GALAXY CONTROL SYSTEMS

ACCESS CONTROL & SECURITY MANAGEMENT SYSTEM

with Digital Video Surveillance

IMPORTANT USER NOTICES:

Cross-References to external sections: Certain cross-references are made to other sections using the variable "XXXXXX" (6 Xs). *These reference variables may appear in red text to help facilitate locating them*.

- The *Spec Writer* can use MS Word's Find function (Ctl+F) to [Find / Find Next] location of each occurrence of "XXXXXX". *Be sure you place your cursor at the top of the document or top of first page, or the point on the current page where you want to begin your search.*

- It is up to the *Spec Writer* to find and replace these cross-references with the actual section number in the real submittal of the BidSpec.

Alternate Choices of Options/Features: Any specifications herein that denote alternate choices are indicated by square brackets [ ]. These references may or may not appear in red text to help facilitate locating them.

- To be sure to find them all, the spec writer can use MS Word's Find function (Ctl+F) to [Find / Find Next] location of each occurrence of " [". *Be sure you place your cursor at the top of the document or top of first page, or the point on the current page where you want to begin your search*.

- It is up to the *Spec Writer* to find and select (keep) the acceptable choices for the real submittal of the BidSpec. Also you should delete the extra unneeded choices where multiple choices are provided.

Surveillance Equipment Specifications: Specifications for DVR and/or NVR are found in Part 1 and Part 2.

- It is up to the *Spec Writer* to keep whichever descriptions of equipment that will be included; and remove the descriptions for the type that will not be used.

- No terms/specifications regarding DVRs or NVRs have been included in Part 3.

PART 1 GENERAL

1.1 SECTION INCLUDES

A. Security/Perimeter Access Control System.

B. Digital Surveillance System.

1.2 SYSTEM DESCRIPTION - SECURITY/PERIMETER ACCESS CONTROL SYSTEM

A. Software Application shall be System Galaxy software communicating with 635 Series Access Control Panels (ACPs).

B. Access Control: shall connect to all reader and alarming devices to support the following:

1. Access Control: the access control system to the building and selected/restricted areas shall support the following technologies:

STANDARD CARD & BIOMETRIC TECHNOLOGIES

a. Proximity (125 KHz),

b. MIFARE®, MIFARE DESFire®, MIFARE DESFire® EV1, (13.56 MHz)

c. Biometric Identification & Authentication (1:1 and 1:N multi-factor),

d. HID® iCLASS®,

e. NFC,

f. Magnetic Swipe

g. Barcode (1D linear, 2D datamatrix, US & International formats),

GOVERNMENT CARDS

h. PIV, PIV-II, TWIC, CAC (Transition, Endpoint) HSPD-12 FIPS 201 Compliant

2. Exterior Doors: Control access into building at locations as shown on drawings.

3. Interior Building Areas: Control access into areas as shown on drawings.

4. Restrict Access of individual credential-holders by time of day, day of week/month/year and specific points of entry via user-configurable software.

5. Unlock Doors to building and selected areas automatically, where shown on drawings, for a scheduled period of time throughout the day allowing free access and egress without the use of a card and avoiding the generation of an alarm condition on the access control system. The system operator shall be able to lock and unlock doors from the computer system.

6. Monitor Points in building and selected areas as shown on drawings that may provide unauthorized access or egress and may be a point for forced entry. The system shall report changes in status for all monitored points indicating the specific location so the operator can respond appropriately.

C. Photo Badge Creation and Printing: the system shall be able to design Photo Identification ID Badges using the same cardholder photographs that are stored in the System Galaxy database / system and shall support and perform the following:

1. Digital photographs shall be stored as Blob in the database, or as JPEG, or both methods as a Blob and JPEG, as determined by system owner.

2. System shall be able to add static and dynamic data fields from the cardholder information, as well as photographs, graphic images, shapes logos, and backgrounds.

3. System shall be able to apply style and layout changes to any static or dynamic data fields; including resize, scale, rotate, flip, border/outline, color, font-style, font-size, and text related attributes such as bold, italics, underline.
4. Shall support standard graphic image editing, cropping, resize/scale, flip and rotate, border.
5. Shall be able to add and print unique, functioning bar codes in 1D (linear) and 2D (data matrix) formats.
6. Shall print badge designs in portrait or landscape layout, and shall be able to print single-sided or double-sided (i.e. one or both sides) PVC type cards using an IP or USB compatible, dye-sublimation printer.

D. Photo Verification: The photo verification feature shall be enabled on a workstation basis and shall use the digital image stored in the database as a blob, or the JPG image stored in the specified system folder.

E. Video Monitoring of doors and alarm points shall be provided when access is requested, or a door is violated. The system interface between the Access Control System and Video Surveillance System shall utilize a TCP/IP connection.

1. The Video Monitoring interface shall be compatible with the Discovery NVR / DVR [Discovery-OWS] [ONSSI] [Avigilon] [Milestone] [Salient] [LENSEC-PVMS] [Panasonic Video Insight VI7] [Digital Watchdog DW Spectrum] [WiseNet Wave] video product line(s), or other approved alternate brands.
2. **Video and Camera Control** shall be supported within System Galaxy.
    a. System shall be able to associate cameras with doors, inputs/alarm points, elevator doors.
    b. System shall support manually and automatically calling up video and shall be capable of playing live video from system-linked points when a system alarm is generated.
    c. System shall be able to retrieve associated video from historical event report.

F. Visitor Management shall support the ability to assign access privileges and add credentials to the access control system, as well as set credential expiration through the visitor management interface. Shall include ability to manage visitor credentials and access privileges including credential expiration from the access control system (System Galaxy). Shall support visitor signing into and out of the visitor management system and be registered with the Access Control System (ACS) and with the access privileges activated/deactivated as appropriate. Shall support visitor management through HID Global EasyLobby® or STOPware ® PassagePoint Global.

G. Real-time Guard Tour shall track and monitor progress and times from tour start and progress to check points, to tour stop. Sequential and Random tours supported, track late/overdue tour start, late/overdue to check points, late to finish tour. System shall report missed points, expired and incomplete tours, successful tours, and time expired between tours. System shall support multiple tours using a common start reader and starting tours with PIN codes.

H. Real-Time Hall Pass / Card Tour shall track and monitor progress and times from tour start and progress to select checkpoints, to tour stop. The system shall provide notification based on skipped checkpoints and incomplete / overdue tours.

I. Graphical Display of building maps shall be provided on all access control workstations using dynamic icons that display real-time status of doors and alarm points.

J. Report Generation shall be provided for all system events and alarm events by date and time.

K. System Interface shall provide the following:

1. A real-time display of all alarms and system events
2. The ability to archive all events to the SQL database
3. And shall serve as the instrument through which all system programming is accomplished.

L. Computers/Workstations shall be configured for the intended system function by installing the appropriate system software, services and operating system.

1. Security Monitoring Workstation: The Security Monitoring Workstation shall be installed in the appropriate secure location and shall run the appropriate System Galaxy software and services needed for interfacing the system activity and database administration with all System Galaxy Clients on the LAN/WAN Network.
   a. This workstation shall have a Windows-10 or Windows-8 operating system.
   b. This workstation shall support event and alarm monitoring, video surveillance and be configured as required by system-owner.
2. Badging Workstation: The Badging Workstation shall be installed in the appropriate secure location and connected to the LAN/WAN Network. The Badging Workstation computer shall run the System Galaxy software and services.
   a. This workstation shall also have a Windows-10 or Windows-8 operating system.
   b. The badging workstation shall support the following devices for card/credential issuance:
      1) Ultra Magicard IP or USB Printer (dye-sub, PVC card compatible).
      2) Videology Digital USB Camera (TWAIN, or WIA, or WDM compatible).
      3) GCS USB Card Enrollment Station.
      4) HID OMNIKEY USB Smart Card Reader/Writer Enrollment Station.
      5) Sagem MorphoTrak MSO-300 USB Fingerprint Enrollment Station.
      6) Topaz USB Signature Pad.
3. Central Database Server: The Central Database Server shall be installed in the appropriate secure location. The system shall provide connectivity between the Central Database Server all Access Control Panels over a Local/Wide Area Network (LAN/WAN).
   a. The database server shall serve as the instrument through which all system programming is stored.
   b. The system shall provide real-time transactional storage of all system events.
   c. The system shall archive date/time-ordered events in a separate archive database.
   d. The database server shall have Windows Server 2012 R2 | 2016 operating system.
4. Access Control Panels (ACPs): The ACPs shall be installed in the secure equipment rooms as indicated on the Contract Documents, communicating to the Central Server over a local LAN/WAN connection.

1.3 SYSTEM DESCRIPTION FOR DIGITAL SURVEILLANCE

A. The surveillance system shall be capable of operating in a multi-system configuration using LAN/WAN connection.

1. The Digital Surveillance Software shall be capable of operating with System Galaxy software and security monitoring stations; and shall be capable of producing court-

admissible video evidence for use by officials and law enforcement.

2. The System shall be capable of supporting up to a minimum of 32 IP cameras or Analog cameras in various frame-rate speeds at up to 30 frames/second per camera.
    a. The camera connectivity and frame-rate performance shall use the identical application software.
3. Systems shall be interchangeable and be connectable through the same Remote Access Software within a security management system, regardless of the scale or system configuration.
4. The System shall be configurable in a desktop or rack-mount model for indoor use in a secure location that maintains the appropriate environment for computer equipment.
5. The Application software shall allow multiple systems to be concurrently accessed by remote users from a single screen.
6. The Application software shall allow multiple systems to intercommunicate using LAN/WAN connections without additional hardware or software.

B. The Network Video Recorder (NVR) shall offer current digital recording technology, product reliability, security, ease of use, and customer support structure.
1. Model availability in 16, 32 or 64 channel configurations with a system-wide recording rate up to 960 IPS (NTSC or PAL).
2. The Network Video Recorder (NVR) shall be a complete network video recording solution. The combination of motion detection features, email alarms, advanced search capabilities, full megapixel support on all channels, and specialized remote monitoring technologies shall provide a highly robust and reliable system.

C. The Hybrid Digital Recorder (DVR) shall offer current digital recording technology, product reliability, security, ease of use, and customer support structure.
1. Model availability in 16 and 32 channel configurations with a system wide recording rate up to 480 IPS (NTSC or PAL); supporting both IP cameras and Analog cameras.
2. The Digital Video Recorder (DVR) shall be a complete hybrid digital video recording solution. The combination of motion detection features, email alarms, advanced search capabilities, full hybrid support on all channels, and specialized remote monitoring technologies shall provide a highly robust and reliable system.

1.4 RELATED WORK

A. In addition to work described above, the work shall include, but not necessarily be limited to, the following:
1. Equipment identification, as specified elsewhere.
2. Access control devices and surveillance identification, as specified elsewhere.
3. Providing all cabling, conduit and connections as required for complete and functional systems, as specified elsewhere.
4. Providing 120/220 VAC uninterruptible power as required for all equipment provided under this section, as specified elsewhere.
5. Furnished equipment shall be assembled and installed in accordance with manufacturer's recommendations and instructions, as specified elsewhere.
6. Providing door hardware for remote monitoring and control of openings as scheduled under this section as specified elsewhere.

1.5 RELATED DOCUMENTS

A. The Drawings and General Provisions of the contract, apply to this section.

B. Refer to all Contract Drawings and Specifications listed in [Section XXXXXX] for additional requirements.

1.6 SUBMITTALS

A. Submit under provisions of Section XXXXXX - Administrative Requirements.

B. Product Data: Manufacturer's data sheets on each product to be used, including:

1. Preparation instructions and recommendations.
2. Storage and handling requirements and recommendations.
3. Installation methods.

C. Shop Drawings: Include system components and controls, installation requirements, and relationship with adjacent construction.

1.7 QUALITY ASSURANCE

A. Manufacturer Qualifications:

1. Company specializing in manufacturing the products specified with minimum 30 years documented experience.
2. Manufacturer shall be capable of providing through its resellers a sole-source, turn-key solution including, but not limited to system server, customary cameras, wiring, networking components, and other peripherals essential for operation of the solution.
3. Manufacturer shall be directly accessible to end users for advice on service, support, and warranty issues. Manufacturer shall maintain support information for public access on a web site and facilitate contact with technical resources.
4. Software updates shall be freely accessible for download from the manufacturer's web site and available at no charge with a valid maintenance agreement. Terms for release of software revisions offering substantially new capabilities shall be offered for sale or at no cost with a valid maintenance agreement.
5. Manufacturer's operation manual and training tutorials shall be directly accessible through the software main menu and provided on PC-compatible CD for installation on any personal computer. The manual and tutorial shall provide for intuitive topic search and help for system operation and function explanations. Additional computer support and help utilities shall be included on the system server main menu to assist in managing functions such as multi-media control, file management, disk and media management, file authentication, backup and more.

B. Installer Qualifications:

1. Company specializing in installing the Products specified in this section and Related Work with minimum five (5) years documented experience. Experience shall include projects with access control systems of similar scope and magnitude of the project. Company shall be a Certified Dealer/Value Added Reseller of the manufacturer and within ### miles (### km) of project.

1.8 DELIVERY, STORAGE, AND HANDLING

A. Store products in manufacturer's unopened packaging until ready for installation.

B. Store and dispose of solvent-based materials, and materials used with solvent-based materials, in accordance with requirements of local authorities having jurisdiction.

1.9 PROJECT CONDITIONS

A. Maintain environmental conditions (temperature, humidity, and ventilation) within limits recommended by manufacturer for optimum results. Do not install products under environmental conditions outside manufacturer's absolute limits.

1.10 COORDINATION

A. Provide system including networked computers, access control panels (ACPs), credential readers, credentials and badging station.

B. Provide detection devices.

C. Connect electric strikes and monitor status of door controls.

D. Provide request for egress Passive Infrared Detectors (PIR) and/or pushbuttons.

E. Provide all required power supplies.

F. Provide all cabling connections required.

G. Provide all specialty conduit requirements. Coordinate with the Electrical Contractor.

H. The security contractor in coordination with the door hardware supplier shall provide the security components as scheduled and indicated on the Contract Drawings.

1.11 WARRANTY

A. Manufacturer’s Warranty of Security/Perimeter Access Control System:

1. Provide a full performance and material guarantee for two years from the final acceptance of the Galaxy manufactured hardware. The warranty shall be unconditional for all Galaxy manufactured hardware.
2. Technical support shall be available for 24 hours per day and 7 days per week to all Certified Dealers/Value Added Resellers.

B. Manufacturer’s Warranty of Digital Surveillance System:

1. The digital recorder shall come with a minimum 3-year manufacturer’s warranty with the 1st year including advance replacement service. Each unit shall have the purchase option to upgrade the warranty period up to 5 years and 2 years of advance replacement service.
2. Technical support shall be available for 24 hours per day and 7 days per week to all integrators and Certified Dealers/Value Added Resellers free of charge.
3. Certified Dealer/Value Added Reseller shall include a 3-year conditional warranty and shall offer additional services such as manufacturer system configuration.
4. Manufacturer's warranty shall include 30-day exchange for new equipment from the Dealer/VAR’s date of invoice plus one-year depot parts and labor repair for systems not having had the terms of the warranty voided. Extended warranty contracts shall include extended term and hot-swap provisions.

C. Dealer/Value Added Reseller Warranty of Installation:

1. [Dealer/VAR to supply terms and conditions here].

1.12 SPECIAL TOOLS, EQUIPMENT AND MATERIALS

A. All necessary equipment, materials, and special tools that are required to maintain each system provided under this Contract, shall be delivered to the System Owner or owner's representative by the Contractor. Additionally, a complete list of said necessary equipment, materials, and special tools shall be submitted to the System Owner within a minimum of two (2) weeks prior to final acceptance test.

