system controllers are to be encrypted.

b. The ACSMS client software applications to be password protected with passwords stored in the central server database in an encrypted manner.

5) Distributed Processing: The system is a fully distributed processing application allowing information, including time, date, zones, valid codes, tasks, access levels, and similar data, to be downloaded from the central host station to controller interface devices allowing access-control decisions with or without central host station communication. If communications to a central host station are lost, the controllers will automatically buffer event transactions until

communications are restored and events are automatically uploaded to the central host station.

a. Provide for a higher level of distributed database management at defined perimeter access points such that no-single-point-of-failure will allow more than two access points to fail, or affect more than two access points at perimeter points system wide.

6) Single Data Base: The system to support a single database for access control site setup, credential and identity file creation, alarm and control setup, and system user operation and command functions.

7) System Access Management: The system to allow operators through password authentication the ability to make access granted or denied decisions, define access levels, time zones, holidays, assign cardholders, access groups, develop tasks, and generally manage access control, alarm monitoring and response activities system wide from a single login. Operator and user privileges are managed by a system administrator allowing for different levels of system access and system control. Authorization management is fully Owner definable.

8) Cardholder Management: The system to include a cardholder management system integrated within the access control system. This cardholder management functionality allows the enrollment of cardholders into the database, and import/export of employee data.

9) Access Groups and Access Levels: The system to provide adequate access groups and access level assignment capability to meet Owner requirements for the specified project. If required, software application can be expandable to support unlimited access groups and access levels.

10) Alarm Monitoring: The system is able to monitor, report, and provide information about the time and location of alarms, along with their priority.

11) Event Monitoring: The system is able to monitor, report, and archive network access control activity.

12) Transaction Logs: The system to support an unlimited number of logs and historical transactions (events and alarms) with the maximum allowed being limited by the amount of hard disk space available.

13) System Monitoring: The system to have ability to report on the integrity of all network assigned devices, circuits and communications and provide a diagnostics screen showing field level communications system wide

14) Lock/Unlock Commands: The system to allow an operator to manually lock and unlock doors overriding scheduled access control restrictions and configurations if necessary.

15) Hardware Interface: The system to integrate with and control specified electrified hardware, signaling and monitoring devices.

16) Report Generator: The system to have the ability to generate and output reports with any and all combinations of system fields and data including, but not limited to: by cardholder, by door, by site, by time, by groups of doors and by cardholder field. Any and all combinations of fields must be available for reporting. The report feature to allow exporting of generated reports over a network connection or by remote printing.

17) Multi-User/Web Based Network Capabilities: The system to support multiple operator workstations via local area network/wide area network (LAN/WAN),

the Internet, or VPN. The system to be capable of supporting minimum of 4 concurrent users/clients with software expansions to an unlimited number of workstations based on the Owners network requirements.

18) Systems Integration: The system shall be fully and seamlessly integrated with the specified video surveillance (CCTV) systems in Section 282300.

- Open Architecture: The access control system infrastructure will be based on an open architecture design capable of supporting multiple access control hardware manufacturers and integrate with multiple non-proprietary network processors, controllers, interface modules, integrated locking hardware, remote card readers, keypads and display terminals, and other third party applications.
- Open Protocol: The ACSMS manufacturer to provide non-proprietary, open protocol hardware for the system control processors and associated device sub-controllers. Systems utilizing a single manufacturer solution that encompasses combined proprietary software and integrated electronic hardware combinations are not acceptable. In addition, integrated electronic locking hardware requiring a processor or sub-controller module upgrade, or extensive access control firmware upgrades to accommodate integrating with an alternate software package, will not be considered.
- Network Support: Communication network connecting the central server host software modules, client workstation software applications, and hardware controllers to be designed to support all of the following:

  1) LAN/Ethernet enterprise ring topology and localized star topology based on TCP/IP.

  2) Direct-connected RS-232 and RS-485 communication cabling.

11. Manufacturers

- General: Provide integrated electrified door hardware and access control system equipment and accessories for each designated opening to comply with requirements in this Section and with the Access Control Hardware Sets listed at the end of Part 3.

  1) Access Control Hardware Sets: Requirements for quantity, item, model, design, grade, finish, size, and other distinctive qualities of each type of electrified door and access control hardware are indicated in the Access Control Hardware Sets at the end of Part 3.

  2) Named Manufacturer's Products: Product designation and manufacturers are listed for the purpose of establishing requirements**.**

- System Design: The equipment and materials supplied are standardized components regularly manufactured and utilized within the source manufacturer’s access control systems.

  1) System components (electronic integrated locking hardware) to be non-proprietary in design and implementations, providing for an open protocol platform with multiple manufacturers having functional software capable of integrating with the hardware specified. The installed integrated product is to be part of a single, cohesive management and access control system.

- Substitutions: Requests for substitution and product approval for inclusive integrated electronic door hardware and access control systems in compliance with these specifications must be submitted in writing and in accordance with the procedures and time frames outlined in Division 01, Substitution Procedures. Approval of requests is at the discretion of the architect, owner, and their designated consultants.

- GMU currently uses the following Access Control and Site Management System Manufacturers

  1) RS2 Technologies. (Access Control System Control Processors, Reader Controllers, I/O Monitor/Control Modules, Entry/Display Terminals, Multiplexers, Channel Input/Output Modules, System Application Software)

  2) Mercury Hardware (Remote Card Readers)

  3) Sargent Manufacturing (Integrated Card Reader Locking Devices and Accessories)

  4) Altronix (Power Supplies)

12. Access Control and Site Management System Hardware

- General: Provide all necessary access control field hardware devices required to receive alarms and administer all access granted/denied decisions. Field hardware devices must be designed to meet UL 1076 and UL 294 standards and installed in accordance with applicable electrical codes.

  1) The access control system to interface and be connected to electronic door control hardware not specified in this section (electrified exit devices) and as described under Division 8 "Door Hardware".

- Central Computer Host Server (Owner Provided): The central server is interconnected to all system components, including client workstations and field installed controllers, providing operator interface, interaction, display, control, and real-time monitoring.

- System Control Processor Dual Reader Interface: The System Control Processor (SCP) Dual Reader Interface is a 32-bit micro-controller utilized as the enhanced management processor between down line access readers, input monitors and relay output modules, and the host system and software.

  The SCP Dual Reader Interface supports up to (2) security industry standard reader communication and control ports. Each port terminates with industry standard access control readers, data entry/display terminals (keypad with display), and/or integrated reader-in-trim locking units for authorized access and egress management. Each SCP access port will include supervised portal monitoring (door status), request to exit monitoring (manual or automated inputs) and electrified lock output control.

  The SCP must meet the following, minimum, design, and performance specifications.

  1) Internal memory minimum of 16 Mbytes with a minimum of 6 Mbytes of memory set aside for user configuration.

  2) Support for up to (32) I/O module addresses.

  3) Capacity for up to, and in any combination, 64 reader locations including status/ position monitoring, egress request automation and electric lock control, (512) input monitoring points, and (512) relay output points.

  4) User selection of serial, dial-up and/or Ethernet (TCP/IP) communications to the host computer with the specified system software. No external network card or attachment is required for the SCP to connect to the host system on a conventional Ethernet. Users have the ability to connect with the SCP using static IP or DHCP conventions.

  5) Provide 128-bit AES data encryption with the host system.

6) On-board Network Interface Circuit (NIC) supporting 10/100-BaseT automation.

7) Support a minimum of (8) active card formats per processor.

8) Support anti-pass back functions including free pass, exempt flags, last area accessed, last reader accessed and time and date of last access.

9) Support area management functions including two man rules, two card rules, multiple occupancy, maximum occupancy, and nested areas. Area management functions defined in minimum of (32) Access Area assignments per SCP. Access Areas shall be treated within the system as a single logical point and any controls applied manually or by automation will apply to all of the access points assigned within the Access Area.

10) Support alarm management functions incorporating inputs and reader events into Alarm Zones allowing the zones to be armed and disarmed creating various user definable events that are supported in SCP tasks and host macro processing. Support a minimum of 64 fully user configurable Alarm Zones per processor.

11) Alarm management to provide task as well as arm/disarm functionality using a standard keypad/display terminal/card reader with features for user command and key selection. Support down loads to the display of the keypad for date and time, zone status, error messages and special text messaging defined by the user.

12) Support up to (256) user definable tasks configured to execute pre-defined process commands in response to manual user commands, input or event changes, time zone activations, automated commands or Macro operations.

13) Support up to (256) user definable user commands configured to execute pre-defined process commands in response to manual user commands, input or event changes, time zone activations, automated commands or Macro operations.

14) Allow variable stored transaction storage from 1,000 to 100,000 events per SCP.

15) Allow variable local card database storage from 5,000 to 250,000 records per SCP.

16) Operational programming is stored in non-volatile Flash Memory allowing for on-line program upgrades.

17) Provide on board memory battery backup to retain all database information during a complete power loss for up to sixty (60) days, per manufacturer's specifications.

18) Provide ports for tamper and power failure notification.

19) Provide status LED's for heartbeat, battery status, upstream communication, and downstream communication.

20) Utilize two-wire RS-485 communications. The minimum data rate is 38,400KBps at IEEE standards for up to 4000 feet for interconnection to up to (31) access reader, monitor input and relay output modules.

The SCP Dual Reader to support the following:

21) Support up to (2) security industry standard readers, data entry/display terminals (keypad with display), and/or integrated reader-in-trim locking units for access or egress authorizations.

22) Reader ports to provide up to 150 mA of unregulated 12 VDC power for each reader. At a minimum card/data input support to be Wiegand, TTL or RS-485 format. Single and dual wire LED output provided supporting bicolor display and reader buzzer support.

23) Provide (8) on-board fully supervised monitoring points (inputs). Monitoring points configured as follows: (2) monitoring points dedicated for access portal status (door contact inputs) one per reader port. (2) monitoring points dedicated for exit request inputs (manual or automated egress) one per reader port. (4) monitoring points as auxiliary and fully user defined for monitoring other devices or points within the site.

24) Input monitoring point settings are user defined as normally open, normally closed, or supervised normally open or normally closed. At a minimum input supervision to be a series parallel 1/4W, 1%, 1K by 1K Ohm resistor circuit.

25) Provide (4) on-board output relays for controlling electrified devices or switching inputs. Relays configured as follows: (2) relays dedicated for electric portal locking device control one per reader port. (2) relays as auxiliary and fully user defined for controlling or switching other devices or points within the site.