1.13 CODES, STANDARDS, REGULATIONS AND COMPLIANCES

A. The codes, standards, regulations and compliances listed in the Contract Documents are part of the Contract to the extent of their applicability to the project. The latest edition of the following codes, standards and regulations apply:

B. Precedence & Conformity:

1. In the event of any conflicts between or among different codes or standards, the Contractor shall notify the Design Professional to obtain clarification before proceeding with the work.
2. Conform to local jurisdictional requirements where appropriate.

C. National Fire Protection Association (NFPA):

1. NFPA 70 - National Electrical Code.
2. NFPA 101 - National Life Safety Code.

D. Safety Standards:

1. UL 294, Fifth Edition, Access Control System Units.
2. UL 1076, Fifth Edition, Proprietary Burglar Alarm Units and Systems.
3. CSA C22.2 No. 205-M1983, First Edition, Signal Equipment.

E. Federal Communications Commission (FCC) Rules and Regulations: (Title 47 CFR) Part 15 - Subpart-B: Radio Frequency Devices – Unintentional Radiators.

F. Encryption Standards: (AES) Advanced Encryption Standard Algorithm.

G. Homeland Security Presidential Directive 12 (HSPD-12) Policies for Common Identification Standard for Federal Employees and Contractors.

1. Federal Information Processing Standards (FIPS): FIPS 201 thru 201-2 (PIV, PIV-I, PIV-II): Personal Identity Verification of Federal Employees and Contractors.
2. Option to perform PKI challenge to the Personal Certificate (PACS)

H. DoD Information Assurance Certification and Accreditation Process (DIACAP): United States Department of Defense (DoD) process to ensuring the application of risk management to information systems.

PART 2 PRODUCTS

2.1 MANUFACTURERS

A. Acceptable Manufacturer: Galaxy Control Systems, which is located at: 3 North Main Street ; Walkersville, MD 21793-0158; Toll Free Tel: 800-445-5560; Tel: 301-845-6600; Fax: 301-898-3331; Email:request info (info-usa@galaxysys.com); Web:www.galaxysys.com

B. Substitutions: No substitutes will be permitted.

C. Substitutions: Requests for substitutions will only be considered in accordance with provisions of [Section XXXXXX - Product Requirements].

D. Cards shall be manufactured by Allegion Plc., Farpointe Data Inc., HID Corporation, or approved equal.

E. Card readers, long range proximity card reader shall be manufactured by Allegion Plc., Bridgepoint Systems Inc., Essex Electronics Inc., Farpointe Data Inc., HID Corporation, Identive Inc., Nedap N.V., Veridt Inc., or approved equal.

F. Wireless reader locksets shall be manufactured by Assa Abloy, Allegion Plc, Salto Systems Inc.

G. Biometric readers shall be manufactured by Sagem MorphoTrak.

H. Dye-sublimation “badging” printers shall be Magicard manufactured by Ultra Electronics.

2.2 ACCESS CONTROL AND MANAGEMENT SYSTEM

A. System: Access Control System shall be System Galaxy provided by Galaxy Control Systems.

B. System Requirements:

1. The contractor shall be responsible for providing a complete and functional system as specified. All devices required to complete the installation may not be described within this subsection but shall be provided as if specifically called for within the specification. All system components shall be approved and certified for the function they will perform.
2. The Access Control System (ACS) shall be an enterprise-class system that supports system programming, system monitoring, administrative activities, report generation, card/credential enrollment and ID badge issuance.
3. The system’s database server shall be Microsoft SQL Server 2012 R2 / 2012 R2.
4. A workstation that gives a user an interface allowing the control of the local/global sites shall be provided by Contractor or Customer as agreed upon in contract documents.
5. The system shall be capable of utilizing a true client-server network that is configured to support the system database, all services, all applications, all access control panels.
6. The Contractor shall optimize existing system settings as required by system owner to support the system operation, system monitoring, credential enrollment, badge ID issuance, and record keeping.
7. Contractor / VAR shall provide adequate system & end-user training
8. A single Microsoft SQL database shall store both credential-holder’s records, access system information, and programming parameters.

C. Access Control Panels (ACPs) and Cabinet Enclosures:

1. The Access Control Panels (ACPs) shall be of a distributed database design; and shall use intelligent microprocessors to make smart decisions at the Access Control Panel.
2. Physical Specifications for wall-mounted Access Control Panels (ACPs):
    a. Enclosure shall be a NEMA 1 / IP1-A standard.
    b. Description: 18-gauge, metal electrical cabinet with hinged, locking door.
    c. Electrical requirements: 120/220 VAC, 60/50 Hz, 220 Watts, POE 15/30 Watts.
    d. Panel Configurations & Physical Dimensions:
        1) 2-door panel - 2 amps; (12” x 12” x 4” in).
        2) 2-door POE panel - 15/30 Watts; (12” x 12” x 4” in).

3) 8-door panel - 2 amps; (18” x 13.75” x 6.25” in).
4) 16-door panel - 10 amps; (32” x 13.75” x 6.25” in).

3. Physical Specifications for rack-mounted Access Control Panels (ACPs):
   a. Description: 18-gauge, metal electrical cabinet with hinged, locking door.
   b. Electrical requirements: 85/264 VAC, 60/50 Hz, 220 Watts.
   c. Standard Rack Units: 4 Units(4U). Dim: 7x19x18.75 in. HxWxD (18 x 49 x 48 cm).
   d. Weight: 26 lbs. (11.79 kg).
4. Environmental Specifications for Access Control Panels (ACPs):
   a. Temperature Range: -10° C to +60° C, non-condensing.
5. Relay Output Ratings for Access Control Panels (ACPs):
   a. Form-C Relays, 24 VAC, 1.5 amps maximum.
6. Communication Specifications for Access Control Panels (ACPs):
   a. TCP/IP 10/100 MB Ethernet
7. The following components shall be mounted in appropriate location in relation to the access control panel:
   a. Central Processing Unit (CPU) for the Galaxy Access Control Panel (ACP).
   b. The appropriate daughter boards (DRM, DIO, DSI, AMM or Output Modules) as required to provide proper access control and to control of inputs and outputs or other peripheral devices (hardwired or wireless) according to the system requirements.
   c. Two-piece, standard DB type connectors, for connecting boards to peripheral hardware.
   d. The supervision resistors shall be installed as close as possible to the device-end and according to requirements of system owner.
   e. Lock diodes shall be installed over locking device, as required per lock type.
   f. Power Supply(s) and Batteries: power supply and sealed back-up batteries shall be included with the ACP.
   g. Tamper switch: The cabinet shall be protected by an anti-tamper device in such a way that a tamper alarm shall be generated if any portion of any door moves more than one quarter of one inch from its closed position. This alarm shall be sent to the Monitoring Station.
   h. Other equipment required to provide a functional, working system.

D. Power Requirements:
1. The Access Control Panels and related hardware shall be fed from a UPS system power at 120/220 VAC as required.
2. Each Access Control Panel shall have the following:
   a. Sealed, no-maintenance, rechargeable batteries.
   b. Sufficient power shall be included to allow the ACP to operate a minimum of 8 hours when loaded to its maximum configuration and capacities.
   c. Power back-up shall be of such size and capacity that 8 hours can be increased to a minimum of 24 hours.
   d. An alarm with descriptive message shall be generated at the Computer whenever an ACP loses AC power and is operating on battery power.

e. An alarm with descriptive message shall be generated at the Computer whenever an ACP loses back-up battery power.

3. Lock Power Supply:

a. The electric lock power supply shall be +24 VDC at 4 Amp, 6 Amp, or 10 Amp as required by site loads.

b. The lock power supply shall include multiple DC outputs on separate Class 2 current-limited fuses, fused line voltage input, and individual manual on/off switching with individual LED indicated power status.

c. Provide quantity of BPS-24 power supplies and batteries as required to maintain maximum 75% load for each power supply set.

d. Provide a means to release doors as required by NFPA or local jurisdiction.

E. Life Safety

1. Card access system's lock power supply shall be connected to the fire alarm system by the Security Contractor.

2. All electric doors in pathway of building egress shall release as required by life safety codes.

F. Access Control System - Database Server Requirements:

1. Provide computer operating current, compatible Microsoft Server operating system supported by manufacturer, with the following specifications:

a. Microsoft SQL Server 2012 R2 | 2016

b. 16 Gigabytes (GB) of RAM,

c. 40 GB Free Hard Drive Space (minimum); or scale to size of system.

d. 10/100/1000 Mbps fiber optic NIC Ethernet card,

e. CD-RW Drive,

f. Two (2) USB Ports (minimum speed 2.0),

g. Additional ports as required to meet each manufacturer's interface requirements and to provide a fully integrated system.

h. Wide-screen Monitor, capable of 1280x1024 minimum resolution

i. Optical Mouse,

j. Keyboard,

k. LaserJet report printer (USB or network),

l. The database server shall meet or exceed specified requirements for the current version of System Galaxy software.

2. Provide complete programming as required for proper operation:

a. Provide password protection and operator levels.

b. Microsoft Database Management Studio software shall be installed.

c. Provide integration to 3rd Party Applications as required by Owner under Contract agreement at commissioning of system.

G. Access Control System - Security Monitoring Workstation Requirements:

1. Provide computer operating current, compatible Microsoft Server operating system supported by manufacturer, with the following specifications:

a. Microsoft Windows-10 or Windows-8 operating system

b. 4 Gigabyte (GB) of RAM,

c. 40 GB Free Hard Drive Space (minimum); or scale to size of system

d. 10/100/1000 Mbps fiber optic NIC Ethernet card.

e. CD-RW Drive,

f. Two (2) USB Ports (minimum speed 2.0),

g. Additional ports as required to meet each manufacturer's interface requirements and to provide a fully integrated system.

h. Wide-screen Monitor, capable of 1280x1024 minimum resolution

i. Optical Mouse,

j. Keyboard,

k. LaserJet report printer (USB or network),

l. The monitoring workstation shall meet or exceed specified requirements for the current version of System Galaxy software.

2. Provide complete programming as required for:

a. Password protection and operator levels.

b. Graphical User Interface (GUI), including graphic maps/floor plans with all devices shown. Provide all alarm, trouble, access, Alarm/event reporting, and GUI operator interfacing through the graphic maps in the system software.

c. Alarm notification, acknowledgement and actions taken.

d. Provide integration to 3rd Party Applications as required by Owner under Contract agreement at commissioning of system.

e. Interface with Video Surveillance System for integrated GUI screens and on-screen camera call-up and control.

f. System Management Reports: Provide an interface report printer as specified in this Section.

H. Access Control – Credential Enrollment & Badging Client Workstation:

1. Provide computer operating current generation Microsoft operating system supported by manufacturer, with the following specifications:

a. Microsoft Windows-10 or Windows-8 operating system

b. 4 Gigabyte (GB) of RAM,

c. 40 GB Free Hard Drive Space

d. 10/100/1000 Mbps fiber optic NIC Ethernet card

e. CD-RW Drive,

f. Wide-screen Monitor, capable of 1280x1024 minimum resolution

g. Optical Mouse,

h. Keyboard,

i. Two (2) USB ports, minimum 2.0.

j. Additional ports as required to meet each manufacturer's interface requirements and to provide a fully integrated system. See following subparagraph for full list of devices supported by System Galaxy for credential enrollment and badge issuance, as well as manufacturer's specifications for visitor management software.

k. Videology USB Camera - either TWAIN, or WIA, or WDM compatible; including flash, tripod and backdrop.

l. Ultra Magicard, Dye-sublimation Printer for printing PVC ID-badges.

m. LaserJet Report/Dossier Printer (USB or network).

n. The badging workstation shall meet or exceed specified requirements for the current version of System Galaxy software.

2. Provide complete programming as required for:

a. Password protection and operator levels.

b. Provide integration to 3rd Party Applications as required by Owner under Contract agreement at commissioning of system.

c. Credential Management: The credential enrollment and badging workstation shall support the following devices for card/credential and ID badge issuance:

1) Ultra Magicard IP or USB Printer (dye-sub, 1-/2-sided PVC card compatible).

2) Videology Digital USB Camera (TWAIN, or WIA, or WDM compatible).

3) GCS USB Card Enrollment Station.

4) HID OMNIKEY USB Smart Card Reader/Writer Enrollment Station.

5) Sagem MorphoTrak MSO-300 USB Fingerprint Enrollment Station.

6) Topaz USB Signature Pad.

d. System Management Reports: Provide an interface report printer as specified in this Section.

e. Client workstation may be additionally configured to support system programming, diagnostics, and security monitoring operations as a secondary line of duty when not in use as a badging, or credential enrollment, or cardholder management station.

I. Software Capacities:

1. The software development tools and language shall be an existing, industry-accepted, type that is widely used in commercial systems. The system shall be modular in nature, allowing the system capacities to be easily expanded without requiring major changes to the system operation, while maintaining all defined system data as well as historical information.

2. Graphical User Interface (GUI): All System functions shall be accessible via point and click mouse control. Systems requiring command string control or complex syntax are not acceptable.

3. The following features are included in the system:

a. Access Control Panel Capacities and Hardware Attributes:

1) 10,000-event log buffer for disconnect transaction storage at intelligent ACP.

2) 50,000 credential capacity at the intelligent ACP; Unlimited card/credential capacity from SQL Database with Card Lookup enabled at the ACP.

3) Up to 32,000 Input/Output capacity with the ability to control field devices using Boolean logic (configured through software) .

4) 256 Time Schedules per loop/cluster with unlimited loops/clusters per site; includes “Always”, “Never”, and 254 user-definable schedules/periods.

5) Two (2) Time Formats for programming Time Schedule (15-Minute Schedule format and 1-Minute Schedule format; defined at the loop-level).

6) Nine (9) unique Holiday Types when using 15-minute schedules; i.e. 9 x 254 user-definable schedules per loop/cluster (unlimited loop/clusters per site).