26) Output relays are Form-C, 5A@30 VDC, resistive relays.

27) Output relays allow configuration for fail safe or fail secure operation and support ON, OFF, and PULSE, command states.

- Access Control Dual Reader Input/Output Module: System Control Processor (SCP) to provide distributed processing and management for each Dual Reader I/O Module incorporated in the system Dual Reader I/O Module to meet the following, minimum, design and performance specifications:

  1) Support security industry standard magnetic, Wiegand, and proximity and specified biometrics readers.

  2) Support integrated reader-in-trim locking units, keypads, and keypad readers.

  3) Support connectivity and interface with system arm/disarm functionality using a standard keypad/display terminal/card reader with features for user command and key selection. Support down loads from the SCP to the display of the keypad for date and time, zone status, error messages and user defined special text messaging.

  4) Hardware interface and card format settings to be loaded through software commands from the specified system software to associated SCP modules to each Dual Reader I/O Module.

  5) Support up to (2) security industry standard readers, data entry/display terminals (keypad with display), and/or integrated reader-in-trim locking units access or egress authorizations.

  6) Support different reader technologies on the same module, user defined.

  7) Reader ports to provide up to 150 mA of unregulated 12 VDC power for each reader. At a minimum card/data input supports Wiegand, TTL or RS-485 format. Single and dual wire LED output shall be provided supporting bicolor display and reader buzzer support.

  8) Provide (8) on-board fully supervised monitoring points (inputs). Monitoring points configured as follows: (2) monitoring points dedicated for access portal status (door contact inputs) one per reader port. (2) monitoring points dedicated

for exit request inputs (manual or automated egress) one per reader port. (4) monitoring points as auxiliary and fully user defined for monitoring other devices or points within the site.

9) Input monitoring point settings are user defined as normally open, normally closed, or supervised normally open or normally closed. At a minimum input supervision shall be a series parallel 1/4W, 1%, 1K by 1K Ohm resistor circuit.

10) Provide (6) on-board output relays for controlling electrified devices or switching inputs. Relays configured as follows: (2) relays dedicated for electric portal locking device control one per reader port. (4) relays as auxiliary and fully user defined for controlling or switching other devices or points within the site.

11) Output relays are Form-C, 5A@30 VDC, resistive relays.

12) Output relays to allow configuration for fail safe or fail secure operation and support ON, OFF, and PULSE, command states.

13) In the event of a communication failure with a System Control Processor (SCP), the Dual Reader I/O Module capable of locally processing access requests based on facility code verification.

14) Operational programming is stored in non-volatile Flash Memory allowing for on-line program upgrades.

15) Utilize two-wire, RS-485 communications with data rates up to 38,400KBps up to an IEEE standard of 4000 feet.

16) Up to (32) Dual Reader I/O Modules are allowed to connect with any SCP within the system.

- Access Control Panel Enclosures: Access control panel enclosures as required for the System Control Processors and Dual Reader Input/Output Modules must be approved to meet the design standards of GMU security personnel prior to being installed on-site. The access control panel enclosure to meet the following, minimum, design, and performance specifications.

  1) NEMA Type 1 lockable enclosure, 36” x 24” x 5”.

  2) Completely wired for board power, RS485 communications, and door control.

  3) Complete wire management system.

  4) 12/24 VDC 20 A power supply/charger with door control relay board and fire alarm interface.

  5) 110 VAC Dual outlets with illuminated reset switch/breaker.

  6) Each Panel must include a sticker inside the enclosure listing the following:

     a. Vendor name, Installation Date, Service Phone number

     b. Warranty expiration dates for both parts and labor

- On-Line Wireless (Wi-Fi) Networked Locking Mortise Devices:

  1) Mortise Lockset: BHMA certified extra heavy duty, lever type mortise lock conforming to ANSI 156.13 Series 1000, Grade 1 standard and meeting ANSI A117.1 accessibility guidelines. Motorized locking control with 3/4" anti-friction deadlocking latch and 1" case-hardened steel deadbolt. UL listed and labeled for up to 3 hour fire rated openings. Locks must include the latest version of firmware from the vendor BEFORE installation at the job site.

2) Completely intelligent and integrated locking unit with on-board memory and network communication capability directly from the lock back to the central system server via an 802.11b/g wireless network.

   a. Communication from the lock back to the central system server does not require additional access control hardware or components to be able to interface into the network (excluding wireless access point).

3) Networked locks are able to read, analyze, and control access to level of authorization encoded on keycard. Centralized control allows updating of user permissions, and retrieval of audit trails (event history) and alarm reporting over a communication network without having to visit each lock unit.

   a. Users per door: 2,000.

   b. Audit trail maintained by lock: 10,000 events

   c. Time schedules: 32

   d. User Groups: 32

   e. Exception Periods (holidays): 64

4) Access by vertical swiping of magnetic stripe card and/or keypad pin number or by vertical swiping of magnetic stripe card only.

   a. Card track: Track 2

5) Monitoring and Signaling: Latch bolt, auxiliary latch, request-to-exit, door position status (requires hard wiring option). Provide alarm monitoring capability including door forced, door propped, access denied, and low battery condition.

6) Emergency override access capability through system-generated special access keycards and keypad codes, which are time, date, and location specific.

   a. Provide mechanical key override capability with no electronic activation necessary for latch or lock retraction.

   b. Deadbolt overriding capability available from outside on any level keycard, keypad code, or mechanical key.

   c. ALL mortise cylinders must accept the “BEST” 7-Pin interchangeable cores

7) Inside lever retracts latch bolt and deadbolt simultaneously.

8) Locks to be water resistant on external installations with keypads having all metal external parts.

9) Power Supply: 6 AA alkaline batteries with a minimum typical life cycle of 1 to 3 years (approximately 65,000 transactions) depending on usage. Supervised with advance low capacity warning. Hard wiring power option available.

   a. Batteries and electronics, except card reader heads and keypads, to be sealed on secure side of door for security and exposure to weather.

10) Wireless Radio Requirements:

   a. Comply with IEEE 802.11b/g Wi-Fi standard for Wireless LAN communications.

   b. All wireless locks MUST be WPA2 compatible

c. Frequency Range: Worldwide product covering 2.4 to 2.5 GHz, programmable for different country regulations.

d. Maximum Output Power: 100 mW.

e. Power Management: Continuous aware power saving polling mode.

f. Supports AES-128 encryption for end-to-end link security.

g. 802.11b/g Wireless Access Point by Owner.

- On-Line Wireless (Wi-Fi) Networked Locking Cylindrical Devices:

1) Bored (Cylindrical) Lockset: ANSI/BHMA A156.2 Grade 1 bored lockset with integrated magnetic stripe card reader and request to exit signaling in one complete unit. Motor driven locking/unlocking control of the lever handle trim with ½ " deadlocking stainless steel latch lock is UL listed and labeled for use on up to 3 hour fire rated openings. Locks must include the latest version of firmware from the vendor BEFORE installation at the job site.

2) Completely intelligent and integrated locking unit with on-board memory and network communication capability directly from the lock back to the central system server via an 802.11b/g wireless network.

a. Communication from the lock back to the central system server does not require additional access control hardware or components to be able to interface into the network (excluding wireless access point).

3) Networked locks are able to read, analyze, and control access to level of authorization encoded on keycard. Centralized control allows updating of user permissions, and retrieval of audit trails (event history) and alarm reporting over a communication network without having to visit each lock unit.

a. Users per door: 2,000.

b. Audit trail maintained by lock: 10,000 events

c. Time schedules: 32

d. User Groups: 32

e. Exception Periods (holidays): 64

4) Access by vertical swiping of magnetic stripe card and/or keypad pin number or by vertical swiping of magnetic stripe card only.

a. Card track: Track 2.

5) Monitoring and Signaling: Provide alarm monitoring capability including door forced, access denied, and low battery condition.

6) Emergency override access capability through system-generated special access keycards and keypad codes (with keypad module (optional,)) which are time, date, and location specific.

a. Provide mechanical key override capability with no electronic activation necessary for latch or lock retraction.

b. ALL key override capabilities must accept the "BEST" 7-Pin interchangeable cores.

7) Locks to be water resistant on external installations with keypads having all metal external parts.

8) Power Supply: 6 AA alkaline batteries with a minimum typical life cycle of 1 to 3 years (approximately 65,000 transactions) depending on usage. Supervised with advance low capacity warning. Hard wiring power option available.

   a. Batteries and electronics, except card reader heads and keypads (if chosen,) to be sealed on secure side of door for security and exposure to weather.

9) Wireless Radio Requirements:

   a. Comply with IEEE 802.11b/g Wi-Fi standard for Wireless LAN communications.

   b. All wireless locks MUST be WPA2 compatible

   c. Frequency Range: Worldwide product covering 2.4 to 2.5 GHz, programmable for different country regulations.

   d. Maximum Output Power: 100 mW.

   e. Power Management: Continuous aware power saving polling mode.

   f. Supports AES-128 encryption for end-to-end link security.

   g. 802.11b/g Wireless Access Point by Owner

- Remote Card Readers: Access control remote card readers to interface with the access control reader modules and the door control hardware as specified in the Access Control Hardware Sets under Part 3. Card readers to meet the following, minimum, design, and performance specifications.

  1) Reader technology to be either magnetic stripe as required by Owner.

  2) Reader to be weatherproof type when installed in exterior or other wet environments.

  3) Reader to communicate with the reader I/O modules using industry standard Wiegand protocol interface.

  4) Reader to operate on 5VDC power from the reader I/O modules at a maximum current rating of 150 mA per reader.

  5) Card reader type and model to meet the design application need of each entry point as indicated on the drawings.

  6) Card readers will have an integrated tamper switch.

  7) All card readers must be installed with appropriate security screws

- Power Supplies: Provide UL294 and UL1481 Listed 12VDC or 24VDC (field selectable) filtered and electronically regulated power supplies. Provide the least number of units, at the appropriate amperage level, sufficient to exceed the required total draw for the specified electrified hardware and access control equipment.

  1) Provide short circuit and thermal overload protection.

  2) Provide battery backup with built-in charger for sealed lead acid or gel type batteries. Battery backup shall provide enough power for up to 1 hour of normal operation.

  3) Provide automatic switch over to stand-by battery when AC fails with zero voltage drop.

4) Provide low battery, battery presence, and AC fail supervision (form “C” contacts).

5) Rated for Fail-Safe and/or Fail-Secure operation.

6) Provide separate power supplies for locking power and control panel power.

13. Access Control and Site Management System Application Software

- The access control application software provides the interface for control and configurations of all access control points, monitors input points, and relay controlled outputs as indicated on the drawings and described in this specification.
- The basic access control application software for this project will tie into the existing campus wide system. Any licensing fees as required to expand the existing campus wide system are to be included as part of the turnkey system provided within this specification. At a minimum, vendor must provide 2 additional seat licenses to GMU.

14. Cables and Wiring

- Comply with Division 28 Section "Conductors and Cables for Electronic Safety and Security."
- All Access Control low voltage wire will be furnished and installed by Section 281300 Security Contractor.
- All low voltage wire shall be plenum rated and terminated at all door and panel locations.

15. Hardware Finishes

- Standard: Comply with BHMA A156.18.
- Protect mechanical finishes on exposed surfaces from damage by applying a strippable, temporary protective covering before shipping.
- Where specified, finishes on integrated card key locksets or exit hardware to incorporate an FDA recognized antimicrobial coating (MicroShield™) listed for use on equipment as a suppressant to the growth and spread of a broad range of bacteria, algae, fungus, mold and mildew.
- BHMA Designations: Comply with base material and finish requirements indicated by the following:

1) BHMA 626: Satin chromium plated over nickel, over brass or bronze base metal.

2) BHMA 628: Satin aluminum, clear anodized, over aluminum base metal.

3) BHMA 630: Satin stainless steel, over stainless-steel base metal.

16. Execution

- Examine scheduled openings, with Installer present, for compliance with requirements for installation tolerances, labeled fire door assembly construction, wall and floor construction, and other conditions affecting performance of the installed access control system.
- Examine roughing-in for electrical source power to verify actual locations of wiring connections before electrified and integrated access control door hardware installation.
- Examine pathway elements intended for cables. Check raceways and other elements for compliance with space allocations, installation tolerances, hazards to cable installation, and other conditions affecting installation.

- Examine roughing-in for LAN and control cable conduit systems to PCs, controllers, card readers, and other cable-connected devices to verify actual locations of conduit and back boxes before device installation.
- Notify architect of any discrepancies or conflicts between the specifications, drawings, and scheduled access controlled hardware. Proceed only after such discrepancies or conflicts have been resolved in writing.

17. Preparation

- Doors and frames at scheduled access controlled openings to be properly prepared to receive specified electrified and access control hardware and connections.

18. Installation

- Install each item of electrified door hardware and access control equipment to comply with manufacturer's written instructions and according to specifications.
- Mounting Heights: Mount integrated access control door hardware units at heights indicated in following applicable publications, unless specifically indicated or required to comply with governing regulations:
  1) Standard Steel Doors and Frames: DHI's "Recommended Locations for Architectural Hardware for Standard Steel Doors and Frames."
  2) Wood Doors: DHI WDHS.3, "Recommended Locations for Architectural Hardware for Wood Flush Doors."
  3) Where indicated to comply with accessibility requirements, comply with ANSI A117.1 "Accessibility Guidelines for Buildings and Facilities."
- Boxed Power Supplies: Verify locations.
  1) Configuration: Provide the least number of power supplies required to adequately serve doors with access control equipment.
- Install cables and wiring according to requirements in Division 28 Section "Conductors and Cables for Electronic Safety and Security."
  1) RS-232 Cabling: Install at a maximum distance of 50 feet.
  2) RS-485 Cabling: Install at a maximum distance of 4000 feet.
  3) Integrated Card Key Locking Hardware, Remote Card Readers, Keypads, and Display Terminals: Install appropriate number of conductor pairs, in the wire gage (AWG) recommended by manufacturer, corresponding to the electronic locking functions specified, amperage drawn, and distances covered between the power supplies, transfer hinges, electrified hardware, and access control equipment.
  4) All low voltage wire shall be plenum rated
- Final connect the system control switches (integrated card key locking hardware, remote readers, keypads, display terminals, biometrics), and monitoring, and signaling equipment to the related Controller devices at each opening to properly operate the electrified door and access control hardware according to system operational narratives.
- System Application Software: Install, and test application(s) software and databases for the complete and proper operation of systems involved. Assign software license(s) to Owner.

19. Field Quality Control

- Comply with AIA A201 1997, section 3.3.1, which reads as follows: "The Contractor shall be solely responsible for and have control over construction means, methods, techniques, sequences and procedures and for coordinating all portions of the Work under the Contract, unless the contract Documents give other specific instructions concerning these matters."
- Field Inspection: Engage a factory authorized service representative to perform a final inspection of the installed electrified door hardware and integrated access control system and state in report whether installed work complies with or deviates from requirements, including whether each component representing the opening assembly is properly installed, adjusted, operating and performing to system operational narratives.
- Commissioning and Testing Schedule: Prior to final acceptance of the access control system installation, the following testing and documentation will be performed by the integrator and the final results provided to the Owner.

  1) Inspection: Verify that units and controls are properly installed, connected, and labeled and that interconnecting wires and terminals are identified.

     a. Each reader input will be labeled with the appropriate door number

     b. Any auxiliary inputs and outputs will be labeled

     c. Power Supply location and outputs will be labeled

     d. Each Panel must have a typed address list of readers and boards located inside the panel. Listing will include: reader ID/Door number; Address; Fail Safe/Secure; Any special configurations; and locations of any external power supplies, if applicable. In addition, these lists will be duplicated and turned over to the owner for record.

  2) Pre-testing: Program and adjust the system and pretest all components, wiring, and functions to verify they conform to specified requirements. Provide testing reports indicating devices tested, pass/fail status, and actions taken to resolve problem(s) on failed tests. Items required to be tested includes, but not limited to, all door lock hardware, readers, REX, door contacts and relays

  3) Acceptance Test Schedule: Correct deficiencies identified by tests and observations and retest until specified requirements are met.

  4) Provide “as designed” drawings showing each device and wiring connection and electronic enclosure legends indicating cabling in and out.

  5) Provide a complete set of operating instructions for access control hardware devices and a complete software user manual. The documentation includes module reference guides for each electronic enclosure.

20. Adjusting

- Adjust and check each operating item of integrated access control door hardware, and each door opening to ensure proper secured operation and function of every unit. Replace units that cannot be adjusted to operate as intended.
- One week before student occupancy, vendor is required to run a battery report on all wireless locks installed and replace any batteries that have less than 25% battery life remaining with fresh, new batteries.

21. Cleaning And Protection

- Clean adjacent surfaces soiled by access control system installation.

- Clean operating items as necessary to restore proper finish and provide final protection and maintain conditions that ensure access control door hardware is without damage or deterioration at time of owner occupancy.
- One week before occupancy, Vendor is required to clean all card readers with a manufacturer approved cleaning device. Normally, alcohol cleaning cards are used for this purpose.

22. Demonstration
    - Engage a factory-authorized representative to train Owner's maintenance personnel to adjust, operate, and maintain electrified door hardware and the integrated access control system.
23. Access Control System Hardware Sets
    - The access control system hardware sets listed below represent the design intent and direction of the owner, architect, and security consultant (if applicable). They are intended as a guideline only and should not be considered a detailed opening schedule. Discrepancies, conflicting, and missing items should be brought to the attention of the architect with corrections made prior to the bidding process.
24. Inventory
    - EAC Contractor shall provide 1,000 magnetic stripe cards to the owner for inventory.
    - EAC Contractor shall provide 50 read head cleaning cards to the owner for inventory.
    - EAC Contractor shall provide for owner stock each installed item in Section 2.3 totaling 2% of the total of each type installed, not less than 1 of each type to the owner.
    - Provide 1 electronic key/card machine that accepts Best interchangeable cores and internal storage of key cards. Key box must hold 8 hard keys and 8 key cards. Electronic key box must use dual validation via PIN pad and card swipe access to remove keys/cards. See keystorage.com for more information

END OF SECTION 281300

SECTION 28 23 00 VIDEO SURVEILLANCE

1. Related Documents
    - Drawings and general provisions of the Contract, including General and Supplementary Conditions and Division 01 Specification Sections, apply to this Section.
2. Summary
    - An IP, PoE, Closed Circuit Television (CCTV) system. Number of cameras will be equal to or greater than 1 camera per 2,700 square feet of total gross building space. There also will be one NVR for each set of 32 cameras. Include all software and licensing to make the system useable. Cameras are also required in each elevator. Owner will approve final camera layout.
    - This camera specification of H.264 (MPEG 4, Part 10) must provide a minimum 1280 x 1024 megapixel (1.3 megapixel camera) resolution with minimum video frame rates of 24fps.
3. Performance Requirements

- Delegated Design: Design this project element, including comprehensive engineering analysis by a qualified design professional, to meet or exceed the program requirements, performance requirements, code compliance, applicable ASTM quality standard, and design criteria as outlined and / or referenced within this RFP package.

4. Quality Assurance

   - Comply with NFPA 70, National Electrical Code.

5. Video Management System

   - Video Management System - Software Overview

     1) The Video Management System (VMS) software shall be used to view live and recorded video from capture cards and IP devices connected to local and wide area networks. The VMS software shall have a client/server-based architecture that can be configured as a standalone VMS system with the client software running on the server hardware and/or the client running on any network-connected TCP/IP workstation. Multiple client workstations shall be capable of simultaneously viewing live and/or recorded video from one or more servers. Multiple servers shall also be able to simultaneously provide live and/or recorded video to one or more workstations. The VMS server software shall also have the ability to be installed on an IP edge device—such as an IP camera or encoder that allows for 3rd party applications—allowing the device to serve as both a server and IP video recording device.

     2) The VMS shall not charge for the number of concurrent clients.

     3) The VMS system shall utilize manufacturer built servers, commercial-off-the-shelf (COTS) computer workstations, servers, IP edge devices that allow for third-party application installation, networking devices and storage equipment.

     4) Recording of all video transmitted to the VMS shall be continuous, uninterrupted, and unattended.

     5) The VMS system shall offer the capability of video motion detection recording, such that video is recorded when the NVRMS detects motion within a region of interest of the camera's view. Video prior to the detection of the motion shall also be stored with recording using the pre-recorded feature.

     6) The VMS system shall manage the video it has been configured to monitor. Loss of video signal shall be configured to annunciate on VMS client by an on-screen visual indication alerting operators of video loss.

     7) The VMS software shall have an open architecture supporting IP cameras and encoders from multiple manufacturers providing best-of-breed solutions ranging from low-cost, entry-level features to high-resolution, megapixel features.