7) 100 Day Types / Holiday Types when using 1-Minute Schedules, including 256 user-definable Time Periods and 256 user-programmable Schedules per loop/cluster (with unlimited loop/clusters per site).
8) 2000 user-defined Access Groups. Scales to unlimited access privilege combinations by using the Individual/Personal Doors feature, which can be assigned exclusively or in tandem with Access Control Groups.
9) Dedicated Door Contact and Request to Exit (REX) inputs for each defined reader.
10) Provides primary and auxiliary door outputs for each defined door/reader.
11) User-definable Door Supervision
12) User-definable Alarm Input Supervision
13) Traditional Elevator Control through general output relays
14) Otis Compass® Destination Entry elevator system integration.
15) Schindler Port Technology Destination Dispatch elevator system integration.

b. Access Control Privileges:
1) 2000 user-defined Access Groups. Scales to unlimited access privilege combinations by using the Individual/Personal Doors feature, which can be assigned exclusively or in tandem with Access Control Groups.
2) Ability to assign any combination individual doors to credential using the Individual/Personal Doors feature.
3) Ability to assign multiple Access Groups per credential as well as combine both Access Groups and Individual/Personal Doors on credentials.
4) Access Override from Server – configurable through user-defined override rules and exception conditions.
5) Access Group deactivation option – changes affected access group from the scheduled privileges to “Never” only for all users’ who are assigned to the deactivated Access Group upon applying deactivation.
6) Automatic Activation and Expiration by Date & Time for Access Groups.
7) Automatic Active/Expire Dates for cards/Credentials.
8) Automatic Expire by Date & Time for cards/credentials.
9) Automatic Expire by Maximum “number of uses”.

c. Additional Hardware Functions Configured from Software:
1) Setup Wizards – for adding hardware loop/cluster and panels
2) Software Diagnostic Tools
3) Global Anti-Passback.
4) Door Interlocking (Mantrap).
5) Door Groups – lock/unlock access and/or door group reporting.
6) Schedulable PIN Required option
7) Scheduled Unlock, with optional rule to require a Valid Unlock on the “day of” the scheduled unlock.
8) Remote Door Control - lock/unlock access.
9) User-selectable Reader LED behavior.
10) Optional door programming to meet Americans with Disabilities Act (ADA) compliancy in door and access operation.
11) Input/Outputs linking with Boolean logic.
12) Wireless Reader Interfaces for door access control (ASSA Aperio, Salto Sallis, and Schlage AD-400/AD-300).
13) IP Reader Interfaces for door access control ASSA ABLOY.

d. Access Control, Event and Alarm Monitoring & Control:
   1) Routable Alarm events.
   2) Event Log Output by email, TCP/IP, RS-232, and text file.
   3) Alarm Event Priority - user-definable priority ranges, priority assignment at the individual device level (reader/door, input, camera, etc.);
   4) Dynamic Device Graphic Screen (fixed GUI display; or detachable/floating GUI window with one-click preset command).
   5) Manual, Automated, and Scheduled Operator-command control of system hardware: control doors, inputs, outputs, elevators, request to enter, call up DVR/NVR video. Operator control commands issued through manual clickable GUI options and through user-definable automated script macros.
   6) Photo Verification, with trigger by Valid Access Events, Invalid Access Attempts, and/or on Passback Events; and optional 'automatic next' credential queuing.
   7) Traced Cards/credentials.
   8) Operator Commands: provides real-time operator control to control the state of the physical device through a mouse-click (lock/unlock, arm/disarm, shunt/unshunt, disable for service, etc.)
   9) Command Scripts: provides operator real-time intervention and scheduled control of the physical devices by launching a pre-configured script (lock/unlock, arm/disarm, shunt/unshunt, disable for service, etc.)

e. Credential Management and ID Badge Issuance:
   1) ODBC Data Import/Export (external databases) through an Import Utility.
   2) Import Cardholders and Credential IDs through an Import Utility from any ODBC compliant files.
   3) Import, activate & deactivate cardholders through Active Directory changes.
   4) Enroll access cards, proximity and smart cards; biometric credentials.
   5) Encode credentials: magnetic swipe, biometric, smart card (MIFARE®, MIFARE DESFire®, HID® iCLASS®).
   6) Supports multiple cards and/or biometric credentials per single cardholder.
   7) Enroll and assign alarm control cards - for arming/disarming the Access Control System from a card reader.
   8) Assign credentials as Guard Tour cards or as Hall Pass (Card Tour) cards.
   9) Design (create, modify, print) ID Badges – see Badge Printing in this section.
   10) Cardholder Badge: Print Tracking Print Count, Print Limit, Print Preview.
   11) Cardholder Dossier: Print Tracking, Print Count, Print Limit, Print Preview.
   12) 50 user-customizable Data Fields: supports user-customized field names (columns); function as text data entry or as pre-configured select lists;
   13) 14 additional user-definable Data Select Lists.
   14) Able to designate any system-default or user-customizable fields as mandatory, thereby requiring data entry or item selection before committing the cardholder record to the database.
   15) Configurable Alarm Panel User ID per person/cardholder (with Bosch).
   16) Operator-entered memo notes on Cardholder records.
   17) Programmable message text for LCD display: Supports system-wide text and unique-text per individual credential-holders.
   18) Ability to partition credential-holder population by "Customer" (DB entity)
   19) Ability to partition credential-holder population by "Department" (DB entity)
   20) View and Print credential activity reports & cardholder management reports.

21) Cardholder Audit Reports: view and print chronological audit trails of change history by Operator name; date/time and description of actions are included.
22) Online Help System: view and print information and instructions on how to configure and operate the system features.

f. Integrations:
1) DVR/NVR integrations with Discovery NVR / DVR [Discovery-OWS] [ONSSI] [Avigilon] [Milestone] [Salient] [LENSEC-PVMS] [Panasonic Video Insight VI7] [Digital Watchdog DW Spectrum] [WiseNet Wave] video product line(s), or approved alternate brands.
2) Import Camera names and link cameras to readers, inputs, and other devices.
3) **Active Directory Integration** (LDAP protocol) allowing the system to manage cardholder accounts using the AD domain user management tools.
4) Elevator System Interface with Otis Compass® Destination Entry, including passenger features. Reporting floor destination; controlling elevator call, speed, or exclusive car selection based on access privileges and USER-definable cardholder indicators for Otis Elevators (i.e. VIP, Split Group, Vertigo, and Extended Door Open Time for Accessibility).
5) Elevator System Interface with Schindler PORT Technology Destination Dispatch: automatically import credential-holder access privileges and supports multiple Master Group configurations.
6) Traditional Elevator Control Interface using relay output linking.
7) Visitor Management via STOPware® Interface or EasyLobby® – including ability to manage visitor credentials and access privileges including credential expiration from the access control system (SG). When a visitor signs into visitor management system, the visitor is registered with the Access Control System (ACS) and their access rights/privileges activated.
8) Alarm Panel Intrusion Detection Systems

g. Activity Reporting using a selection matrix.

h. Embedded Crystal Report™ Templates

i. Customizable Operator Privileges: allow/restrict commands, system programming and viewing/editing data. Privileges are enforced system wide.

J. Software Operation:

1. The system shall provide a top-down configuration methodology. System shall allow the system operator to programmatically configure the software and hardware devices, options, and features in a fluid and logical method. The system shall organize the configuration of features so as to allow the operator to progress from the highest to the lowest configuration levels/entities in the system. The operator shall be able to move progressively through the configuration of dependent levels/entities in a logical manner without unnecessarily swapping between menus and screens.

2. The system shall utilize dynamic icons. The dynamic icons shall change appearance, in both color and icon display based upon the status of the associated object. This appearance change shall occur in real time and shall not require the system operator to perform a screen refresh or exit the current screen.

a. Dynamic icons shall be provided to represent:
1) Doors lock control.
2) Cameras and domes.
3) Alarm inputs.
4) Output control relay.

5) Manual operator actions.

b. For intelligent access control panels that are online and communicating with the Communication Server, the dynamic icons shall reflect the true state of the device represented by the icon.

3. User-definable/populated “Drop-down List” Data Fields (i.e. select-list, drop-list boxes): Where certain data fields within data screens may contain the same information, the system shall provide the ability to define default settings for these data entry fields including "drop-down" select lists. The operator shall be able to change the default setting without impacting objects that have already been defined.

4. It shall be possible to use third party report tools, such as Crystal Reports to generate reports not already provided by the Access Control System, such as statistical or graphical reports of system activity.

5. Date format: The system shall support the date being formatted in the GUI display as dd/mm/yy or mm/dd/yy, depending upon the customary local date formatting.

6. Configurable Operator Account Profile: The system shall support creating unique operator accounts with unique login and passwords. System shall support operator levels that control access to viewing and editing data, online options and filters privileges.

K. Hardware Configurations:

1. Menu Configuration: The system software shall allow for the configuration of the access control panels through the use of simple menu commands. The menu commands may be executed by keyboard keystroke and point-and-click mouse control.

2. Clusters/Sites: The system software shall allow the configuration for up to 255 Clusters each maintaining up to 254 intelligent access control panels with ability to configure and maintain all Clusters simultaneously.

3. Database Updates: The system software shall download/upload information to/from the System Server automatically while the ACP is in communication with the CPU.

L. Time Specifications: Configuration of Time Periods and Holidays.

1. Configuration of Time Periods: Each time period shall represent a one (1) week and shall be divided into seven (7) days (i.e. seven fixed 24-hour time segments).

a. Each time 24-hour segment shall represent one (1) day and shall be divided into user-configurable time capsules. The number of time capsules (or their time equivalency) shall be determined by the chosen format assigned to the cluster (i.e. 1-minute or 15-minute formatting). All ACPs within the Cluster will operate on the same time formatting.

b. The software shall provide granular control of the time capsules by single-click, double-click and click-and-drag mouse functionality to allow the user activating and deactivating each individual time capsule.

c. The time period programming shall include the ability to assign holidays/special days and shall utilize the same granular formatting as assigned to the cluster (i.e. 1-minute or 15-minute formatting).

d. The software shall provide a utility to copy time segments and also support the operator defining time ranges to expedite the task of configuring time periods.

2. Configuration of Holidays: The system software shall not limit the number of days that can be chosen as a holiday. Holidays shall be considered as additional days of the week and shall have user-programmable date/time parameters that are independent from the normal date/time designations for each day.

a. When using the 15-minute time schedule format, the system shall allow up to

nine (9) types of holidays to be defined/created per cluster/site. User shall have control over setting the 15-minute time segments as active or inactive, independently from the non-holiday programming.

b. When using the 1-minute time schedule format, the system shall allow up to one hundred (100) day-types to be defined per cluster/site. The system operator shall be able to determine which Day Types are designated as holidays. User has control over setting the 1-minute time segments as active or inactive.

3. Global Cluster/Site Control of Schedules: using the Loop Group feature, the software shall allow the system to propagate changes to schedules, time periods, holidays and day types across all clusters/sites. A main cluster/site shall be able to selectively include or exclude other clusters/sites when propagating changes within a Loop Group. Clusters must be assigned to the Loop Group in order to participate in the propagation of time changes. Participating clusters/sites shall be able to override the propagated changes at the local level.

M. Time Zone Management:

1. General: The system shall allow the end user to configure the system server, workstations, and access control panels to be in different time zones (such as Eastern Standard Time, Pacific Time, etc.).
2. Operating System: The system shall support all time zones supported by the operating system. When defining a time zone to be used by the system, the system shall be provided with a drop-down listing of all time zones defined by the operating system. The operator shall be able to select the appropriate time zone from this listing.
3. Event Monitoring Workstations: The event activation date/time will be the date/time at the access control panel based on its geographical location according to its assigned time zone.

N. Alarm Events:

1. Alarm Event Function: Events shall be used to allow the system to react to system activity. When an event occurs, the system shall be able to perform multiple functions such as notify operator, display event message, activate a signal or bell, display list of response actions, call up live video, call up graphic map, etc.
2. Alarm Event Priority: The system shall allow a user-definable alarm priority (numeric value) to be assigned to individual devices and events.
   a. The system shall provide 10,000 priority levels.
   b. Each monitoring workstation shall be individually configurable to display alarm events in chronological order by date/time or display events in order of alarm priority value.
   c. Each monitoring workstation shall be individually configurable to include (display) some or all alarm events by assigning a minimum and maximum range of priorities (value range), so that the events from an acknowledgeable alarm will only display if falls within that workstation’s assigned range.
3. Configuration of Alarm Event behavior: The system shall allow alarm events to be configured as follows:
   a. Displaying Alarm Events:
      1) Shall be able to display/or not display alarm events from each individual alarm input, device, or other configurable cause.
      2) Shall be able to display an alarm event for invalid access attempts, door forced and door open to long events.
      3) Shall be able to display incoming alarm events in order of highest importance based on an assigned priority value.

4) Shall be able to include or excluded incoming alarm events from displaying at specified workstations based on user-definable priority range and assigned priority levels.
5) Shall be able to configure the size of the event buffer of the display window.
6) Shall be able to display alarm events for panel-level alarms at the ACP.
7) Able to persist alarm events that are acknowledged but not restored.

b. Audio-Visual feedback for incoming and pending Alarm Events:
1) The system shall display the incoming/pending alarm events in a different color than acknowledged alarm events; and will allow the system owner/administrator to change the system default colors of text and background.
2) Shall be able to associate an audio wave file with an alarm event.
3) Shall be able to repeat the alarm audio sound at a configurable interval.
4) Shall be able to prevent the software application from being closed when and active alarm event is unresolved and is pending/unacknowledged.

c. Operator Response, Acknowledging, and Clearing Alarm Events:
1) Shall be able to require an operator to acknowledge an alarm event.
2) Shall be able to prevent operator from acknowledging an alarm event if the cause of the event has not been reset (restored).
3) Shall be able to enforce an operator response above a specified priority level.
4) Shall be able to require a text message to be entered when operator acknowledges an alarm event.
5) Shall be able to define the minimum text length (number of characters) of an operator response.
6) Shall be able to allow, or disallow, operator to acknowledge all pending alarm events with a single command (configurable).
7) Shall be able to allow, or disallow, operator to delete alarm events with a command (configurable).
8) Shall be able to allow, or disallow, operator to acknowledge alarm events with a double-click mouse function (configurable).

d. Operator Instructions for Alarm Events:
1) Shall be able to display a predefined text message when an incoming alarm event activates; (up to 255-character message length).

e. Automated features for Alarm Events:
1) Software shall be able to prevent application shutdown when pending alarm events are unacknowledged (configurable with operator confirmation).
2) Software shall be able to ‘pop’ the Alarm Event screen to the forefront of the GUI focus when an incoming alarm event is logged.
3) Shall be able to automatically open a Graphical Display (floor plan) on the Monitoring Station when an associated alarm event activates and is within the workstation priority range, if applied.
4) Software shall be able to automatically call up the live digital video feed from the camera that is associated with the cause of the alarm activation.
5) Software shall be able to automatically treat credentials that are ‘non in system’ as an alarm event/invalid attempt.
6) Software shall be able to automatically delete alarm events that are both acknowledged and restored.

f. Incoming Alarm Event Instructions: The system shall allow the owner/administrator to preconfigure text instructions (up to 255 Characters) that shall be displayed to the system operator when responding to an incoming event activation.

4. Operator Command List (Action List): The system shall allow an event (input, valid access, etc.) or trigger to be configured to cause other system actions to occur. These system actions shall include:

   a. Lock/Unlock door(s) and/or door group(s).

   b. Momentary unlock of door(s) and/or door group(s).

   c. Secure door(s) and/or door group(s).

   d. Incremental counting results.

   e. Decrementing counting results.

   f. Limit counting results.

   g. Alarm/disarm event(s) and/or I/O group(s).

   h. Alarm/disarm alarm input(s) and/or input group(s).

   i. Activate/deactivate output control relay(s) and/or output control relay group(s).

   j. Momentary activate output control relay(s) and/or output control relay group(s).

   k. Activate CCTV action.

   l. Automatic display of an associated map on a Monitoring Station.

   m. I/O Group set triggering.

   n. Activate Discovery DVR (or approved equal) action.

   o. Activate Discovery DVR (or approved equal) pop-up.

   p. Activate PC audible alert.

5. Crisis Mode: The system shall control, on an action-by-action basis, dynamic physical access, input and output changes. So that when initiating Crisis Mode on a site, the access privileges will be modified to an alternate setting (system-wide) and the inputs and outputs can react accordingly.

   a. System shall support triggering Crisis Mode through the GUI (graphical user interface).

   b. System shall support triggering Crisis Mode through an input or a mechanical switch/button.

   c. System shall provide the operator with a single-click capability (GUI) to issue and restore crisis mode. The single-click button shall always be visible and available to the system operator without having to navigate menus or open screens to see and invoke or revoke crisis mode condition/status.

   d. System shall prompt operator with a confirmation/warning message that allows operator to withdraw issuance or clearance of crisis mode commands before system-wide issuance occurs.

   e. The system shall provide the operator with the means to diagnostically confirm and display the current state of crisis mode (on vs. off) at each panel.