     8) The VMS client software shall be able to view live video and audio, recorded video and audio and be able to configure the complete system all from a single application.

     9) The VMS shall continue to record video and audio at all times during the administration and configuration of any feature.

     10) The VMS client software shall have the same functionality when connected remotely as it does when it is run locally on the same computer as the server software.

     11) The VMS client software shall add and remove features based on the permissions of the user and the licensed functionality.

12) The VMS client software shall operate on all of the following operating systems:

a. Microsoft Windows Server 2003/2008

b. Microsoft Windows XP (all versions)

c. Microsoft Windows Vista (all versions)

d. Microsoft Windows 7 (all versions)

e. Linux Ubuntu 8.04/10.04 Debian Package

f. Mac OSX (operating on Intel CPU)

13) The VMS software shall allow the user to have any combination of VMS client applications running on any of the supported operating systems and be able to connect to any of the VMS servers running on any of the supported operating systems. For example, a VMS client running on Microsoft Windows 7 shall be able to simultaneously connect to four (4) different VMS servers all running on different operating systems, such as Windows Server 2003, Windows XP, Vista, and Linux.

14) The VMS software shall have the capability to run multiple client applications simultaneously on one workstation with multiple monitors. Up to 12 monitors shall be configured on a single workstation with one (1) client application running on each monitor. Because decompressing video is CPU-intensive, the PC workstation shall have multiple core processors with a recommendation of one core for each VMS client application.

15) The VMS shall also allow an authorized user to view video through a web client interface. The web client interface shall allow authorized users to view live video; view recorded video, control pan-tilt zoom (PTZ) cameras and activates triggers. The web client interface shall allow connections to multiple VMS servers simultaneously.

16) The web client interface shall operate without requiring installation of any software.

17) When using the web client interface, the VMS server shall transcode the video into a JPEG file of the size as the browser screen before sending it to the browser.

18) The web client interface shall support the following browsers:

a. Internet Explorer 6 and later

b. Firefox 2 and later

c. Opera 9 and later

d. Safari and later

e. Chrome

f. The web client interface shall also connect with non-JavaScript browsers and shall be compliant with HTML 4.0 (www.w3.org).

19) The VMS server software shall record and retrieve video, audio and alarm data and provide it to the VMS clients upon request.

20) The VMS software shall provide at no additional charge a purpose built mobile application capable of viewing multiple simultaneous live video streams and

playing a recorded video stream. Application shall be provided for both iOS and Android operating systems (including Kindle Fire).

21) The VMS server software shall operate on any of the following operating systems:

a. Microsoft Windows Server 2003/2008

b. Microsoft Windows XP (all versions)

c. Microsoft Windows Vista (all versions)

d. Microsoft Windows 7 (all versions)

e. Linux Ubuntu 8.04/10.04 Debian Package

22) The VMS server shall not decode video for the purpose of motion detection.

23) The VMS server shall not decode video for the purpose of repacking it for transmission to clients.

24) The VMS server software shall record video based on metadata generated by an edge network device. The edge network devices shall generate the metadata and transmit it with the video stream to the VMS server software.

25) The VMS shall license the total number of cameras on the system. This license shall be based on the MAC address of a single network card that is present on the system. The VMS shall only require that this network card be enabled and does not require that data is actually sent through it.

26) The VMS shall not require the manufacturer to be contacted when a camera fails.

27) The VMS server software shall run as a service. The VMS shall not require any application to be running in order to operate.

28) The VMS shall be able to use the Active Directory or LDAP features of a network to authenticate users and determine which permissions they will have on each server.

29) The VMS shall allow for a user's permissions to be configured across multiple servers from a single screen.

30) The VMS shall allow the use of maps. The maps will be accessible to users with the appropriate permission levels and display video sources and their status.

31) The VMS shall allow maps to be embedded inside of maps (i.e. hierarchical or nested maps). When an event happens on a map that is embedded inside of a map, it shall transmit the alert to all parent maps and change the color of the icon on the parent map and all subsequent parent maps.

32) The VMS allows soft triggers to be placed, viewed, and triggered from a map.

33) The VMS shall have a single page that displays the status of all servers and cameras currently connected. This page shall display any alarms, events, MAC addresses, camera configuration, format and frame rate from each individual camera.

34) The VMS shall support the use of a panoramic lens on an analog or IP camera. The VMS client shall de-warp the image on both live and recorded video.

35) The VMS software shall have three methods of allowing third-party integration: command line, API, and web SDK. The command line shall allow for the most

basic of interfaces, calling up the appropriate video when requested using command line functionality. The API shall allow for a deeper interface, allowing video to be transmitted from the VMS software into the party software interface. The web SDK shall use the web server to transcode the video and send it to the third-party software interface. The web SDK method shall use standard HTML, XML, CGI, and JavaScript commands.

- Video Management System - Software Features

1) When in live display mode, the user shall be able to view live video, live audio, point of sale (POS) data and alarm information.

2) The VMS shall be able to organize the camera video view panel in the following patterns:

   a. 1-camera (full-screen) layout

   b. 4-camera (2x2) layout

   c. 8-camera (3 large views and 4 small views) layout

   d. 10-camera (2 large views and 8 small views) layout

   e. 13-camera (1 large view and 12 small views) layout

   f. 16-camera (4x4) layout

   g. 8-camera (1 very large view and 7 small views) layout

   h. 9-camera (3x3) layout

   i. 6-camera (2x3) widescreen layout

   j. 12-camera (4x3) widescreen layout

   k. 20-camera (5x4) widescreen layout

   l. 30-camera (6x5) widescreen layout

   m. 48-camera (8x6) widescreen layout

3) The VMS shall allow the customization of the user interface to allow software triggers to be shown. This shall allow them to activate events through the push of a button, which could trigger recording, PTZ presets, output triggers, or email.

4) The VMS shall allow the user to pick their own icon and select the software triggers to display in the client. The VMS shall also display the status of any soft triggers on connected VMS servers.

5) The VMS software shall allow control of PTZ cameras to authorized users and be used to maneuver a PTZ camera. When used on a non-PTZ camera, it shall allow you to digitally pan, tilt, and zoom on any video whether in live or recorded mode.

6) The VMS shall allow following methods of controlling a PTZ camera to be available:

   a. PTZ graphics control windows

   b. Live graphic overlay PTZ control icons

   c. Keyboard control (up, down, left, right arrows; page up, page down for zoom)

   d. PTZ presets

e. Digital PTZ

f. USB joystick to control PTZ cameras

g. Proportional PTZ control by clicking the mouse in the center and moving it

7) The VMS software shall allow virtual matrix functionality by designating a cell to do so. This video cell shall automatically show video as it is triggered.

8) The VMS software shall have a feature for viewing logical groups of cameras. This shall allow efficient viewing of cameras in a logical order.

9) The VMS software shall have a feature to organize your cameras into preset views. Views are preconfigured arrangements of the video panels so that they may be easily recalled later. A view can save the location of the video streams, audio streams, POS data, maps, and event views. These views shall be accessible in both live and recorded video modes.

10) The VMS software shall have the capability to automatically cycle through two or more saved views to create a video tour. The VMS shall allow the configuration of the dwell time and the different views it shall use.

11) The VMS client software shall be used to search for and play back recorded video, audio, and events from VMS servers.

12) The VMS software shall have the capability to search for and play back video from multiple cameras simultaneously. All recorded video shall be played back and displayed in a synchronized multi-camera layout.

13) The VMS software shall support searching through recorded video based on time, date, video source, and image region and have the results displayed as both a clickable timeline and a series of thumbnail images.

14) The VMS software shall allow search and play back of audio in synchronization with video.

15) The VMS software shall allow you to search on a specific area of recorded video and only display the frames where motion happened in that area.

16) The VMS software shall have the capability to export video, maps, POS data and audio files.

17) The VMS software shall provide the option of exporting the file in the following formats:

a. Standalone Exe (*.exe) – includes an executable player with the video and audio data

b. AVI File (*.avi) – a multimedia container format

c. PS File (*.ps) – a format for multiplexing video and audio

d. QuickTime File (*.mov) – native for Macintosh computers

18) The VMS standalone player shall package all of the exported video into a single executable. The VMS standalone player shall be able to authenticate that the video has not been tampered with using a keyed Hash Message Authentication Code (HMAC).

19) The VMS client software shall be able to connect to multiple systems simultaneously. Each of the systems could have individual permissions, thereby

limiting the client's configuration or viewing abilities for that system, but not affecting the abilities on the other systems.

20) The VMS system shall be able to display system information about users that are currently logged into the system, plug-in file version information number, and status, and a system log that contains a detailed history of the processes that occur on the system.

21) The VMS system shall have the ability to record an audit trail of when users log in that shows what changes they have made, what video they have viewed and what they have exported.

22) The VMS system shall allow the configuration of the video devices to be performed in the client and pushed out to the devices. The configuration itself is stored both on the camera and on the VMS.

23) The VMS shall allow monitoring of the inputs on both network devices and on manufacturer provided hardware. The VMS shall also allow triggering of outputs on the network devices and manufacturer provided hardware.

24) The VMS shall allow for the configuration of what drives to use for recording video. Those drives may be local drives, direct attached storage drives or iSCSI drives.

25) The VMS shall allow for the configuration of rules of how to record the video. These rules shall allow you to set a maximum number of days or minimum number of days on a per video stream basis.

26) The VMS shall not require a database when recording video.

27) The VMS shall use the operating systems native file system for recording the video. For example, if there was video that was recording on March 1, 2012 from 10:00 AM to 10:35 AM. Files for that day would be in the data drive, in the path 2012 for year, subfolder 03 for the month, with a sub folder 1st for the day, and then the 10 sub-folder for the hour. So when the client sends a request to search for video, the VMS shall look in the D:\2012\03\01\10 directory. Each video stream shall be kept in 5-minute increments in a paired video and index file. The video file shall contain the data of the video, audio, and include Meta data. The index file shall contain the index of the metadata from the network device. So when the VMS searches for the video, it shall gather up the information in the index files and display those results. When the client then requests to display the video, the VMS will then transmit the video file data from the server to the client.

28) The VMS shall have the ability to receive ASCII data through the COM port on the server or over the network.

29) The VMS shall have the ability to look for keywords in the ASCII data and use these to execute various events such as PTZ presets, recording video, recording audio and sending email notifications.

30) The VMS software shall be able to send a predefined email based on an event trigger. The VMS software shall also support SSL and TLS connections for transmissions of the mail.