6. Graphical Map Display: The system shall allow a graphical map display to be linked to an event. This graphic map shall be available to the system operator when responding to an event activation. Graphical maps shall be centralized on the network on a shared location and be available for display on all operator workstations. See other sub-sections within this section for functionality of the Graphical Display

7. Automatic Graphical Map Display: The system shall allow for the automatic display of a graphic map-linked to an alarm event. This graphic map shall be available to the system operator to display when responding to the event activation. At the Monitoring Station, when an event is configured to automatically display a map, a map will pop up each time the event is activated. The map will disappear when the event is acknowledged. Graphical maps shall be centralized in the network on a shared disk and be available for display on all operator workstations. See other sub-sections within this section for associated parameters**.**

O. Graphical Display:

1. Graphical Floor Plan Map: The system shall provide a user interface Graphical Display of building floor plan maps with dynamic display of door status, device status, alarms, and cameras at all access control workstations.
2. Control Doors and Devices: The Graphical Display shall allow the system operator to control doors and devices from the dynamic icons. The dynamic icons shall support the operator's issuance of 'online commands'.
3. Start Live Surveillance Video: The Graphical Display shall support Dynamic Icons for surveillance cameras and shall support the operator's issuance of 'online commands' to request live video feed or request playback of recorded video.
4. User-definable Dynamic Icon State Image: The graphical appearance of dynamic icons shall be configurable. The system shall support the ability to assign a unique, static graphic image to every state that the dynamic icon must represent based on the type of device/door that the dynamic icon represents.
5. Drag-n-Drop Setup: The system shall be able to 'drag-n-drop' the dynamic icons for doors, cameras, and input/output devices from the Hardware Tree onto the graphical display of the floor plan map. The user shall be able to manage graphic icons including the ability to add, move, resize, reposition, and delete icons as needed

P. Floating Graphical Display:

1. Detachable or "Floating" Graphical Floor Plan Map: The software application shall support detachable or "floating" graphical displays of building floor plan maps with dynamic display of door status, device status and alarms at all access control workstations. The detachable floating graphic shall be able to be moved and repositioned on a second (dual) monitor and be in view at all times.
2. Configurable, Single-Click Commands: The dynamic icons on the Floating Graphic shall support single-click or one-click commands, which are issued from the operator by executing one mouse-click on the dynamic icon. The single-click or one-click command shall be uniquely configurable as the default single-click command for each individual device and door.
3. Control Doors and Devices: The Graphical Display shall allow the system operator to control doors and devices from the dynamic icons. The dynamic icons shall support the operator's issuance of 'online commands' from the operator command menu.
4. Start Live Surveillance Video: The Graphical Display shall support Dynamic Icons for surveillance cameras and shall support the operator's issuance of 'online commands' to display and playback live video feed.
5. Drag-n-Drop Setup: The system shall be able to 'drag-n-drop' the dynamic icons for doors, cameras, and input/output devices from the Hardware Tree onto the graphical display of the floor plan map. The user shall be able to manage graphic icons including the ability to add, move, resize, reposition, and delete icons as needed.

Q. Automated Operator Commander Scripts (macros): The system shall provide the means to issue a list or sequence of operator commands by executing a macro (i.e. set of script commands).

1. Command Script Editor: The system shall provide a Command Script Editor GUI that

allows the user to create preconfigured macros that contain a sequence of Operator Commands. The Editor shall allow the user to create uniquely named macros and shall be able to add, delete and move (reorder) desired operator commands with the macros (scripts), as well as add descriptive notes to describe the purpose or function of the macro.

2. Automatic Execution by Command Script Scheduling: The system shall be able to automatically execute Command Script Macros without operator intervention. The scheduling GUI shall allow the user to set the execution times by date (month/day/year) and time (hour:minute:seconds). The scheduling GUI shall allow the user to set the macro to run one time or on a repeat cycle with selectable cycles (every # seconds, or # hours, or # days, where '#' is configurable by the user; or by selected weekday(s).
3. Manual Command Script Execution by Ad-hoc Selection: The system shall allow the operator to manually execute one or more macros (command scripts) by selecting them ad-hoc from the system list and clicking a GUI button to initiate the execution of the preconfigured macro(s).

R. Door/Reader Configuration: The system shall support the configuring of options that affect the behavior of readers and doors. The options configured shall be stored in the ACP.

1. Door Names: Each door shall be addressed within the system by a unique, hard-coded name that represents its location within the ACP. The software shall also allow the user to create a descriptive, "user-friendly" name for easy recognition within the system.
2. Reader/Door Operation: The system shall allow a reader/door to be configured to operate using the following functions:
    a. Readers shall read cards while the door is in the open position.
    b. The door lock automatically locks upon the door contact being opened.
    c. The door lock may be configured to lock upon the door being closed.
    d. The door lock may be configured to unlock upon request to exit.
    e. Door Timers: The system shall provide separate timers for controlling and monitoring the states of the locks and door contacts for each door/access point. These timers shall be configurable in the software and stored in each ACP, as well as the system database.
        1) Unlock Duration (mm:ss): The system shall support a user-configurable amount of time that the ACP will wait before locking a door/access point after a valid access, request to exit, or pulse command has occurred. The ACP shall generate an event if this timer expires before the door is closed.
        2) Unlock Delay (mm:ss): The system shall support a user-configurable amount of time that the ACP will wait before unlocking a door/access point when a valid access occurs.
        3) Reclose Time (mm:ss): The system shall support a user-configurable amount of time that the ACP will wait (shunt contact) for a door contact to reclose after a valid access, request to exit, or pulse. The ACP shall generate an event if this timer expires before the door is closed.
        4) 2-digit PIN Specifies Reclose Time: The system shall support a user-configurable option that enables a cardholder to enter the amount of time (mm) that the ACP should use as the Reclose Time (shunt contact) after a valid access occurs. The ACP shall generate an event if the time entered expires before the door is closed.
    f. Door Schedules: The system shall allow control (lock/unlock) of the door/reader based on assignment time schedules.

1) Scheduled Auto-unlock: The system shall support assigning a user-customizable time schedule that the ACP will use to automatically lock and unlock doors/access points.
2) Require Valid Card before Scheduled Unlock (a.k.a. Snow Day rule): The system shall provide a user-configurable option that prevents an ACP from unlocking a door unless a 'Valid Access' occurs within the time period that is designated for the door to be unlocked.
3) PIN Required Schedule: The system shall support assigning a user-customizable time schedule that the ACP will require a PIN code for valid access based on user-defined time parameters.
4) Suppress Door Violation Events by Schedule: The system shall allow the system to suppress door forced and door open too long events based on user-defined time schedules. The events will be suppressed only during the scheduled time periods as configured.

g. Ingress areas shall be disarmed based on Valid Access at the door by a software mechanism without the use of an auxiliary relay.

h. Readers may be configured to disarm I/O Groups (partitions) via Valid Access.

i. Door Alarms: The system shall allow each door to be configured to cause a variety of events to occur based upon activity at that door. Alarm associations may be configured based on the following events:
1) Door Forced Open.
2) Door Open too long.
3) Invalid Access Attempt.
4) Duress.
5) Passback Violation.
6) Reader Heartbeat

j. Auxiliary Relay (R2) may be configured to react based upon events:
1) Door Forced Open
2) Door Open too long
3) Invalid Access Attempt
4) Valid unlock.
5) Duress.
6) Passback Violation.

k. Door Supervision: The system shall allow for unique configuration of door supervision resisters (series only, parallel only, and series-parallel, no resistor).

l. Reader shall be configurable as a time and attendance reader.

m. Automatic Photo Verification: The system shall allow for associating a reader with the Photo Verification Module so that the module is automatically launched when a credential is presented at an associated reader.

n. Launch Photo Verification for Passback Violation: The system shall allow automatically launching the Photo Verification Module when a passback violation occurs at an associated reader.

o. Surveillance Camera Association: The system shall allow a reader to be associated with a specific DVR and camera for displaying live video from the associated reader using the system's DVR Viewer module.

3. Output Activation: The system shall allow each reader to be configured to cause an output to activate based on activity at that door.

4. Report View: The system shall allow reports to be generated directly from the Reader Screen without having to search sub-set report menus. The system shall also allow for a right-click function to run reports from a Hardware Tree or event transaction of the door. Reports shall be available for viewing or printing.

S. Input/Alarm Configuration:

1. Input/Alarm point name: Each alarm point shall be addressed within the system by a unique, hard-coded name that represents its location within the ACP. The software shall also allow the user to create a descriptive, "user-friendly" name for easy recognition within the system.
2. Input/Alarm point configuration: The system shall accept as an alarm input: supervised alarm inputs, unsupervised alarm inputs and dedicated alarm points such as device tamper alarms and Access Control Panel AC power failure.
3. Input/Alarm arming: The system shall have the ability of monitoring input points in eight (8) trigger conditions as follows:
    1) Active: the input is active, whether or not it is armed.
    2) Alarm: the input has been activated while in an armed state.
    3) Armed: the input has been armed, either by an arming input or arming schedule.
    4) Disarmed: the input has been disarmed, either by a schedule, an event, or an operator command.
    5) Nothing: No states/conditions under which the input will trigger an output.
    6) On: the input that has been activated, but not armed.
    7) Trouble: a supervised input cannot validate the correct resistance value (due to cut or short).
    8) Trouble or Alarm: the input is set for either a trouble condition or alarm condition.
4. Report View: The system shall allow reports to be generated directly from the Input Screen without having to search sub-set report menus. The system shall also allow for a right-click function to run reports from a Hardware Tree or event transaction of the input. Reports shall be available for viewing or printing.

T. Output Control Relay:

1. Output Control Relay Name: Each output point shall be addressed within the system by a unique, hard-coded name that represents its location within the ACP. The software shall also allow the user to create a descriptive, "user-friendly" name for easy recognition within the system.
2. Activation Control: Output control relays shall be defined as maintained or momentary. Maintained output control relays shall be configured to be activated/deactivated based upon a user defined time schedule, linked to a system event or operator command. Momentary output control relays shall have a user-defined pulse time (defined in 1 second increments). It shall be possible to use the momentary output control relays for the momentary control of devices other than door locking hardware. Output control shall also have the inherent ability to utilize Boolean logic including ability to act upon logic, limiting, and counting triggers.
3. Virtual Outputs: There shall be the ability to trigger software-based outputs that can later be associated as future triggering inputs for advanced logical schemas.
4. Report View: The system shall allow reports to be generated directly from the Output Screen without having to search sub-set report menus. The system shall also allow for a right-click function to run reports from a Hardware Tree or event transaction of the input. Reports shall be available for viewing or printing.

U. Operators/Users:

1. Password: The system software shall be capable of identifying an unlimited number of system operators. Passwords shall be hidden from the Software GUI
2. Operator Name: Each operator authorized to operate any portion of the system shall be addressed within the system by a unique user defined name. The operator name will be used throughout the system to identify commands and functions that the operator has executed as part of an audit trail.
3. Operator Activity: All commands issued by a system operator while monitoring system activity including locking/unlocking doors, event acknowledgment, etc. shall be stored in the historical archive for later recall. The report command shall include the operator name, time and date the command was issued and the command issued by the operator.
4. Report View: The system shall allow reports to be generated directly from the Operator Screen without having to search sub-set report menus. Reports shall be available for viewing or printing.
5. Operator Privileges:
    a. Privilege Control: Each operator shall be assigned an operator privilege matrix. Operator privilege matrices define the individual commands within the system that the operator is authorized to execute. Privilege matrices also determine which fields the operator can see and/or edit. The privileges and filters shall be unique to each operator.
    b. Administrative/Master Privilege: When selecting the Master Operator privilege option within the system, the operator shall be given access to assign/modify the Operator privileges along with select Workstation options. Certain system programming or configuration may be reserved for operators with master privileges.
    c. Online-Actions Privilege Control: Each operator may be configured to have access to perform online (software generated) actions with Doors/Readers, Inputs, Outputs, I/O Groups, Elevators, and Card Commands to include:
        1) Unlock: Unlocks the door/reader until a subsequent command, trigger, or schedule relocks the device.
        2) Lock: Locks the door/reader until a subsequent command, trigger, valid access, or schedule unlocks the device.
        3) Pulse: Performs a momentary (pre-configured duration) unlock of the door/reader.
        4) Enable (Reader): Enables the reader after a disable command.
        5) Disable (Reader): Disables the reader (typically for service operation).
        6) Relay 2 On (Reader): Fires (Turns On) the auxiliary relay of the door/reader port.
        7) Relay 2 Off (Reader): Releases (Turns Off) the auxiliary relay of the door/reader port.
        8) Shunt (Input): Masks reporting of the input device until a subsequent command trigger or schedule unshunts the device.
        9) Unshunt (Input): Enables reporting of the input device until a subsequent command, trigger or schedule shunts the device.
        10) Service Mode (Input): Disables Input actions for service operations.
        11) Restore (Input): Enables input actions after Service Mode is selected.
        12) Arm (Input): Manually places input into an armed state until a subsequent command, trigger, valid access or schedule disarms the device.
        13) Disarm (Input): Manually places input into a disarmed state until a

subsequent command, trigger, or a schedule arms the device.

V. Credential Record Definitions:

1. User Defined Field Labels: The system shall allow a privileged user to specify field name, field type, field restrictions and whether or not a field is mandatory and/or functions as a select list.
2. Personnel Records: Personnel records shall be constructed to contain personnel data and user-defined fields. The personnel data shall consist of the following data fields:
   a. Cardholder Personnel and Data Fields:
      1) Record ID number (system-defined, Primary Key)
      2) Common ID (user-determined identification code)
      3) Cardholder Name (credential-holder name)
      4) Cardholder Inactive option (deactivates all credentials of cardholder)
      5) Cardholder Trace option (traces all credentials of cardholder)
      6) Last Access (door/reader name, date, time)
      7) Date/time Cardholder record was added to database
      8) Date/time Cardholder record was last modified
      9) Assign Department at Cardholder level.
      10) Assign Customer at cardholder level.
      11) Phone and address of the cardholder.
      12) Date of Birth of cardholder.
      13) 2 user-definable date fields.
      14) 10 user-definable select lists.
      15) 50 user-defined data fields
      16) Stored photo image of the person (card/credential-holder).
      17) Store alternate photo image of the person (card/credential-holder).
      18) Stored signature of the person (card/credential-holder).
      19) Assign Otis Elevator criteria (Split Group, VIP, Vertigo, Physical Disability)
   b. Card/Credential Data:
      1) Card Technology Type (multiple card types supported)
      2) Card number (store the encoded card ID number)
      3) Personal Identification Number (PIN code)
      4) Facility number / Facility Code (with Wiegand format)
      5) Card Role (Access Control, Alarm Control)
      6) PIN Exempt option
      7) Passback Exempt option
      8) Multiple Card Credentials per Cardholder
      9) Multiple Biometric Credentials per Cardholder
      10) Store biometric fingerprint identification of the person (cardholder)
      11) Biometric data capture and encode: encoding biometric finger data on contactless smart cards (HID® iCLASS®, MIFARE®); storing biometric finger data, comparing biometric finger data,
      12) BioPIN data and encode: assigning and encoding biometric finger data on contactless smart cards (HID® iCLASS®, MIFARE®); storing biometric finger data, comparing biometric finger data
      13) Capture and encode card code on contactless smart cards (HID® iCLASS®, MIFARE®);

14) Card Disabled (Credential Disabled)
15) Credential Activation by Date.
16) Credential Automatic Expiration by Date & Time,
17) Credential Automatic Expiration by Date only
18) Credential Automatic Expiration by “number of uses”
19) Assign Access Privileges: Loop/Cluster Access Profiles, Access Groups, Personal Doors,
20) Assign Credential to Card Tour/Hall Pass
21) Configure Access Override and Server Exception rules.
22) Forward Cardholder data to Time and Attendance system

c. Cardholder Identification & Badge Printing:
1) Assign ID Badge Design to the cardholder
2) Assign Dossier Design to the cardholder
3) Print and Preview Badge and Dossier with photograph
4) ‘Date last printed’ for Identification Badge and Dossier
5) Print Limit and Print Count for Identification Badge and Dossier

d. Operator Notes: system allows operator to create/store chronological notes in the cardholder’s record (date/time stamped)

3. Mandatory Data Fields: The software shall provide a means whereby the user may configure fields in the personnel record as being mandatory. Personnel performing data entry on a cardholder record will be required by the system to enter information in all fields marked by the system as mandatory.
4. Select List Fields (droplists): The software shall provide a means whereby the user may configure certain data fields in the personnel record as ‘select list’ fields. The user shall be able to define the selectable values to be available in the select lists. The operator, when performing data entry, shall be able to choose one of the values defined (available) in the select list for the record being modified.
5. Database Query Capabilities: The system shall provide a cardholder selection list, allowing the operator to choose individual cardholder records from the selection list. The selection list shall provide a quick sorting display of all cardholder records and advanced SQL query tools including an SQL query builder.
6. Report View: The system shall allow reports to be generated directly from the cardholder screen without having to search sub-set report menus. The system shall also allow for a right-click function (context menu/shortcut menu) to run reports from the event transaction of a cardholder.

W. Automated Personnel Data Import:

1. Overview: The system shall provide a means to import personnel information from a Galaxy provided Application Programming Interface (API), a Database Stored Procedure, or an external ODBC data source. Additionally, the import shall execute in the background periodically. The import procedure shall also perform the necessary validity checking.
2. Bulk/Batch Import/Export: The system software shall provide means for bulk importing and bulk editing of card records through the use of a data file generated from another source. The external source file shall be ODBC compliant. The system shall also provide the means to generate/export the same format file of existing card records, allowing the information in the system to be exported to other computers and applications. The system shall allow the user to select the records that shall be included in the export file.
3. Active Directory Integration (LDAP protocol): The system shall support use of domain

user management tools to manage the cardholder accounts. Options shall include the ability to add and remove users from the cardholder database through group membership administration via a Windows domain, and a single sign-on feature that passes SG user log on credentials to the SG software. Shall allow control of user passwords and configuration of permissions– user-definable, automatic import (pull) by AD Group of personnel data (text fields) and images (person photographs) and assign access privileges.

X. Reports:

1. Data Storage: All programmed and transactional history is automatically stored to the database for later recall. Information written to the database shall be immediately available for report generation.
2. System Function: The system software shall be able to generate reports without affecting the real-time operation of the system.
3. Media: Reports shall be generated from the database and generated to the operator's screen, hard disk, floppy disk or printer(s).
4. Search Criteria: The database shall be structured such that the operator shall determine the search parameters based on variables available on the individual report matrix. Systems requiring the user to type complicated search strings are not acceptable.
5. Report Types: Programmed data reports shall be available for Database Configuration and Historical Activity.
6. Database Configuration Reports: The system shall be capable of producing reports of database configuration information. These database configuration reports shall include hardware and software configuration, group, time zone, activity and audit log reports.
7. Report Selection: Depending upon the type of report being generated by the system operator, the system shall provide a listing of previously defined reports. The operator shall be able to pick an existing report, modify an existing report or generate a new report.
8. System-Defined Reports: The system shall contain pre-defined reports that shall report the database configuration for area, holiday, time specifications, time zones, elevator, event, all groups, control outputs and authorized cardholders.

Y. User Status "Who's-In" Report: The "Who's-In" report shall provide a listing of all personnel that the system has determined to be in a user-specified area. The "Who's-In" report can be used in emergency evacuation situations, to determine if personnel are in the building, and where they are in the building. The "Who's-In" report can be initiated by an event or run as a report by a system operator that can be automatically refreshed on the screen to keep current as personnel exit the area.

Z. Audit Trail: The system shall provide an audit trail function that records permanent changes in data configured by system operators. The audit trail shall record permanent changes made to the configuration database by manual operator data entry. Data Audit Trail reporting shall provide the chronological actions (date/time) of all operators by name for the following: additions, modifications, deletions performed for programming and configuration of software features, hardware and hardware functions, programming related to access privileges, rules, schedules, and programming of cardholders and their credentials. Audit Trail Reporting also covers the operator accounts themselves – i.e. creation and changes to their accounts, permissions and filters. Audit Reports are available for printing or online viewing.

AA. Help Screens - On line help: The system software shall have online help available at any point requiring operator input. The help screen shall be accessible from a pull-down menu. This help screen shall contain information that shall allow the operator to enter correct data.

BB. System-wide and workstation-specific settings: The system software shall provide the ability to

control (enable and disable) select settings on a system-wide and workstation-specific basis.

CC. System Redundancy/Double-Take:

1. Overview: The system shall support redundant server with automated failover for disaster recovery using the Double-Take software to create a hot-redundant copy of the system database including all data, system programming, and system activity.

DD. Activity (Event) Monitoring:

1. General Display Features: The activity monitoring screen shall include the event, date/ time display, user, active events, events require acknowledgement and loop/site information.
2. Event Audible Annunciation: Event audible annunciation refers to the beeping behavior of the operator workstation when there is at least one active and unacknowledged event. The operator workstation shall beep continuously as long as there is at least one active and unacknowledged event. The beeping shall continue until the operator acknowledges all such events or uses the "Silence" button to silence all audible for all such events.
3. Pop-Up Events:
    a. When an event needing acknowledgment becomes active, the alarm monitoring screen shall be displayed on all operator workstations currently logged in designated to receive such a priority alarm.
    b. If the System Galaxy program has been minimized on the Windows taskbar or as an icon, the alarm monitoring window shall pop open and be displayed on the operator workstation as the front-most window.
    c. If the monitoring window is behind other tabs/windows, the alarm monitoring window shall be pop forward and displayed on the operator workstation as the front-most tab.
4. Scrolling Display: The system shall contain a scrolling display of system activity.
    a. The system shall provide a vertical and horizontal scroll bar to allow the system operator to move up/down among the event messages on the screen.
    b. The system operator shall be able to scroll back through the previous 1000 transactions of system activity
    c. Length of event log buffer shall be configurable per workstation.
5. Display Types: The system shall provide an activity (event) monitoring screen which shall operate in multiple modes. The first mode shall allow the system operator to view all system activity (including scheduled actions, card accesses events, etc.) in chronological order. The second mode shall display only those system events, which require operator action. The system shall allow the operator to view events in order based upon alarm priority or time of activation. A third mode shall allow for a split screen (on one or multiple monitors) providing the ability to display both General Events and the Alarm Events.
6. Event Instructions: The operator shall also have the ability to view additional details of the event through the use of a single keystroke. By clicking on the event item with the mouse, the operator shall be presented with alarm response instructions that have been programmed into the system.
7. Message Color: The system shall allow the operator to select the color that shall be used in displaying event messages on the operator workstation. The operator shall be able to choose from any of fourteen (14) colors. The event message color shall be based upon event message type and event priority.

EE. Graphics:

1. File Format for Graphic Map/Floor Plan: The system software shall allow the importation of existing drawings and shall support .bmp, .jpg, .dxf, .dib, .rle, .pcx, and .dcx formats for graphic maps/floor plans.
2. File Format for Graphic Symbols/Device Icons: The system software shall allow the importation of graphic icons in .bmp format.
3. Configuration: The system software shall allow the graphic symbols to be mapped or associated to every state that each hardware/field device can report, and will allow, the device icons to act as a dynamic icon when being monitored on the graphic map/floor plan. The system software shall allow each device icon to be placed on the graphic map/floor plan through the use of a mouse (drag-&-drop). The system shall allow each device icon to be moved and resized as necessary. The graphic icons placed on the floor plan shall include alarm inputs, output control points, doors, cameras, motion detectors, alarms, and other graphic symbols that represent field devices and their states. On a floating graphic floor plan, the system shall allow each device icon to be preconfigured to issue a specified operator command with a single mouse-click when selected.
4. Operation: Upon activation of an event, the operator shall, by the use of a single keystroke, be able to view the associated graphic/floor plan on the workstation monitor. The dynamic icons shall display the graphic symbol that is mapped in the system for the current state of each field device represented. The operator shall use the mouse to click on any of the icons on the graphic and issue a command that is associated with the field device.
5. Storage: The graphics feature shall take advantage of the Client/Server system configuration, with all graphics being created/stored on a shared drive/location on the system's network. These graphics shall be available to all authorized monitoring workstations.

FF. Field-upgradable Flash ROM for Access Control Panels: the Security Management System shall utilize a field-upgradable Flash ROM for storing the ACP's operating program. The Flash ROM operating program shall be field-upgradable directly from the Security Management System. The system shall not require a technician to physically change a ROM chip in the ACP in order to change a panel's operating system. The system shall not require special hardware or hand-held device to load the panel.

1. Loading the Flash Program from the Security Management System:
    a. The Security Management System shall provide the system user with the ability to display the version/revision level of the flash operating program that is currently loaded and running in each access control panel (ACP).
    b. The Security Management System shall provide controls to allow a privileged system operator to issue a command to load the Flash program to each/all ACPs. The privileged operator shall be able to select which ACPs shall receive the flash load. The operator shall also be able to choose the version/revision level of the Flash program that the ACPs shall receive.
    c. If an ACP is not communicating with the Security Management System, the loading of the Flash program shall be delayed until communications are restored, or until a system operator cancels the load request.
2. Access Control Panel (ACP) Operation:
    a. The access control panel shall continue to operate as normal while the Flash operating program is being loaded from the Security Management System.
    b. The Flash program being loaded shall be stored in temporary memory of the ACP until the entire operating program is received. When the ACP receives the entire Flash program, the system shall provide the operator the option of when begin running the new Flash program. The ACP shall delete the previous version

of the Flash program when the ACP begins running the new operating program.

GG. Access Control Panel Design: The access control panel shall be an intelligent ACP with a modular design that is capable of supporting any combination of field devices within one panel.

1. ACP Communications: Each ACP is responsible for initiating the connection and communications to the Main Communication Server using the Security Management System's software services.

   a. Security Management System's Software Services: The software services are a set of common functions and applications that shall handle system events and bidirectional communications between the ACPs and the system (database, system software, monitoring workstation, credential enrollment station, and other hardware). The Security Management System shall also handle events and communications between other ACPs.

2. Access Control Panel Design:

   a. Network Communication: The 635 Series ACP shall support 10/100 auto-negotiating Ethernet Communication. The interface to the Ethernet services shall be through a standard RJ-45 connector.

   b. ACP Inputs/Outputs: The ACP shall provide three (3) on-board inputs. The inputs are reserved for reporting tamper, AC power fail, and low battery conditions.

   c. Serviceable Hot-Swap Modules: The ACP shall allow for "Hot-Swap" serviceability. This allows for modular boards (DRM, DIO, DSI, AMM, ORM/ERM, etc.) to be changed without an ACP power-down.

   d. Diagnostic LEDs: There shall be diagnostic LEDs indicating the receiving and transmitting data for the on-board communications.

   e. ACP Reader Sections: There shall be multiple on-board communication sections per ACP that support external readers. The number of readers supported varies according to the ACP configuration.

   f. Intelligent ACP Design: the ACPs shall be able to determine the validity, authorization privileges, and schedules associated with each credential presented. The ACP shall be able to validate credentials without having to connect or communicate with the Security Management System in order to accurately grant or deny access. The ACP shall be capable of storing in resident memory all access credentials and their privileges, all door and other hardware configuration, and all associated schedules, I/O groups, timers, delays, and any related hardware linking and configured behavior. Each ACP shall have the capacity to store 10,000 system events at the panel until reconnection with the system communication server is established; including the activation of reader/door events, inputs/outputs, ACP inputs, scheduled events, etc.

   g. Embedded Diagnostic Web Tools (DWT): Each ACP shall have an embedded web tool that allows for identification of boards, display and configuration of panel options, and diagnostics of the ACP's hardware operations.

      a) Availability: The authorized technician shall be able to access (open and view) the ACP's embedded web pages.

      b) Identification of Boards/Interfaces: The Diagnostic Web Tools shall support identification of hardware modules within the ACP; including board type, board address, position, and currently running flash firmware version. The DWT shall also report the current status of each attached module (i.e. normal operation, updating flash, etc.)

      c) Configuration: The DWT shall allow configuration of special options and other parameters available in the ACP panel.

d) Diagnostics: The Embedded Web Tool shall provide an automated means exercise and prove the operation of the hardware components on each daughter board in the ACP (i.e. states and conditions of locks, relays, inputs, outputs, etc.). In this way the ACP can be field-tested for proof of operation and as a diagnostic troubleshooting of the ACP, system, and hardware peripherals.

h. ACP Boards & Interface Modules:

1) CPU Board (Central Processing Unit):

a) Purposes: The CPU Board shall provide the intelligent access control and bidirectional communication with the Security Management System. The CPU shall store all configuration for doors, readers, timers, delays, door locks, door contacts, REXs, relays, user credentials, access privileges, schedules, holidays, inputs, output relays, door groups, floor groups, i/o groups, and any related options and linking between field devices.

b) ACP Network Addressing: Each Central Processing Unit (CPU) shall be capable obtaining an IP address through DHCP server of maintaining a static IP Address if DHCP is not used.

c) Special Features and panel options: Enabling/disabling of special features and extended options shall be supported at the CPU and shall be accessible through the Embedded Diagnostic Web Tool.

d) Configuration and Diagnostics: The CPU shall provide an embedded web page for online configuration, diagnostics, and operational testing using the network connection. A direct-connect serial port shall be provided to support field configuration and diagnostics as an alternative.

2) Dual Reader Module (DRM):

a) Purposes: The DRM Board shall provide bidirectional communication with readers, monitoring and control of door hardware such as locks, contacts, RTE/REXs for the purpose of controlling and monitoring access and egress in a building, facility, or designated area.

b) Connections for Standard Reader & Hardware: Each DRM shall support two (2) Reader Sections per board. Each reader section shall support an access control reader and the accompanying door hardware (door contact, REX, Lock Relay-1, and alternate Relay-2).

c) Door Supervision: Each DRM shall provide two (2) on-board, socketed resisters for door supervision (one for each section) that can be changed for a different resister values as allowed.

d) Relays: Each DRM board shall provide four (4) Form-C SPDT relays per board. Each reader section on the DRM shall operate Relay-1 for the door lock control and Relay-2 for an alternate output purpose as required.

e) RS-485 Communication: A DRM board shall provide one (1) RS-485 communication port allowing the DRM to be remotely deployed from the RS-485 Section of a Dual Serial Interface (DSI) Board.

3) Digital I/O Board (inputs/outputs):

a) Purposes: The DIO Board shall provide supervised monitoring and control of inputs, and shall provide control and monitoring of outputs.

b) Inputs: Each Digital I/O Board (DIO) shall provide eight (8) fully

supervised, on-board inputs. These inputs shall provide four-state supervision with user-selectable resistor values for Normally Open, Normally Closed, Trouble Open, and Trouble Short.

c) Outputs: Each Digital I/O board shall provide four (4) Form-C SPDT Relays for output control. Each output terminal connection shall have contacts for Normally Open (NO) or Normally Closed (NC) states.