31) The VMS software shall have a feature to export a video segment from specific cameras or audio inputs to a CD or DVD upon an input trigger or other event being activated.

32) The VMS software shall be used to connect different types of events, such as input triggers, to a desired action such as recording video or triggering an alarm. The VMS software shall recognize the following event types:

a. Video Motion

b. Video Loss

c. Input Trigger

d. POS Port

e. POS Profile

f. Health

g. IP Camera Connection

h. Software Trigger

i. Analytics

33) The VMS software shall be able to execute the following action types:

a. Record Video

b. Output Trigger

c. Output Video

d. Send an email

e. Burn a CD/DVD

f. Call a PTZ Preset

34) The VMS software shall have the ability to configure each video input's recording time on an hourly basis. This shall allow the user to schedule when to record on motion, when to record on event and when to not record.

35) The VMS shall use a combination of a user name and a password to authenticate the user's permission level.

36) The VMS shall allow granularity of permissions by creating custom user groups. The members of these custom user groups shall all have the same permissions.

37) The VMS client shall be able to use OpenGL and Direct 3D to decompress and render video.

38) The VMS shall allow the user to perform a visual thumbnail search. The user can select one camera to see one image per set time period. The user shall be able to play video from that image or zoom in to a time range.

39) The VMS client can be configured to automatically switch views on any trigger within the event monitoring function.

- Server Network Video Recorder Hardware Features

1) The server hardware shall operate on either the Microsoft XP Pro or Linux operating systems.

2) The server shall be capable of simultaneously recording, displaying, and playing back digitized video from IP cameras and analog cameras through the use of a video encoder. IP Server models shall be capable of being licensed to add IP cameras in increments from one (1) to 64 camera licenses.

3) The server shall support recording resolutions from CIF to 20 megapixel (camera dependent) and shall be user selectable. MJPEG, MPEG-4, and H.264 video compression format shall be user selectable depending on the IP camera configured to the IP Server. Video recording shall be available at up to 30 images per second per input channel depending on IP camera type selected.

4) Each server shall have serial port capabilities to communicate with serial devices such as point of sale (POS) terminals and automated teller machines (ATM). Once the serial device is connected to the serial port with a cable the serial port shall be configured. Transaction data shall be received from each serial device into a text database and associated with recorded video. User shall be able to search transaction data to locate the associated video.

5) Each server shall have a serial port capable of communicating with pan-tilt-zoom (PTZ) cameras.

6) Each server shall have two Gbit 1000Base T RJ-45 Ethernet connections for networking to Remote PC clients. Multiple servers shall be accessible by multiple clients located anywhere on the network. Each server shall record video, audio, and text while displaying live video or playback video. In the event that there is no client actively attached to the server, the server shall continue to record video and audio, monitor events and all other server functions.

7) Recorded video shall be triggered by the motion detection sensor of the IP camera, an external input device, or in continuous record mode.

8) Each server shall have the capability of automatically exporting a predetermined time frame of video to the internal DVD/CD device upon an external trigger input connected to the server. Such input shall export to the DVD/CD device a user defined amount of video and video camera source both pre and post event schedulable to the maximum capacity of the DVD/CD media selected.

9) Each server shall have the ability to link specific events in an “if-then” scenario. Linked events types shall include video motion, video loss, input trigger, POS port, POS profile, and temperature. Sources of these events shall be any camera connected to the specific server. Action from these events shall include record video, record audio, enable output trigger, output video, notify (send e-mail), and output video to DVD.

10) The server hardware shall have an internal DVD/CD device that will allow the server to export video clips to the device in Standalone.Exe (*exe), AVI files (*.avi) and PS files (*ps) formats.

11) A RAID-5 option shall be available consisting of a 4U chassis and eight hot swappable hard drives. The RAID-5 option shall be internal to the server and shall provide notification of a drive failure to the administrator.

- Specifications And Model Numbers

1) 2U Rack mount IP Server

a. All 2U Rack mount Servers shall have the following specifications:

- Dimensions (L x W x H): (21.25” x 16.75” x 3.5”) (54.7 x 42.6 x 8.9 cm)
- Weight: 27 – 31 lbs. (12.3 – 14.1 kg)
- Input Voltage: 120/240 VAC auto-sensing
- Power Consumption: <250 watts (150 watts typical)

- Video Standard: NTSC (30ips) or PAL (25ips)
- Recording Resolution: CIF to 20 megapixel (camera dependent)
- Compression: MJPEG, MPEG-4 or H.264 by camera or encoder
- Alarm Inputs: 8 optional
- Alarm Outputs: 8 optional
- Serial Connections: 1 serial port
- NIC: 2 Gbit 1000Base T RJ-45 (standard), 4 (optional)
- USB 2.0 Ports: 6 (6 x USB 2.0)
- Audio Inputs: 4 optional
- Hard Drive Storage: Enterprise Class (see models below)
- VGA Output: 1 VGA + 2 HDMI 1.4 (including DVI-D converter), maximum 2 simultaneous monitors
- Keyboard & Mouse: Included
- DVD/CD RW: Included, front panel access
- Operating System: Windows 7 Pro or Server 2008 on 30 GB HDD PartitionO
- Operating Temperature: 40° – 95°F (4.5° – 35°C)
- Relative Humidity: 5 – 95% RH (non-condensing)

b. In addition to the specifications listed above, each 2U Rack mount IP Server shall have unique features defined by the hard disk storage capacity described below:

- IPS-0500-R2 500GB
- IPS-1000-R2 1 TB
- IPS-2000-R2 2 TB
- IPS-3000-R2 3 TB
- IPS-4000-R2 4 TB
- IPS-6000-R2 6 TB

c. 4U Rack mount IP Server

d. All 4U Rack mount IP Servers shall have the following specifications:

- Dimensions (L x W x H): (28” x 16.75” x 7.0”) (71.2 x 42.6 x 17.8 cm)
- Weight: 44 – 60 lbs. (20 – 27.3 kg)
- Input Voltage: 120/240 VAC auto-sensing
- Power Consumption: 500 watts
- Recording Resolution: CIF to 20 megapixel (camera dependent)

- Compression: MJPEG, MPEG-4 or H.264 by camera or encoder
- Alarm Inputs: 8 optional
- Alarm Outputs: 8 optional
- Serial Connections: 1 serial port
- NIC: 2 Gbit 1000Base T RJ-45 (standard), 4 (optional)
- USB 2.0 Ports: 6 (6 x USB 2.0)
- Audio Inputs: 4 optional
- Hard Drive Storage: Enterprise Class (see models below)
- VGA Output: 1 VGA + 2 HDMI 1.4 (including HDMI-DVI-D converter), maximum 2 simultaneous monitors
- Keyboard & Mouse: Included
- DVD/CD RW: Included, front panel access
- Operating System: Windows 7 Pro or Server 2008 on 30 GB HDD Partition
- Operating Temperature: 40° – 95°F (4.5° – 35°C)
- Relative Humidity: 5 – 95% RH (non-condensing)

e. In addition to the specifications listed above, each 4U Rack mount IP Server shall have unique features defined by the hard disk storage capacity described below:

- IPS-8000-R4 8 TB
- IPS-010T-R4 10 TB
- IPS-012T-R4 12 TB
- IPS-014T-R4 14 TB
- IPS-016T-R4 16 TB

f. All 4U Rack mount RAID-5 IP Servers shall have the following specifications:

- Dimensions (L x W x H): (28” x 16.75” x 7.0”) (71.2 x 42.6 x 17.8 cm)
- Weight: 44 – 60 lbs. (20 – 27.3 kg)
- Input Voltage: 120/240 VAC auto-sensing
- Power Consumption: <250 watts (150 watts typical)
- Recording Resolution: CIF to 20 megapixel (camera dependent)
- Compression: MJPEG, MPEG-4 or H.264 by camera or encoder
- Serial Connections: 1 serial port
- NIC: 2 Gbit 1000Base T RJ-45 (standard), 4 (optional)

- USB 2.0 Ports: 6 (6xUSB 2.0)
- Hard Drive Storage: Enterprise Class (see models below)
- VGA Output: 1 VGA + 2 HDMI 1.4 (including HDMI-DVI-D converter), maximum 2 simultaneous monitors
- Keyboard & Mouse: Included
- DVD/CD RW: Included, front panel access
- Operating System: Windows 7 Pro or Server 2008 on 30 GB HDD Partition
- Operating Temperature: 40° – 95°F (4.5° – 35°C)
- Relative Humidity: 5 – 95% RH (non-condensing)

g. In addition to the specifications listed above, each 4U Rack mount RAID5 Server shall have unique features defined by the hard disk storage capacity described below:

- IPS-4000-R4-RAID5 3 TB
- IPS-6000-R4-RAID5 5 TB
- IPS-8000-R4-RAID5 6 TB
- IPS-010T-R4-RAID5 8 TB
- IPS-012T-R4-RAID5 10 TB
- IPS-014T-R4-RAID5 12 TB
- IPS-016T-R4-RAID5 14 TB

- Certifications

1) CE and FCC, Class A (all models)

- Warranty

1) 3-year warranty on parts and labor and a 3-year Software Subscription Agreement (SSA)

- Video Management System Hardware

1) Minimum Server Requirements: The VMS client software shall operate on the following minimum requirements:

a. Processor: Intel® Atom® D525 1.8GHz or higher

b. Graphics: 1280 x 1024 x 32 bits

c. RAM: 1GB

d. NIC: 1x100 Mbps (minimum), 1 Gbps (preferred)

e. Hard Disk: 80GB Serial ATA drive

f. Operating Systems:

- Microsoft® Windows 2003 Server (or)
- Microsoft® Windows 7 (all version)

2) Minimum Client Requirements

a. Processor: Intel® Atom D525 1.8 GHz or greater

b. Graphics: 1280x1024x32 bits

c. RAM: 1 GB

d. NIC: 10/100/1000 baseT Ethernet

e. Disk Drive: Western Digital Enterprise Class drive (RE4 or better), or Seagate Barracuda ES.2 Drives or better

f. Operating Systems:

- Microsoft Windows XP (all versions) or higher
- Linux Ubuntu 8.04 or higher
- Mac OSX 10.4 or higher

3) Recommended Server Requirements

a. Processor: Intel® Core i7-2600 Processor, 3.4 GHz or Xeon E3-1220

b. Graphics: 1280x1024

c. RAM: 4 GB

d. NIC: 2x1Gbps (minimum), 4x 1 Gbps (preferred)

e. Disk Drive: RAID-5 (minimum), RAID-6 (preferred), minimum sustained non-sequential write capacity 70 MBps

f. Operating Systems:

- Microsoft Windows XP (all versions)
- Microsoft Windows Vista (all versions)
- Microsoft Windows 2008 Server (all versions)
- Microsoft Windows 7 Pro (all versions)

4) Recommended Client Requirements (Single Monitor)

a. Processor: Intel® Core i3 2100 Processor, 3.1 GHz or greater

b. Graphics: 1280x1024

c. RAM: 2 GB

d. NIC: 10/100/1000BASE-T Ethernet

e. Disk Drive: Western Digital Enterprise Class drive (RE4 or better), or Seagate Barracuda ES.2 Drives or better

f. Video: 64 MB video card (Direct3D / OpenGL compatible)

g. Operating Systems:

- Microsoft Windows 7 (all versions) or higher
- Linux Ubuntu 8.04 or higher
- Mac OSX 10.4 or higher

5) Multi-Monitor PC Requirements (4 VGA monitors at up to 1920x1200 resolution) The VMS client software shall operate on the following minimum requirements:

a. Processor: Intel® Core i7-2600K 3.4GHz or higher

b. Graphics: Multi-output display adapter

c. RAM: 4 GB

d. NIC: 10/100/1000BASE-T Ethernet

e. Hard Disk: 80GB Serial ATA drive

f. Video: 512 MB video card (Direct3D/OpenGL compatible)

g. Operating Systems:

- Microsoft® Windows 7 (all version)
- Mac OSX 10.6
- Linux Ubuntu 10.04

6. Camera Specification

- The camera shall be compatible with the Video Management Software specified above.
- The camera shall utilize a high sensitivity 1.3 Megapixel effective CMOS sensor with 1/2.7" optical format.
- The camera shall have a dome enclosure with IP66 for water and dust protection.
- The camera dome chassis shall be vandal resistant constructed of aluminum with a 4" polycarbonate dome bubble with IK10 impact rating.
- The camera shall have a 3-axis gimbal with 360˚ pan, 90˚ tilt and 180˚ Z-rotation for easy and accurate positioning
- The camera shall have dual standard compression support with simultaneous streaming of both H.264 and MJPEG formats.
- The camera is fully compatible with PSIA industry standard and passes PSIA conformance tests.
- The camera shall have privacy masking, the ability to select multiple regions of an arbitrary shape to block the video. This feature will support both HTTP and TFTP protocols, as well as the on-camera web interface.
- The camera shall have extended motion detection grid, a higher granularity grid of 1024 distinct motion detection. User can select between 64 zone based motion detection and extended motion detection to provide backward compatibility with the existing Video Management System (VMS) integration. This feature will support both in HTTP and TFTP, as well as the on-camera web interface.
- The camera shall be able to be cropped to any resolution divisible by 2 and maintain H.264 compression.
- The camera shall have multi-streaming support of up to 8 non-identical concurrent streams (different frame rate, bit rate, resolution, quality, and compression format).
- The camera's bit rate control shall be selectable from 100 Kbps to 10 Mbps for each independent stream.
- The camera's shutter speed shall be 1ms - 500ms.
- The camera shall have Real Time Streaming Protocol (RTSP) support allowing for compatibility with media players such as Apple QuickTime, VLC Player and others.

- The cameras H.264 implementation shall maintain full real time video frame rates.
- The camera shall output at a minimum resolution of 1280(H) x 1024(V) pixels up to frame rate of 24 frames per second (FPS).
- It shall be possible to program the camera to output a variety of lower resolution image and increase frame rate.
- The camera shall feature streaming of the full field of view (FOV) and simultaneous multiple regions of interest (ROI) for forensic zooming.
- The camera shall be equipped with a 100 Mbps LAN connector.
- The camera shall provide 21 levels of compression quality for optimal viewing and archiving.
- The camera shall support a minimum HTTP, RTSP, and RTP over TCP, RTP over UDP and TFTP network protocols.
- The camera shall feature automatic exposure, automatic multi-matrix white balance, shutter speed control, 50/60Hz selectable flicker control, programmable brightness, saturation, gamma, sharpness, windowing and decimation, simultaneous delivery of full-field view and zoomed images at video frame rate, instantaneous electronic zoom, pan and tilt, and electronic image rotation by 180 degrees.
- The camera shall incorporate necessary algorithms and circuits to detect motion in low light with clarity.
- The camera shall support a minimum illumination of 0.1 Lux @ F1.2 in color mode and 0 Lux in B/W mode.
- The camera's primary power source shall be Power over Ethernet (PoE) complying with the IEEE 802.3af standard.
- The camera shall have the alternative option to be powered via DC power from 12V to 48V DC or 24V AC power source.
- The camera shall have 9 watts max power consumption and 12.8 watts max power consumption with heater.
- The Camera shall provide total PoE solution to drive heater without any external power input.
- The Camera's heater shall switch on -40˚C (-40°F) to 17C° (62.6 °F) and Off: 30 °C (86 °F)
- The camera's operating ambient temperature shall be minimally -20˚C (-4°F) to 50ºC (122ºF) without heater; -40˚C (-40°F) to 50ºC (122ºF) with heater, stable image temperature is 0˚C (32 °F) to +50˚C (122°F); storage temperature -40˚C (-40°F) to +60˚C (140 °F) at the humidity 0% to 90% (non condensing).
- The camera shall be UL listed (CB Scheme).
- The camera shall integrate with the Video Management System
- The camera shall have a minimum 1 Year parts and labor
- Central IT infrastructure may be used for network traffic but not for PoE. Instead a PoE injector must be used to power the cameras.

END OF SECTION

28 31 11 Fire Alarm Systems

Fire alarm systems shall be installed in buildings when required by this section.

1. Purpose:
    - The primary purpose of a fire alarm system is to notify the appropriate people and initiate the proper response from those people who are notified.
    - The secondary purpose is to initiate fire safety functions, which are building and fire control functions that are intended to increase the level of safety for occupants or to control the spread of the harmful effects of fire.
    - The fire alarm system operation must be coordinated with the facility fire plan.

    Note: This does not preclude the fire plan from being modified to meet the fire alarm system operation.
2. General Requirements:
    - The fire alarm system shall be installed where required by NFPA 101 and shall be designed to meet the requirements contained in NFPA 72 (2007), National Fire Alarm Code, Virginia Statewide Fire Prevention Code (2006) and this manual.
    - Do not combine fire alarm systems with other systems such as building automation, energy management, security, etc. Down time for any of these non-life safety systems will also take the fire alarm system out of service. This is not acceptable to Mason.
    - All fire alarm wiring shall be installed in raceway separate from all other systems.
    - Installation of Fire Alarm Systems, including all conduit, supports, wiring, peripheral devices etc.; shall be installed according to all applicable codes referenced in the VUSBC, signed Architectural Drawings, and project Specifications Manual. All Fire Alarm equipment shall meet the requirements of UL 864 Ninth Edition.
    - All wiring shall be installed in a protected raceway e.g.; conduit, Greenfield, Liquid Tight, MC cable with proper color band for fire alarm use. Under no condition shall free air wiring be installed.
    - Wiring for local building fire alarm systems shall be specified as defined in NFPA 72 as follows:
        1) Initiating Device Circuits (IDC): Class B.
        2) Signaling Line Circuits (SLC): Class B.
        3) Notification Appliance Circuits (NAC): Class B.
    - System shall include an elevator pre-action system.
    - There will be no performance spec system.
    - System shall be approved by BECOM.
    - Existing systems that are obsolete, shall be removed not abandoned in place.
    - Amv does first F.A. inspection.
        1) Communications between building fire alarm control units: Class X.

Note: Class B signaling line circuits (these are not initiating device circuits by definition) are preferable for local building fire alarm systems because it permits the

circuits to be t-tapped and the allowable length of the circuits are not shortened. No clear advantage is seen for running Class A circuits except where signaling line circuits are run between building fire alarm control units. Where signaling line circuits are run between fire alarm control units in separate buildings, fiber optic circuits are preferred because they are not susceptible to damage from lightning strikes. Where Class X copper circuits are installed, provide isolation modules that will ensure that only one building is lost (will not respond) during any type of fault. Although desirable, it is not required that Class X circuits be run in separate conduits from each other.

Note: Installation of the Fire Alarm System shall consume no more than 80% of the systems maximum capacity in all respects. In particular, all addressable circuits shall allow for the future installation of at least (15) additional devices, without requiring additional components in the FACP or new "home-run" wiring. All visual notification circuits shall allow for the future installation of at least (200) linear feet of additional circuit length, with (4) 15cd strobes at the end of the new circuit.

- The use of “wire nuts” shall be strictly prohibited. If it becomes necessary to create a junction point, all wiring shall be terminated under a terminal screw and printed labels showing each wire’s origin and destination shall be affixed to the wire and a clear protective covering over the label shall be used.
- The FACP shall be equipped with the means to disable ALL audio/visual devices, (including sounder bases if so equipped) elevator recall, AHU shutdown, door release, and solenoids for any pre-action or sprinkler dry pipe systems without having to go through menu options, e.g.; single push button for each event listed.
- Analog addressable systems are encouraged where many smoke detectors are required to be installed. These systems do not require the frequent sensitivity testing for smoke detectors that the hard-wired systems require and the savings in testing will pay for the extra cost of the system.

  1) It is the intention of the University to obtain competitive bids for maintenance and repair services and material for the fire alarm system provided. Any special tools, prints, technical data, layouts, hardware, software, etc. required throughout the life of the equipment and which cannot be obtained from multiple suppliers, must be provided by the manufacturer to the Owner at substantial completion of the project.

  2) Mason will accept the following systems, or any viable alternative with RFI approval from Mason:

     a. Notifier

     b. FCI (Fire Control Instruments)

     c. Simplex

     d. Siemens

  3) Any and all maintenance diagnostic tools, electrical schematic wiring diagrams and any access codes and passwords required to perform any maintenance function over the life of the equipment such as diagnostics, adjustments or reprogramming shall be provided to the Owner on the Date of Substantial Completion. Tools may be handheld or built into the control system and shall function for the life of the equipment without the requirement to return them to the Manufacturer. Provide complete operations and maintenance manuals including diagnostics instructions for troubleshooting the system. The Owner

shall not be required to sign licensing agreements related to the use of maintenance or repair tools.