4) Dual Serial Interface Board (DSI):

a) Purposes: The DSI Board shall provide monitoring and control of multiple devices the serial communication channel.

b) Connections: Each Dual Serial Interface Board (DSI) shall provide two (2) RS-485 Sections on the board. Each RS-485 Section shall provide A/B contacts and ground (GND) for RS-485 communication.

c) Output Power: Each RS-485 Section of the DSI Board shall provide a configurable +12/+24 VDC output power.

d) Termination: The DSI Board optional on-board termination (120Ω) for each RS-485 Section.

5) 635-Series Alarm Monitoring Module (AMM):

a) Purposes: The AMM Board shall provide supervised monitoring and control of inputs.

b) Communication: Each AMM shall communicate on an RS-485 Channel (section) of a Dual Serial Interface (DSI) Board.

c) Each AMM shall provide sixteen (16) fully supervised contacts for connecting field inputs. Each input shall provide four-state supervision with user-selectable resistor values for Normally Open, Normally Closed, Trouble Open, and Trouble Short.

d) LED Indicators: Each AMM shall provide sixteen (16) discrete LEDs (one for each input position), with each LED indicating the state of the contact – i.e. Normally Open or Normally Closed.

e) Voltage & Tamper Inputs: Each AMM Module shall provide an on-board tamper input and on-board voltage input that detects safe, high, and low voltage conditions.

6) 635-Series ORM/ERM (Output Relay Module / Elevator Relay Module):

a) Purposes: The ORM/ERM Board shall provide control and monitoring for general-purpose output (GPO) or traditional elevator output control.

b) Communication: Each ORM/ERM shall communicate on an RS-485 Channel (section) of a Dual Serial Interface (DSI) Board.

c) Output Relays: Each ORM/ERM board shall provide eight (8) Form-A SPST Output Relays. Each ORM/ERM board shall support eight (8) general-purpose outputs (ORM) or shall support eight (8) traditional elevator relays (ERM) representing 8 floors.

d) LED Indicators: Each ORM/ERM shall provide eight (8) discrete LEDs with each LED indicating the state of the relay – i.e. On/Engaged or Off/Disengaged.

HH. The ACP Finder & Web Configuration Tool:

1. Availability: The Web Configuration Tool shall reside on a networked PC and provide the ability to view the networked ACPs from a standard web browser, such as Internet Explorer.

2. ACP Finder: The Web Configuration Tool shall be capable of detecting a networked access control panel (ACP) by MAC address.
3. Addressing and Configuring the ACP: The Web Configuration Tool shall provide the ability configure the IP addressing for each ACP, as well as configure whether a panel uses DHCP or static IP Addressing.
4. Configuring ACP Options: The Web Configuration Tool shall provide the ability to configure a descriptive, logical name for each ACP, which can further distinguish the panel's location and purpose from other ACPs on the same network.

II. 635 Series Access Control Panel (ACP) Software Features and Settings:

1. Access Control Operation:

a. Door Access Control: The ACP shall handle the door control based upon configurations stored locally at the panel (door/reader, configurations, authorized credentials, privileges, schedules, etc.). The door configuration defines the behavior of a door and includes the following parameters:

1) Monitor & Control the Lock Relay (Relay 1): The ACP shall monitor and control the state of the door lock relay (lock/unlock). If a door contact is open when the lock is in the locked state, the ACP will generate a Door Forced Open alarm event.
2) Door Lock Timers: The ACP shall store and maintain the timers for Unlock Duration and Unlock Delay. The ACP shall unlock the door immediately when a valid access, REX, or pulse command occurs. If the door contact is still open when the timer expires, the ACP will generate an alarm event. If an Unlock delay is configured, the ACP will wait to unlock the door when a valid access occurs.
3) Monitored Door Contact: The ACP shall monitor changes is the state of the door contact (door opened or closed). If the door contact input becomes active while contact is not shunted, the ACP will generate a Door Forced Open alarm event.
4) Door Shunt Times: The ACP shall store and maintain the shunt times (Reclose Within, and PIN-specified Reclose timers) that determine how long a door contact should be shunted after a valid access. If the door contact remains open after a shunt time expires, the ACP shall generate an alarm event.
5) Request to Exit (REX) Input: The REX device Input shall be placed on the protected side of the door.
6) Door Control: The ACP shall allow door control from a Security Management System. The door mode may be set to lock, unlocked, momentarily unlocked, or access disabled modes. A momentary unlock request will start a valid access cycle process on the door.
7) Door Status Reporting: The ACP shall report door events and alarm status changes including *door open too long* and *door forced open*.
8) Door Event Configuration: The ACP shall allow the configuration of Events that are activated by certain door events. The supported events shall include:

a) Door held open causes an Event.
b) Door forced causes an Event.
c) All valid access causes an Event.
d) All invalid access attempt causes an Event.
e) Duress causes an Event.
f) Passback violation causes an Event.

g) Reader Heartbeat causes and Event.

2. Door Groups: The ACP shall allow the configuration of door groups by the Security Management System. Door groups may then be used in emergencies, or to group doors for common control.
3. Reader Configuration: The access control panel (ACP) shall allow reader configuration from the Security Management System software. The reader configuration defines the behavior specific to a reader on a door and includes the following parameters:
    a. Default PIN Mode - If a card reader includes a keypad, it may be configured to require the cardholder to enter a Personal Identification Number (PIN), in addition to presenting a card, to gain access at a door. A Time Specification may be entered to control this mode on a time basis.
    b. Card Only Mode – a valid access card shall be granted access to the door/access point. An invalid or unknown card shall be denied access to the door/access point. The ACP shall generate the valid access, invalid access attempt or unknown card events as appropriate.
    c. PIN Only Mode – a valid access PIN code shall be granted access to the door/access point. An invalid PIN shall be denied access to the door/access point. The ACP shall generate the valid access or invalid access attempt events as appropriate.
    d. Card plus PIN Entry through Combo Keypad Reader - If card reader includes a keypad, a valid card with valid PIN shall be granted access to the door/entry point. An invalid or unknown card and/or an invalid PIN shall be denied access to the door/entry point. The ACP shall report the valid access, invalid access attempt or unknown card as appropriate.
    e. Biometric Modes: a valid biometric credential shall be granted access to the door/access point. An invalid or unknown credential shall be denied access to the door/access point. The ACP shall generate either a valid access, invalid access attempt, or unknown card event, as appropriate. The following modes/factors are supported:
        1) Single-factor (1:1) and Multifactor (1:n)
        2) Finger Only mode
        3) Card Only mode
        4) Card + PIN mode
        5) Card + PIN + Finger (or BioPIN) mode
        6) Card + Finger (or BioPIN) mode
4. Input Monitoring and Control: The access control panel (ACP) shall allow the configuration and control of inputs, whether they are connected to AMM modules, or to DIO boards and any logical input that may be maintained by the ACP.
    a. Input Control: The ACP shall allow the control of inputs including arming/disarming the input.
    b. Input Status Reporting: The ACP shall allow the retrieving of the current status of inputs and shall log changes in input status.
    c. Input Event Configuration: The ACP shall allow the configuration of input Events. These Events will include:
        1) Activation during a specified time specification causes Event.
        2) Activation outside a specified time specification causes Event.
        3) Supervision error causes Event.
        4) Tamper on AMM input board Event.

5. I/O Groups: The access control panel (ACP) shall allow the configuration of input/output groups which may be used to control input and outputs. I/O Groups may be referenced by Events.
6. Output Monitoring and Control: The access control panel (ACP) shall allow the configuration and control of outputs connected to the ACP.
    a. Output Definition: The ACP shall allow the configuration of outputs. Output configuration controls the behavior of the Output and includes Enabled/Disabled and reversed outputs.
    b. Output Control: The ACP shall allow the control of outputs, including setting the current state to activated, deactivated, or momentarily activated.
    c. Output Groups: The ACP shall allow the configuration of output groups.

2.3 DIGITAL SURVEILLANCE SYSTEM

A. General Description: The surveillance system server and software capabilities shall consist of the following components and facilitate camera connection, administer the control program, create sequential and multiplexed camera displays, store recorded video, provide for computer assisted search and playback, and facilitate for authorized connection from remote computers.
    1. System: Discovery Series Video Solution as manufactured by Galaxy Control Systems.

B. Installation of the system shall include battery backup and power conditioning for server and cameras with auto-recovery upon restoration of main power.

---------- Beginning of Hybrid DVR Section – Delete if using NVR – SEE NEXT SECTION----------

C. Operating Specifications for the HYBRID Digital Recorder DVR – the specifications in this paragraph and subparagraphs apply to the Hybrid DVR.
    1. Environmental Conditions: the Hybrid Digital Recorder shall be designed to operate under the following environmental specifications:
        a. Operating Temperature: 40°F to 104°F (5°C to 40°C) non-condensing.
        b. Emissions: FCC: Part 15, Subpart B
        c. Safety: IEC 60950-1 2nd Edition & EN 60950-1:2006+A11:2009
    2. Power Requirements: Components shall have the following electrical specifications:
        a. Power Requirement: 115 – 230 VAC
        b. Output over voltage protection
        c. The Hybrid Digital Recorder Power Supply shall be approved by IEC 60950-1 2nd Edition & EN60950-1:2006 +A11:2009 (CB Report)
    3. Product Label Requirements:
        a. The digital recorder shall have the UL and CE Certifications all clearly labeled on the outside of the box.
    4. Dimensions (H x W x D): 7.1” x 17.3” x 21.25” (181 mm x 441 mm x 549 mm)
    5. Weight: 64 lb. (29 kg)

D. HYBRID Digital Recorder DVR - Operational Requirements: the requirements under this paragraph and subparagraphs apply to the Hybrid DVR. The digital video recorder shall include, as a minimum, the following features/functions/specifications. The digital video recorder shall:
    1. Be fully assembled in the U.S.A.

2. Include a minimum Intel Dual Core i3 processor with the ability to expand to an Intel Quad Core i7 processor performance upgrade.
3. Include 4 Gigabytes of system memory with the ability to expand to 8 Gigabytes of system memory.
4. Include two onboard 10/100/1000 Network Interface connection offering stability, security, and allow the user to easily modify the system network settings.
5. Be optimized and support the Windows 7 Embedded Operating System.
6. Provide full Hybrid operation capabilities allowing recording of both high-resolution analog and IP video, selectable by user, on all video channels.
7. Include up to 32 hybrid channels standard.
8. Support analog or Megapixel IP cameras.
9. Support the recording of audio streams from all IP devices (cameras and encoders).
10. Provide remote capabilities including remote for Windows, remote for Macintosh, multi-site management software and mobile applications for Apple and Android devices.
11. Include the ability to unlock additional IP camera licenses offering up to a combined total of 64 IP and analog cameras per DVR with a maximum recording throughput of 400Mbps in a RAID 5 configuration and 200Mbps in a single drive configuration.
12. Include support for the ONVIF 1.01 and 1.02 core specifications. Full list of ONVIF compliant and tested devices: www.galaxysys.com
13. Support a majority of IP cameras from major manufacturers including:
    a. OpenEye
    b. ACTi
    c. Arecont
    d. Axis
    e. IQ Invision
    f. Panasonic
    g. Toshiba
    h. Samsung
    i. Sanyo
    j. Sony
    k. VIVOTEK
    l. Full list of IP compatible devices: www.galaxysys.com
14. Provide a Live Digital Zoom function for IP cameras that allows the operator to zoom in and out of a live picture.
15. Support static IP and DHCP IP addressing through configurable TCP/IP settings.
16. Include DDNS (Dynamic Domain Name System) for free for the life of the product. DDNS shall allow the operator to use a URL address instead of a static IP address.
17. Provide 16 or 32 video camera inputs, depending on model, at a minimum system wide recording rate of 480 images per second (IPS). The system shall have an equivalent number of looping video outputs to the number of video inputs available. The 32-channel model shall include BNC Dongles used for looping outputs. Looping outputs shall also have 75-Ohm termination available.
18. Record at a rate of up to 480 images per second, with real-time live viewing of 30 IPS per camera for analog cameras and shall support NTSC- or PAL-formatted video.

19. Be capable of recording up to 30 IPS on a single channel in an environment where all channels are being utilized. The operator shall have the ability to assign each channel a specific recording rate varying from 1 to 30 IPS. The Digital Recorder shall support the following recording resolution and frame rate configurations:

Resolution	CCTV	480 IPS Model
360x240	1CIF	480 IPS
720x240	2CIF	240 IPS
720x480	4CIF	120 IPS

20. Be able to assign each channel a different recording resolution ranging from 360x240 to 720x480.
21. Offer a Multi-Codec option that allows the operator to select M-JPEG, MPEG4, or H.264 as the compression format for recording video. The compression method may further be specified on a per camera basis allowing multiple compression formats to be used simultaneously.
22. Allow the user to adjust the resolution, quality, motion sensitivity, and number of images per second each camera will record. These adjustments shall be configurable per video input.
23. Offer the following on-board hard drive capacity options with four removable hard drive bays housed in an internal, fan cooled, 6.0 Gbps, power controlled hard drive enclosure that support large capacity 4 Terabyte hard drives:
    a. 2.0 Terabytes
    b. 4.0 Terabytes
    c. 6.0 Terabytes
    d. 8.0 Terabytes
    e. 12.0 Terabytes
    f. 16.0 Terabytes
24. Only use high performance Video Surveillance rated hard drives engineered for reliability and 24x7 “always on” environments.
25. Be housed in a high performance 4U metal chassis. The chassis shall be designed to fit into a 19” EIA rack. The front panel shall come with the ability to be locked by a key.
26. Provide exceptional internal cooling through two high output silent 65mm front intake fans, one high output silent 92mm side output fan and one high output silent 40mm rear back panel fan.
27. Have the ability to easily backup important video to an external media location, CD/DVD disk, or a USB Drive. The recorder must not stop recording during the backup process. To ensure the integrity of data, the digital recorder shall use a proprietary viewer that can detect image tampering.
28. Allow the inclusion of backup viewer software during the backup of media to allow viewing of the proprietary video from any location.
29. Include a standard DVDRW drive capable of Read/Write/Burn at the following speeds: 24x DVD±R Burn, 18x DVD±R Read, 8x DVD+RW, 6x DVD-RW, 8x DVD±R9, 12x DVD-RAM, 48x32x CD-R/RW to which the operator may backup video in its proprietary format or in AVI format.
30. Have the ability to span backed up recorded video over multiple DVDs.

31. Include a minimum of the following front panel controls and LEDs:
    a. DVD-RW drive
    b. Hard drive activity LED
    c. Power LED
    d. One 2.0 USB ports
    e. Power switch
    f. Removable Hard drive array – up to 4 HDDs
32. Include a minimum of the following rear-panel connectors:
    a. BNC Connectors for Camera Inputs and Looping Outputs
    b. Up to 16 Sensor/Alarm Inputs
    c. Up to 16 Control Outputs
    d. Power input
    e. Two high-speed USB 3.0 inputs
    f. Two USB 2.0 inputs
    g. HDMI
    h. DVI-D
    i. VGA
    j. Display Port
    k. Two Gigabit RJ-45 Network Jacks
    l. RS-485 Interface (with RX, TX)
    m. Line in / Speaker out – RCA
    n. RCA video out
    o. Up to 16 Audio inputs
    p. Include the following components:
    q. USB Mouse
    r. USB Keyboard QWERTY
    s. DVR System Image Disc
    t. Software Accessory Disc
    u. Power Adapter
    v. PTZ Adapter cable
    w. Rack mount attachments with screws
    x. DVR front door key
    y. User Manual (Digital format)
    z. HDMI to DVI-D adapter
33. Offer the following accessory hardware components (add-ons):
    a. Factory or Field upgradable Quad Core i7 Processor. Expands system memory to 8 Gigabytes.
    b. Fully equipped internal RAID 5 configuration capable of full data redundancy and

exceptional management capabilities. There shall be a separate dedicated RAID 5 ACP Card that will provide off-loaded XOR parity calculation. RAID parity calculations shall be handled on the RAID 5 card exclusively and shall not utilize resources from the motherboard's on-board processor. The storage Drives shall be Hot Swappable when in a RAID 5 configuration. The RAID 5 configuration shall only use high performance enterprise level hard drives manufactured specifically for RAID environments. Recording throughput will be 400 Mbps maximum, with a minimum guaranteed value of 225 Mbps during RAID rebuild conditions.

c. Field storage upgrades that include internal hard drive capacities ranging from 1 terabyte to 4 terabytes.

d. 4U rack mountable iSCSI external storage option capable of RAID 5, 6, and 10 in the following storage capacities:
   1) 16.0 Terabytes
   2) 24.0 Terabytes
   3) 32.0 Terabytes
   4) 48.0 Terabytes
   5) 64.0 Terabytes

34. Solid State Drive (SSD) capable of operating as a BOOT drive in a RAID configuration or in a Single drive configuration. The SSD shall be exclusively dedicated to the Operating System. No Video will be allocated to the solid-state drive for the purposes of video storage and archiving. This Solid-State Drive shall be internal to the DVR and should not replace any of the system hard drives. Overall storage capacity shall not be decreased by adding an SSD hard drive.
35. Dual Solid-State Drives (SSDs) in a RAID 1 BOOT drive configuration. The SSD configuration shall be exclusively dedicated to the Operating System. No Video will be allocated to the solid-state drive for the purposes of video storage and archiving. This Solid-State Drive configuration shall be internal to the DVR and should not replace any of the system hard drives. Overall storage capacity shall not be decreased by adding an SSD hard drive.
36. Internal Dual Redundant Power Supply with two shared 400W power modules.
37. A Multiplexed Analog Composite output card providing four analog video outputs on the back of the unit. The outputs shall be capable of displaying in either multiplex or single channel modes. Multiplexed mode shall allow various multiplexed output configurations through channels 1 and 2. Single channel mode allows all four channels to display one channel at a time to four separate video output devices. It shall also provide up to 16 channels of video on a single display. The outputs shall be programmable to sequence through any number of cameras, and the operator shall have the ability to disable the defined sequence and manually select a camera to the output. The sequence must be easily reactivated by simply enabling the sequence again.
38. A single or dual port 10/100/1000 Gigabit Network Interface Card.
39. Serial RS-232 expansion capabilities providing up to 4 independent Serial connections for Joystick control or POS connectivity.

E. HYBRID DVR - RECORDING CAPABILITIES – The DVR recording capabilities shall provide the following characteristics/features/functions. The DVR recording capabilities shall:

1. Provide support for 360° view cameras. Digital pan, tilt and zoom shall be supported in both live and recorded video.
2. Provide an IP camera configuration setting utility that allows the user to export and import full camera settings from the Network Camera section.

3. Allow the user to upgrade the Server Software version from the System Information section from within the Server Software setup.
4. Provide an advanced Dual Stream feature allowing the user to record an HD stream while transmitting a low-resolution stream to remote/VMS clients. The Dual Stream shall support H.264, MJPEG or MPEG4 codecs.
5. Allow multiple IP video streams to be recorded from a single device while only reserving a single recording channel license.
6. Provide an iFrame Only live view feature that reduces CPU load allowing the user to enable up to 16 channels of live view IP HD recording. iFrame shall support H.264 and MPEG4 codecs.
7. Be able to run Point of Sale Software. The system shall have the capability to overlay text from POS systems directly onto the video and maintain an index of transaction data associated with the video for indexing and searching.
8. Be able to natively run optional Video Analytics software allowing intelligent video monitoring including real time notification of detected events and search capabilities selectable on a per camera basis.
9. Provide a LAN/WAN connection. Required software or hardware shall be provided for operating the digital recorder over the network free of charge. The remote operator shall also be capable of backing up still JPG images, and/or video segments to the local hard disk in AVI or proprietary file format.
10. Include a dynamic System Log to record and display information pertaining to alarm events, digital recorder reboots, and other related information, record/display hardware information pertaining to system recording successes and failures, and other related information.
11. Provide exportable system and event log files which may also be viewed and searched by date in the software interface.
12. Provide email notification to one or more recipients for video loss, motion, sensor, hard drive smart check, and system health events.
13. Provide a CPU performance meter clearly visible in the main GUI indicating the current CPU load status.
14. Include the ability to discover IP cameras from the network with an integrated camera discovery protocol and add them to your digital recorder from a single interface.
15. Include an option to enable Wide Screen support for monitors that output in 16:9 ratios. The feature shall allow the operator to switch between the standard 4:3 ratio and the widescreen 16:9 ratio.
16. Provide a software spot monitor application pre-loaded on the recorder that allows the operator to use multiple monitors to view camera channels and individually configure each monitor.
17. Provide full ONVIF ® support including camera-side VMD, Alarm and Sensor I/O, Audio, Live and Recording capabilities.
18. Have the ability to customize cameras with operator-defined names. These names must be viewable and transferable after proprietarily backing up.
19. Provide the ability to Bookmark a video clip during search with the option to export bookmark data. Additional options shall include the ability to change the start or end time of the clip, add comments, change the title and add additional cameras.
20. Provide a Clip Backup feature allowing the backup of a single camera or multiple cameras at a time. Options include backup time frame, specific camera selection, memo inclusions, and the ability to include a copy of the proprietary Backup Viewer Software.
21. Have built-in motion detection for each camera (including all IP cameras). The operator

shall be able to independently select the cameras motion detection area with the ability to draw up to 5 different motion detection boxes within the cameras view. The operator shall be able to adjust the cameras sensitivity independently.

22. Include Advanced Motion detection capabilities and when enabled, will allow for up to 15 motion boxes to be set. A combination of rectangles, circles and complex polygon shapes can be set within the Advanced Motion detection area.
23. Have the ability to hide cameras from general users, yet still record.
24. Include Active Directory integration (LDAP protocol) which allows domain user management tools to manage the digital recorder user accounts. Options shall include the ability to add and remove users from the digital recorder through group membership administration via a Windows domain ACP, and a single sign-on feature that passes digital recorder user log on credentials to the video management and remote software. Shall allow control of user passwords and configuration of permissions.
25. Be able to restart upon unpredictable power outage while restoring operator custom configurations.
26. Include a hardware monitoring (watchdog) system which will monitor the systems hardware devices. If the system should ever lockup the hardware monitoring system shall automatically reboot the system. Therefore, allowing the system to begin recording immediately upon startup.
27. Provide for at least 100 different usernames (and passwords) to which specific privileges such as search, setup, PTZ, shutdown, and backup may be assigned. The administrator shall be capable of hiding any different combination of cameras from each of the users.
28. Have 16 sensor inputs which are capable of triggering alarm events or initiating recording. The operator shall be able to set each sensor input as normally open or normally closed. A pre-alarm recording feature shall be available to record up to 60 seconds of video prior to the sensor input being activated. A record of all sensor events shall also be provided.
29. Provide 16 dry contact alarm outputs to activate external devices.
30. Provide the necessary software for image authenticity verification of each image recorded.
31. Be capable of programming the system locally through a standard PC keyboard and mouse or remotely over a LAN/WAN via a Remote Management Software Client.
32. Provide a camera sabotage function to allow an alarm event to occur when the camera field of view experiences significant pixel change (e.g. changing the view of the camera, obscuring the lenses, significant shaking or vibration, or blinding light). When a video loss event occurs, the operator shall have the option to enable an alarm beep or a custom WAV file audible alert utilizing the internal speaker of the digital recorder, and/or activate an alarm output.
33. Be capable of notifying the local operator by sound in the event video from a camera is lost (video loss alarm).
34. Be capable of triggering an external alarm device through a control output in the event video a camera is lost (video loss alarm).
35. Be capable of triggering an external alarm device through a control output in the event power is lost (power loss alarm).
36. Have pre and post alarm/motion recording. A pre-alarm recording feature shall be available to record up to 60 seconds of video prior to motion being detected. Furthermore, a post-alarm recording feature shall be available to record up to 255 seconds of video after motion has left the motion grid.
37. Have the ability to playback recorded video on the main screen by simply clicking the

middle mouse scroll button.

38. Have the ability to automatically adjust for Daylight Savings Time changes, with no loss of video when the hour jumps forward or back.
39. Allow an operator to flag video clips distributed across multiple cameras. This feature will allow the operator to back up all clips from multiple cameras in one operation from the backup menu screen. The feature will allow the operator to add a memo to each video clip for review at a later date.
40. Provide dynamic abilities to record images including continuous, motion detection, alarms/events and according to a use defined time schedule.
41. Provide a schedule from which the operator may choose whether the system will record based upon motion detection or continuously 24 hours a day, seven days a week.
42. Accept special day preprogramming so recording schedules may be adjusted around holidays and/or special day events.
43. Allow the user to setup 32 individual schedules for motion detection, sensor recording and continuous recording.
44. Have intensive recording. This will allow the digital recorder to begin recording or boost recording speed based on sensor or motion detection.
45. Be capable of automatically adjusting its recording resolutions and recording rates upon the activation of sensor input and/or motion detection.
46. Have the ability to instant record any camera by simply double left clicking on the camera from the main screen.
47. Provide the user with the ability to export and import software settings using a system setting utility accessible on the recorder in Windows desktop mode.
48. Include an Administrator privilege level, which allows the user to create, edit, and delete user accounts. Each account can be assigned different permissions that limit the usage of the system including:
    a. Search
    b. Set up
    c. Pan/Tilt
    d. Backup
    e. Forbidden Cameras
    f. Shut down
49. The ability to enable or disable access by the Web Viewer Software, allowing a user to view live video using an Internet browser.
50. The ability to adjust the resolution setting when sending video to remote clients.
51. The ability to throttle the bandwidth of the digital recorder to ensure that images and system messages are delivered as quickly as possible within the capabilities of the network’s available bandwidth.
52. Include a User Management Console, which allows the user to create, edit, and delete user accounts. Each account can be assigned different privileges that limit the usage of the system. Privileges shall include, but not be limited to, the following functions:
    a. Search
    b. Setup
    c. Pan/Tilt
    d. Backup

e. Shutdown

f. Intensive

g. Relay Out

h. Pan/Tilt Advance

i. Hidden Cameras/Audio

j. User Ranking

k. Auto Log Off

53. Provide the user ability to obtain the software version of the digital recorder.

54. Run a series of self-tests during power up, and display messages as the various hardware and software sub-systems are activated. After power up, the digital recorder's software must automatically load and display the main screen.

55. Display the camera status for each camera next to the camera number (or name) in the video display area. The information must include:

    a. Camera number and custom name

    b. Recording status, which must show whether a camera is currently recording continuously, or whether a camera is recording based on motion.

    c. Special recording status, which must indicate whether a camera's associated sensor has been activated, and/or when the user activates the instant recording option for the selected camera.

56. Offer the following screen division sets (depending on the model):

    a. Display the first four videos (1–4) in the video display area.

    b. Display the next four videos (5–8) in the video display area.

    c. Display the next four videos (9–12) in the video display area.

    d. Display the next four videos (13–16) in the video display area.

    e. Display all sixteen (16) videos in the video display area.

57. Have the ability to adjust each video input's brightness, contrast, and hue, to optimize the clarity and detail of recorded video.

58. Incorporate motion detection, including the ability to create multiple detection regions for each video input.

59. Include the ability for post-alarm recording, which must record video for a specified time before and/or after a motion or sensor alarm has occurred. The time period must be selectable from zero (0) to ninety-nine (50) seconds.

60. For analog cameras - include the ability to record continuously with one frame rate and then record at an increased frame rate when motion is detected.

61. Include a video loss alarm function to allow an alarm event to occur when a camera loses the signal for any reason (e.g. camera power failure, cable being cut, camera damage, etc.). When a video loss event occurs, the operator shall have the option to enable an alarm output.

62. Include Alarm Monitor software to stream video across a LAN to a client PC when an alarm is detected on the unit. The operator shall have the ability to stop, play forward and backward, frame by frame or at real speed, the video that streams across. The program must constantly monitor for a signal from the digital recorder, and when an alarm signal is detected the Alarm Monitor must notify the operator of an event. The Alarm Monitor image viewer shall also allow the user to search through past events that have been recorded on the client PC.

63. Allow an Instant Recording feature that allows users to manually initiate recording on a

specific camera, overriding the current schedule.

64. Provide, through the remote software, the ability to export single images in the JPG file format and save video clips in the AVI format. A digital signature must be attached to every JPG and AVI file exported by the unit for use with the bundled Digital Verifier application. This function must be unique to the unit and its verification software; and shall not interfere with viewing files using other applications.
65. Include an internal RS-485 connection from which the operator may interface at least 75 different brands of PTZ cameras. The operator shall have the ability to control the PTZ functions while connected to the digital recorder remotely. The operator shall have the ability to control different brands of PTZ cameras which utilize different protocols with a single digital recorder.
66. Offer on screen PTZ camera control by clicking and dragging the mouse over the live video display and include play controls to play back the recorded video either forward or reverse, at multiple speeds.
67. Include the ability to search by using fast forward or rewind. Using the feature, the operator shall be able to search frame by frame using any number of cameras and have the ability to speed up or slow down the speed of playback using a slow/fast slide bar.
68. Include an index search. Using this feature the operator shall be able to search through previously recorded video based on motion detection, sensor trip or instant record.
69. Include a preview search function. Using this feature the operator shall be able to search using a 24-hour visual overview of one single camera by separating a 24-hour period into 24 images, each one representing the first second of each hour. The operator must then have the ability to drill down to the search to 10-minute increments and then 1-minute increments by simple double left clicking on a displayed image.
70. Include a panorama search function. Using this feature the operator shall be able to search one camera frame-by-frame using a 16-image grid.
71. Include an object or post motion (forensic) search. Using this feature the operator shall be able to search through previously recorded video for motion within an operator-defined field.
72. Include a status search. Using this feature the operator shall be able to see a single camera on the screen and, using a split view, view each frame sequentially side by side.
73. The ability to search recorded video on the main screen by simply clicking the middle mouse scroll button and selecting rewind and fast forward options.
74. Provide simultaneous playback viewing while recording live images and backing up recorded images in true multiplex operation.
75. Incorporate a hardware watchdog for restarting the system in the event of a system lock-up.

---------- END OF HYBRID DVR SECTION ----------

---------- BEGINNING OF NETWORKED NVR SECTION – DELETE SECTION IF NOT NEEDED ----------

F. Operating Specifications for the NETWORKED Digital Recorder NVR – the specifications in this paragraph and subparagraphs apply to the Networked NVR.

1. Environmental Conditions: the Digital Recorder shall be designed to operate under the following environmental specifications:

   a. Operating Temperature: 40°F to 104°F (5°C to 40°C) non-condensing.