4) The fire alarm control panel shall be listed under UL Category UOJZ for each of the following:

a. Type: "P (PPU)" (proprietary fire alarm, protected premises control unit).

b. Type Services: "A" (automatic fire alarm), "M" (manual fire alarm), "WF" (waterflow alarm), and "SS" (sprinkler supervisory).

c. Type Signaling: "DAC" (digital alarm communicator).

Note: No other category or use types will be considered

- Upon Date of Substantial Completion, the installing contractor shall provide the Owner all of the following;

1) Four (4) complete sets of binders containing OEM Manuals including the Maintenance, Operation and Programming Instructions

2) Bill of Material of all installed equipment, part numbers, and the replacement cost of each item. Prices shall remain valid for two (2) years including the warranty period

3) Cut sheets and wiring diagrams

4) Device point list and contact ID transmission data (to be programmed into Keltron)

5) Electronic copy of the FACP program

6) Written sequence of operation

7) Complete battery calculation sheets

8) Four (4) sets of reproducible as-built drawings

3. Typical Operations:

- Table 7.3(1) & (2) is provided to identify the typical operation required by the respective fire alarm systems. A table similar to this should be added to the contract documents to indicate the specific operation required of the system.

TABLE 7.3(1) ADMINISTRATION BUILDING'S GENERAL MATRIX

INPUT DEVICE / OUTPUT --->	1. Sound general building alarm	2. Initiate alarm to GMU Police via Digital alarm communicator	3. Initiate supervisory signal to GMU Police	4. Close associated smoke barrier doors on the floor	5. Shutdown air handeler served by detector	6. Recall elevator	7. Initiate elevator shut down and disconnect elevator	8. Open all locked egress doors.	9. Disconnect fuel source from cooking equipment.
Duct Smoke Detector			X		X				
Area Smoke Detector	X	X						X	
Door Release Smoke Detector	X	X		X				X	
Elevator Smoke Detector	X	X				X		X	
Manual Pull Station	X	X		X				X	
Elevator Machine Room Heat Detector	X	X					X	X	
Generator Room Heat Detector	X	X						X	
Sprinkler Waterflow/Pressure Switch	X	X		X				X	
Water Control Valve Tamper			X						
Fire Pump (Any alarm condition required by NFPA 20)			X						
High/Low Pressure Dry-Pipe Sprinkler System			X						
Kitchen Hood Suppression System	X	X		X				X	X
Gas Extinguishing Systems	X	X		X				X	
Dry Pipe Valve Room Temperture Alarm			X						

TABLE 7.3(2) STUDENT HOUSING BUILDING'S GENERAL MATRIX

INPUT DEVICE / OUTPUT --->	• ANNUNCIATION			NOTIFICATION		• CONTROL								
	1. Alarm Annundation FACP, Remote Annun & Send Status to receiveing station & Printer	2. Supervisory Annundation FACP, Printer, Graphic Annundator & Send Status to Receiving Station	3. Trouble Annundation FACP, Printer, Graphic Annundator & Send Status to Receiving Station	4. Sound General Evacuation Horns, Strobes & Audible bases throughout Building	5. Sound Audible Bases Throughout Associated Dwelling Unit (Also Activates Strobes in Dwelling Unit for ADA or HI Unit)	6. Activate Elev Recall to Primary Floor	7. Activate Elev Recall to Alternate Floor	8. Initiate Elevator Shunt Trip	9. Activate Exteriro Electric Bell Device	10. Open Smoke Damper Associated with the Vent at Top of Elev Hoistway	11. Shutdown Applicable Air Handling Unit & Associated Dampers	12. Close Service Counter Door	13. Disconnect Power to Access Control Power Supply
Manual Pull Station	X			X									X
General Area/Corridor Smoke Sensor	X			X									X
First Dwelling Unit Smoke Sensor		X			X								
Second Dwelling Unit Smoke Sensor	X			X									X
Service Counter Door Smoke Sensor	X			X								X	X
Elev Lobby Smoke Sensor (all except first floor)	X			X		X				X			X
First Floor Elev Lobby Smoke Sensor	X			X			X			X			X
Elev Machine Room Smoke Sensor	X			X		X				X			X
Elec Machine Room Heat Sensor	X			X		X		X		X			X
Duct Smoke Sensor for AHU		X									X		
Sprinkler Flow (Floor)	X			X					X				X
Sprinkler Flow (Top of Hoistway/Elev Closet)	X			X					X	X			X
Sprinkler Tamper Switch		X											
High/Low Air PSI (Dry pipe System)		X											
Pressure Alarm Switch (Dry Pipe System)	X			X					X				X
Fire Pump Running		X											
Fire Pump Phase Reversal		X											
Fire pump Phase Loss		X											
Fire Pump on Emergency Power		X											

- Provide initiating devices in accordance with NFPA 101, NFPA 72.
- Notification Appliances: Placement and spacing of notification appliances shall be in accordance with NFPA 72.
- In accordance with NFPA 72 and 101, provide smoke alarms in domiciliary resident sleeping rooms, family/staff quarters, on-call staff sleeping rooms, hotel sleeping rooms, and other sleeping rooms. ABA and ADA require a minimum of 1 unit, and 1 out of each 25 rooms in each occupancy category, to be provided with visible appliances (strobe lights) activated by the smoke alarm. Facilities are encouraged to provide additional visible notification appliances (combination smoke detector/visible notification appliance) up to 100%, where possible. See NFPA 72 for light intensity and mounting instructions.

Note: If visible notification appliances are provided in only 1 in 25 rooms, the facility will have to ensure that hearing-impaired persons are assigned only to those rooms where accommodation (visible notification) is provided. Installing strobes in all rooms will allow a hearing-impaired person to occupy any room. In addition, for every room which contains a strobe light activated by a smoke alarm and where a building fire alarm system is present, the room must also contain a strobe light activated by the building fire alarm system.

- Smoke detectors are to be installed only where required by the National Fire Codes, this design manual, or where required by an equivalency. All smoke detectors shall be photoelectric type only. Alarm verification shall not be used for smoke detectors installed for the purpose of early warning. **Exception: All student sleeping dormitories shall provide at minimum 30sec alarm verification.**

Note: Dormitory smoke detectors shall be supervisory on 1st smoke detector alarm, it will sound all sounder bases within the suite or apartment. If smoke detector does not clear within the verification period the general alarm shall sound throughout the building. If two smoke detectors get activated the general alarm shall activate immediately.

- Heat detectors are not required unless used in conjunction with elevator shutdown, where used as a substitute for smoke detectors in environments unsuitable for smoke detectors, or where used to protect emergency generators that are not equipped with automatic sprinklers.
- Indicate the capacity of all air-handling units. Duct smoke detectors are to be installed only where required by NFPA 101 or NFPA 90A. Where a duct smoke detector is located above a ceiling or in a difficult to reach location, provide a remote indicating lamp and a test key switch on nearby wall at 7ft AFF to facilitate testing.
- ALL Modules e.g., Monitor Modules, Control Modules, Relay Modules etc. shall be installed in their own individual junction box. **Exception: 1) Modules mounted on a DIN Rail or other supporting means and installed within the cabinet of the FCAP shall be acceptable. 2) Where space is limited for the installation of multiple modules, they may be installed on a DIN Rail or other supporting means within a lockable cabinet keyed to the same lock on the FACP. 3) Mini-modules used for addressing manual pull stations and installed in the same box as the pull station shall be acceptable.**

Note: All cover plates for modules shall have the means for module LED's to be seen without having to remove the cover plate. All modules shall have a typed label affixed to the cover plate showing loop number and device address. ALL initiating devices shall

have typed labels affixed to the exterior of the device showing loop number and device address. Modules shall NOT be installed in Troughs or larger junction boxes.

- When an annunciator is required, it shall be located at the building entrances where the fire fighters will respond. The main control panel can act as an annunciator. Coordinate the location with the local fire department. Circuits from the fire alarm control panel to a remote annunciator shall be supervised.
- Elevators: Elevator fire protection shall comply with the requirements of NFPA 13, NFPA 70, NFPA 72, and ANSI/ASME A17.1 or A17.3 as applicable.

Note: Designers are reminded of the requirement in Chapter 7 of NFPA 101 for independent ventilation or air conditioning systems to maintain proper temperature during elevator fire fighters service operation for elevator machine rooms that contain solid-state equipment for elevators having a travel distance of more than 50 feet above the level of exit discharge or more than 30 feet below the level of exit discharge, and the requirement that when standby power is connected to the elevator, the machine room ventilation or air conditioning shall be connected to standby power.

Note: Elevators have been an ongoing fire protection problem, not only for Mason, but also for the entire industry. Many conflicting requirements seem to exist at any given time. Although other methods are permitted in the National Fire Alarm Code for power shut down when sprinkler protection is present, Mason uses the heat detector option as identified in the National Fire Alarm Code and as clarified below.

1) Provide smoke detection for Phase I recall for new elevators. Provide smoke detection for Phase I recall for existing elevators that have a travel distance of 25 feet or more above or below the level of fire department response (this is generally a building greater than three stories).

Note: The requirements for Phase I recall do not apply when the hoistway, or portion thereof, is not required to be fire-resistive construction, the travel does not exceed 6 ft 8 in, and the hoistway does not penetrate a floor.

a. Provide smoke detectors in the elevator lobbies, in elevator machine rooms, and elevator machine and control spaces to initiate Phase I recall. Provide smoke detectors at the top of the elevator hoistway to initiate Phase I recall only when sprinklers are installed at the top of the hoistway.

Note: Smoke detectors are only required above the elevator machine room equipment in larger rooms that contain other mechanical equipment. Some rooms have a lot of space that is not dedicated to elevator equipment; smoke detection would not be required for that space.

b. Provide three supervised control circuits from the fire alarm system to a point within three feet of the elevator controller for the purpose of providing an interface with the elevator system. When actuated, the three circuits will, respectively, 1) initiate recall to the alternate floor, 2) initiate recall to the designated floor, and 3) initiate flashing of the firefighter helmet symbol in the elevator car.

2) Where sprinklers are installed in elevator machine rooms or elevator hoistways, provide heat detection to remove power from the elevator prior to water discharge from these sprinklers. In non-combustible hoistways and where cars meet the flammability requirements of ASME A17.1, the sprinkler at the top of the hoistway should be omitted. Sprinklers can be omitted from elevator pits of enclosed, noncombustible shafts where there are no combustible hydraulic fluids contained in the shaft. Sprinklers, when installed in the pits, shall be sidewall type installed no more than 2 feet above the floor.

Note: Elevator cars which were built to the requirements of the ANSI code since 1985 have a flame spread no greater than 75 and a smoke developed rating no greater than 450 (Class B, per ASTM E 84 / NFPA 255). Where the elevator cars meet these requirements, NFPA 13 allows sprinklers to be omitted from the top of the hoistway as well as from the pit as indicated. When sprinklers are omitted from the top of the hoistway, NFPA 72 does not require, nor does it permit, a smoke detector to be installed at the top of the hoistway due to the difficulty experienced with performing testing and maintenance.

a. Elevator main line power shutdown (commonly known as "shunt trip"): Power to the elevator must be removed prior to or immediately upon release of water from a sprinkler in the elevator machine room (including machine space, control room, or control space) or hoistway. Operation of a heat detector used to initiate shunt trip shall cause the shunt breaker to operate, thereby removing power from the elevator(s) within the common hoistway or controlled by equipment in a common machine room. Cars sharing the same hoistway or the same machine room shall have power removed independently from cars within other hoistways or those controlled from equipment in other machine rooms.

Note: The industry expects that the removal of elevator power (caused by operation of the heat detector) will not trap any occupants on the elevator because sequences under Phase I operation will have already moved the car(s) to the recall level and placed the doors in the open position. Smoke detection required for Phase I initiation is provided at all of the spaces where heat detection is provided for power shut down.

b. Provide 57° C (135° F) rate compensation heat detectors within two feet of each sprinkler in the elevator machine room and hoistway in accordance with NFPA 72. Do not provide a heat detector for the pit sprinkler. Higher temperature rated heat detectors may be used where local conditions warrant; however, the heat detectors must have a lower temperature rating than the sprinklers. The sprinklers in the elevator machine rooms and hoistways must be standard response type; quick response sprinklers are prohibited in these areas.

c. Provide a supervised control circuit from the fire alarm system to a supervised relay within three feet of the shunt breaker. This signal is the input to remove the mainline power to the elevator.

d. Provide a 110-vac power source to the shunt breaker independent of the elevator controller. This power circuit shall be supervised by the fire alarm system as a supervisory signal.

Note: The shunt breaker requires 110-vac to operate and the source must be independent of the elevator in accordance with ANSI A17.1. The intent of the code is to have to a reliable power source and not to rely on one that may be on fire. Without supervision of

the 110-vac power circuit needed for the shunt breaker, the condition of the power necessary for the shunt breaker to operate during a fire is unknown. There have been instances where the breaker to the 110-vac power source for the shunt breaker has been turned off and the elevator power would not shunt upon operation of the heat detector.

3) Fire alarm system elevator interface summary: As described above, there will be five supervised control circuits from the fire alarm system that will interface with the elevator system. They are as follows (see following pictorial and the accompanying notes):

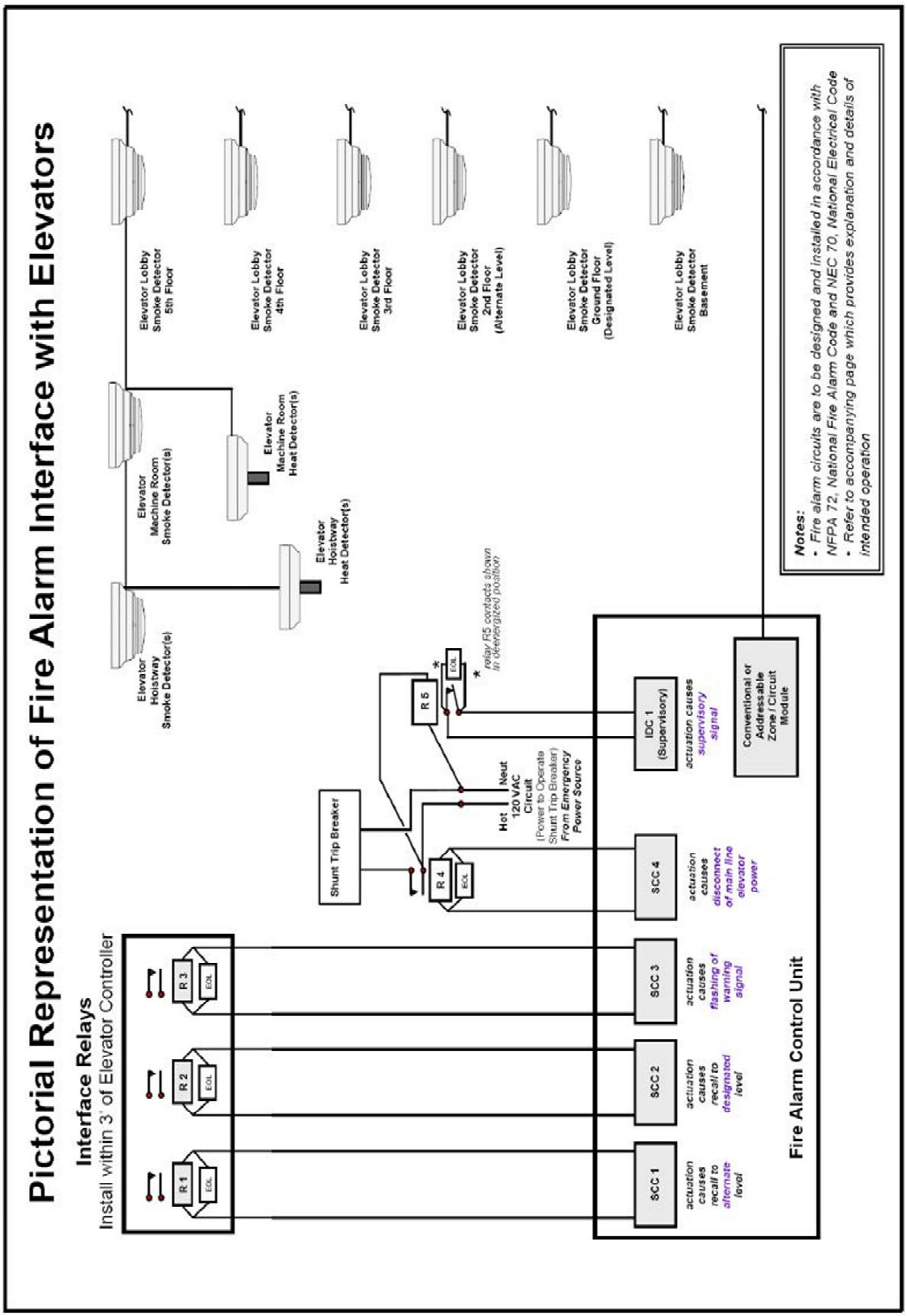
a. Input to elevator controller for Phase I recall to the designated level from actuation of smoke detectors other than at the designated level lobby.

b. Input to elevator controller for Phase I recall to the alternate level from actuation of a smoke detector at the designated level lobby.

c. Input to elevator controller to flash the firefighter helmet signal when recall is initiated by a smoke detector in the elevator machine room or hoistway.

d. Input to elevator main line power shunt trip breaker for power shut down from actuation of heat detectors in the hoistway or machine room.

e. Supervision of the 110-vac power source to the shunt breaker.


Pictorial Representation of Fire Alarm Interface with Elevators
Interface Relays
Install within 3' of Elevator Controller
R 1
R 2
R 3
R 4
R 5
EOL
Elevator Lobby Smoke Detector 5th Floor
Elevator Lobby Smoke Detector 4th Floor
Elevator Lobby Smoke Detector 3rd Floor
Elevator Lobby Smoke Detector 2nd Floor (Alternate Level)
Elevator Lobby Smoke Detector Ground Floor (Designated Level)
Elevator Lobby Smoke Detector Basement
Elevator Machine Room Smoke Detector(s)
Elevator Machine Room Heat Detector(s)
Elevator Hoistway Heat Detector(s)
Elevator Hoistway Smoke Detector(s)
relay R5 contacts shown in deenergized position
Shunt Trip Breaker
Hot
Neut
120 VAC Circuit (Power to Operate Shunt Trip Breaker) From Emergency Power Source
IDC 1 (Supervisory)
actuation causes supervisory signal
Conventional or Addressable Zone / Circuit Module
SCC 1
SCC 2
SCC 3
SCC 4
actuation causes recall to alternate level
actuation causes recall to designated level
actuation causes flashing of warning signal
actuation causes disconnect of main line elevator power
Fire Alarm Control Unit
Notes:
- Fire alarm circuits are to be designed and installed in accordance with NFPA 72, National Fire Alarm Code and NEC 70, National Electrical Code
- Refer to accompanying page which provides explanation and details of intended operation

Explanation of Fire Alarm Interface with Elevators

Notes:

- There can be many variations of the accompanying "Pictorial Representation of Fire Alarm Interface with Elevators."
- In this example, the smoke and heat detectors are addressable initiating devices and the operating relays are "hardwired."
- To achieve supervision, the relay circuits are operated from supervised control circuits. Sometimes NACs (Notification Appliance Circuits) are used to accomplish this function.
- The supervisory initiating device that monitors the power for the shunt trip circuit is connected to a supervisory IDC (Initiating Device Circuit).
- The scenario assumes that:
- There is a sprinklered elevator hoistway.
- Means to disconnect the main line power to the elevator is via a shunt trip breaker.
- System operation is in accordance with NFPA 72.

4) Relay (R5) and an IDC (Initiating Device Circuit) have been included to provide indication (via a supervisory alarm) of absence of voltage (power) to operate shunt trip breaker.

Components Function

R1 ----------Signal to elevator controller for recall to designated level.

R2 ----------Signal to elevator controller for recall to alternate level.

R3 ----------Signal to elevator controller for firefighter notification.

R4 ----------Signal to activate shunt trip relay.

R5 ----------Supervisory relay to monitor presence of voltage (power) to operate shunt trip breaker.

SCC1 ----------Supervised Control Circuit for operating R1.

SCC2 ----------Supervised Control Circuit for operating R2.

SCC3 ----------Supervised Control Circuit for operating R3.

SCC4 ----------Supervised Control Circuit for operating R4.

IDC1----------Initiating Device Circuit to supervise R5 contacts (monitoring power to operate shunt trip breaker).

4. Communications between Buildings:

- Buildings shall communicate trouble, supervisory, and alarm signals to Mason's Proprietary Keltron system, 24-hour staffed by Mason police and have the UL Proprietary designation. All signals must be transmitted via True Point Contact ID format via digital dialer. Provide a printer to make a hard copy of all signals and operator responses. Coordinate with the facility.

------END-----