2. Power Requirements: Components shall have the following electrical specifications:
    a. Power Requirement: 115 – 230 VAC
    b. Output over voltage protection
3. Product Label Requirements:
    a. The digital recorder shall have the RoHS certification all clearly labeled on the outside of the box.
4. Dimensions (H x W x D): 6.9” x 16.9” x 26” (176 mm x 430 mm x 660 mm)
5. Weight: 80 lbs. (36.3 kg)

G. NVR Networked Digital Recorder - Operational Requirements: The network video recorder shall include, as a minimum, the following features/functions/specifications. The network video recorder shall:
1. Be fully assembled in the U.S.A.
2. Include a minimum Intel Dual Core i3 processor with the ability to expand to an Intel Quad Core i7 processor performance upgrade on the 16- and 32-channel models.
3. Include an Intel Quad Core i7 processor on the 64-channel model.
4. Include 4 Gigabytes of system memory with the ability to expand to 8 Gigabytes of system memory on the 16- and 32-channel models.
5. Include 8 Gigabytes of system memory on the 64-channel model.
6. Include two onboard 10/100/1000 Network Interface connections offering stability, security, and allow the user to easily modify the system network settings.
7. Be optimized and support the Windows-7 Embedded Operating System.
8. Provide recording support for high-resolution Megapixel IP video, selectable by user, on all video channels.
9. Support the recording of up to sixteen (16) audio streams dependent on the IP device (cameras and encoders) capabilities.
10. Provide remote capabilities including remote for Windows, remote for Macintosh, multi-site management software and mobile applications for Apple and Android devices.
11. Include the ability to unlock additional IP camera licenses offering up to a combined total of 64 IP cameras per NVR with a maximum recording throughput of 400 Mbps in a RAID 5 configuration and 200 Mbps in a single drive configuration.
12. Include support for the ONVIF 1.01 and 1.02 core specifications. Full list of ONVIF compliant and tested devices: www.galaxysys.com
13. Support a majority of IP cameras from major manufacturers including:
    a. OpenEye
    b. ACTi
    c. Arecont
    d. Axis
    e. IQ Invision
    f. Panasonic
    g. Toshiba
    h. Samsung
    i. Sanyo
    j. Sony

k. VIVOTEK

l. Full list of IP compatible devices: www.galaxysys.com

14. Provide a Live Digital Zoom function for IP cameras that allows the operator to zoom in and out of a live picture.
15. Support static IP and DHCP IP addressing through configurable TCP/IP settings.
16. Include DDNS (Dynamic Domain Name System) for free for the life of the product. DDNS shall allow the operator to use a URL address instead of a static IP address.
17. Be capable of recording up to 30 IPS on a single channel in an environment where all channels are being utilized. The operator shall have the ability to assign each channel a specific recording rate varying from 1 to 30 IPS.
18. Be able to assign each channel a different recording resolution and frame rate based on the network video device capabilities.
19. Offer support for M-JPEG, MPEG4, or H.264 network video devices. Shall allow multiple compression formats to be used simultaneously.
20. Allow the user to adjust the resolution, quality, motion sensitivity, and number of images per second each camera will record. These adjustments shall be configurable based on the network video device capabilities.
21. Offer the following on-board hard drive capacity options with sixteen removable hard drive bays that include exceptional fan cooling, 3.0 Gbps and large capacity HDD (3 Terabyte drives) support:
    a. 16.0 Terabytes
    b. 24.0 Terabytes
    c. 32.0 Terabytes
    d. 48.0 Terabytes
    e. 64.0 Terabytes
22. Non-RAID configurations will only use high performance AV (Audio/Video Surveillance) rated hard drives engineered for reliability and 24x7 “always on” “non-RAID” environments.
23. RAID configurations will only use high performance enterprise RE (RAID Edition) rated hard drives engineered for reliability and 24x7 “always on” “RAID” environments.
24. Be housed in a high performance 4U metal chassis. The chassis shall be designed to fit into a 19” EIA rack. The front panel shall come with the ability to be locked by a key.
25. Include a standard Slide Rack Rail kit for server rack mount installations.
26. Provide exceptional internal cooling through five high output 80mm fans mounted in the center of the chassis, two high output 80mm fans mounted in the rear of the chassis and front/rear cooling intakes for maximum in/out cooling.
27. Have the ability to easily backup important video to an external media location, CD/DVD disk, or a USB Drive. The recorder must not stop recording during the backup process. To ensure the integrity of data, the digital recorder shall use a proprietary viewer that can detect image tampering.
28. Allow the inclusion of backup viewer software during the backup of media to allow viewing of the proprietary video from any location.
29. Include a standard DVDRW drive capable of Read/Write/Burn at the following speeds: 24x DVD±R Burn, 18x DVD±R Read, 8x DVD+RW, 6x DVD-RW, 8x DVD±R9, 12x DVD-RAM, 48x32x CD-R/RW to which the operator may backup video in its proprietary format or in AVI format.
30. Have the ability to span backed up recorded video over multiple DVDs.

31. Include a minimum of the following front panel controls and LEDs:
    a. DVD-RW drive
    b. Hard drive activity LED
    c. Power LED
    d. Two 2.0 USB ports
    e. Power switch
32. Include a minimum of the following rear-panel connectors:
    a. Power input
    b. Two high-speed USB 3.0 inputs
    c. Six USB 2.0 inputs
    d. HDMI
    e. DVI-D
    f. VGA
    g. Display Port
    h. Two 10/100/1000 RJ-45 Network Jack
    i. Line in / Speaker out – RCA
    j. Include the following components:
    k. USB Mouse
    l. USB Keyboard QWERTY
    m. NVR System Image Disc
    n. Software Accessory Disc
    o. Power Adapter
    p. Rack mount attachments with screws
    q. NVR chassis front bezel and door key
    r. User Manual (Digital format)
    s. HDMI to DVI adapter
33. Offer the following accessory hardware components (add-ons):
    a. On the 16 and 32 channels models: Factory or Field upgradable Quad Core i7 Processor. Expands system memory to 8 Gigabytes.
    b. Fully equipped internal RAID 5 configuration capable of full data redundancy and exceptional management capabilities. There shall be a separate dedicated RAID 5 ACP Card that will provide off-loaded XOR parity calculation. RAID parity calculations shall be handled on the RAID 5 card exclusively and shall not utilize resources from the motherboard's on-board processor. The RAID 5 configuration shall only use high performance enterprise level hard drives manufactured specifically for RAID environments. Recording throughput maximum will be 400Mbps with a minimum guaranteed value of 300Mbps during RAID rebuild conditions.
    c. Field storage upgrades that include internal hard drive capacities ranging from 1 terabyte to 4 terabytes.
    d. Internal iSCSI upgrade for separate external iSCSI storage option.

e. 4U rack mountable external iSCSI storage option capable of RAID 5, 6, and 10 in the following storage capacities:
   1) 16.0 Terabytes
   2) 24.0 Terabytes
   3) 32.0 Terabytes
   4) 48.0 Terabytes
   5) 64.0 Terabytes

f. Solid State Drive (SSD) capable of operating as a BOOT drive in a RAID configuration or in a Single drive configuration. The SSD shall be exclusively dedicated to the Operating System. No Video will be allocated to the solid-state drive for the purposes of video storage and archiving. This Solid-State Drive shall be internal to the NVR and should not replace any of the system hard drives. Overall storage capacity shall not be decreased by adding an SSD hard drive.

g. Dual Redundant SSD BOOT drive in a RAID 1 (Mirror) configuration.

h. A single or dual port 10/100/1000 Gigabit Network Interface Card.

i. Serial RS-232 expansion capabilities providing up to 4 independent Serial connections for Joystick control or POS connectivity.

j. Dual Redundant 820W Power Supply Unit

H. NVR RECORDING CAPABILITIES – The NVR recording capabilities shall provide the following characteristics/features/functions. The NVR recording capabilities shall:

1. Provide support for 360° view cameras. Digital pan, tilt and zoom shall be supported in both live and recorded video.
2. Provide an advanced Dual Stream feature allowing the user to record an HD stream while transmitting a low-resolution stream to remote/VMS clients. The Dual Stream shall support H.264, MJPEG or MPEG4 codecs.
3. Provide an iFrame Only live view feature that reduces CPU load allowing the user to enable up to 16 channels of live view IP HD recording. iFrame shall support H.264 and MPEG4 codecs.
4. Be able to run Point of Sale Software. The system shall have the capability to overlay text from POS systems directly onto the video and maintain an index of transaction data associated with the video for indexing and searching.
5. Be able to natively run optional Video Analytics software allowing intelligent video monitoring including real time notification of detected events and search capabilities selectable on a per camera basis.
6. Provide a LAN/WAN connection. Required software or hardware shall be provided for operating the digital recorder over the network free of charge. The remote operator shall also be capable of backing up still JPG images, and/or video segments to the local hard disk in AVI or proprietary file format.
7. Include a dynamic System Log to record and display information pertaining to alarm events, digital recorder reboots, and other related information, record/display hardware information pertaining to system recording successes and failures, and other related information.
8. Provide exportable system and event log files which may also be viewed and searched by date in the software interface.
9. Provide email notification to one or more recipients for video loss, motion, sensor, hard drive smart check, and system health events.
10. Provide a CPU performance meter clearly visible in the main GUI indicating the current

CPU load status.

11. Include the ability to discover IP cameras from the network with an integrated camera discovery protocol and add them to your digital recorder from a single interface.
12. Include an option to enable Wide Screen support for monitors that output in 16:9 ratios. The feature shall allow the operator to switch between the standard 4:3 ratio and the widescreen 16:9 ratio.
13. Have the ability to customize cameras with operator-defined names. These names must be viewable and transferable after proprietarily backing up.
14. Provide the ability to Bookmark a video clip during search with the option to export bookmark data. Additional options shall include the ability to change the start or end time of the clip, add comments, change the title and add additional cameras.
15. Provide a Clip Backup feature allowing the backup of a single camera or multiple cameras at a time. Options include backup time frame, specific camera selection, memo inclusions, and the ability to include a copy of the proprietary Backup Viewer Software.
16. Have built-in motion detection for each camera (including all IP cameras). The operator shall be able to independently select the cameras motion detection area with the ability to draw up to 5 different motion detection boxes within the cameras view. The operator shall be able to adjust the cameras sensitivity independently.
17. Include Advanced Motion detection capabilities and when enabled, will allow for up to 15 motion boxes to be set. A combination of rectangles, circles and complex polygon shapes can be set within the Advanced Motion detection area.
18. Have the ability to hide cameras from general users, yet still record.
19. Include Active Directory integration (LDAP protocol) which allows domain user management tools to manage the digital recorder user accounts. Options shall include the ability to add and remove users from the digital recorder through group membership administration via a Windows domain ACP, and a single sign-on feature that passes digital recorder user log on credentials to the video management and remote software. Shall allow control of user passwords and configuration of permissions.
20. Be able to restart upon unpredictable power outage while restoring operator custom configurations.
21. Include a hardware monitoring (watchdog) system which will monitor the systems hardware devices. If the system should ever lockup the hardware monitoring system shall automatically reboot the system. Therefore, allowing the system to begin recording immediately upon startup.
22. Provide for at least 100 different usernames (and passwords) to which specific privileges such as search, setup, PTZ, shutdown, and backup may be assigned. The administrator shall be capable of hiding any different combination of cameras from each of the users.
23. Have up to 16 sensor input capabilities, dependent on the network video device, which are capable of triggering alarm events or initiating recording. A pre-alarm recording feature shall be available to record up to 60 seconds of video prior to the sensor input being activated. A record of all sensor events shall also be provided.
24. Have up to 16 alarm output capabilities, dependent on the network video device, to activate external devices.
25. Provide the necessary software for image authenticity verification of each image recorded.
26. Be capable of programming the system locally through a standard PC keyboard and mouse or remotely over a LAN/WAN via a Remote Management Software Client.
27. Provide a camera sabotage function to allow an alarm event to occur when the camera

field of view experiences significant pixel change (e.g. changing the view of the camera, obscuring the lenses, significant shaking or vibration, or blinding light). When a video loss event occurs, the operator shall have the option to enable an alarm beep or a custom WAV file audible alert utilizing the internal speaker of the digital recorder, and/or activate an alarm output.

28. Be capable of notifying the local operator by sound in the event video from a camera is lost (video loss alarm).
29. Be capable of triggering an external alarm device through a control output in the event video a camera is lost (video loss alarm). Dependent on network video device capabilities.
30. Be capable of triggering an external alarm device through a control output in the event power is lost (power loss alarm). Dependent on network video device capabilities.
31. Have pre and post alarm/motion recording. A pre-alarm recording feature shall be available to record up to 60 seconds of video prior to motion being detected. Furthermore, a post-alarm recording feature shall be available to record up to 255 seconds of video after motion has left the motion grid.
32. Have the ability to playback recorded video on the main screen by simply clicking the middle mouse scroll button.
33. Have the ability to automatically adjust for Daylight Savings Time changes, with no loss of video when the hour jumps forward or back.
34. Allow an operator to flag video clips distributed across multiple cameras. This feature will allow the operator to back up all clips from multiple cameras in one operation from the backup menu screen. The feature will allow the operator to add a memo to each video clip for review at a later date.
35. Provide dynamic abilities to record images including continuous, motion detection, alarms/events and according to a use defined time schedule.
36. Provide a schedule from which the operator may choose whether the system will record based upon motion detection or continuously 24 hours a day, seven days a week.
37. Accept special day preprogramming so recording schedules may be adjusted around holidays and/or special day events.
38. Have intensive recording. This will allow the digital recorder to begin recording or boost recording speed based on sensor or motion detection.
39. Be capable of automatically adjusting its recording resolutions and recording rates upon the activation of sensor input and/or motion detection.
40. Have the ability to instant record any camera by simply double left clicking on the camera from the main screen.
41. Include an Administrator privilege level, which allows the user to create, edit, and delete user accounts. Each account can be assigned different permissions that limit the usage of the system including:
    a. Search
    b. Set up
    c. Pan/Tilt
    d. Backup
    e. Forbidden Cameras
    f. Shut down
42. The ability to enable or disable access by the Web Viewer Software, allowing a user to view live video using an Internet browser.

43. The ability to adjust the resolution setting when sending video to remote clients.
44. The ability to throttle the bandwidth of the digital recorder to ensure that images and system messages are delivered as quickly as possible within the capabilities of the network's available bandwidth.
45. Include a User Management Console, which allows the user to create, edit, and delete user accounts. Each account can be assigned different privileges that limit the usage of the system. Privileges shall include, but not be limited to, the following functions:
    a. Search
    b. Setup
    c. Pan/Tilt
    d. Backup
    e. Shutdown
    f. Intensive
    g. Relay Out
    h. Pan/Tilt Advance
    i. Hidden Cameras/Audio
    j. User Ranking
    k. Auto Log Off
46. Provide the user ability to obtain the software version of the digital recorder.
47. Run a series of self-tests during power up, and display messages as the various hardware and software sub-systems are activated. After power up, the digital recorder's software must automatically load and display the main screen.
48. Display the camera status for each camera next to the camera number (or name) in the video display area. The information must include:
    a. Camera number and custom name
    b. Recording status, which must show whether a camera is currently recording continuously, or whether a camera is recording based on motion.
    c. Special recording status, which must indicate whether a camera's associated sensor has been activated, and/or when the user activates the instant recording option for the selected camera.
49. Offer the following screen division sets (depending on the model):
    a. Display the first four videos (1–4) in the video display area.
    b. Display the next four videos (5–8) in the video display area.
    c. Display the next four videos (9–12) in the video display area.
    d. Display the next four videos (13–16) in the video display area.
    e. Display all sixteen (16) videos in the video display area.
50. Have the ability to adjust each video input's brightness, contrast, and hue, to optimize the clarity and detail of recorded video.
51. Incorporate motion detection, including the ability to create multiple detection regions for each video input.
52. Include the ability for post-alarm recording, which must record video for a specified time before and/or after a motion or sensor alarm has occurred. The time period must be selectable from zero (0) to ninety-nine (50) seconds.

53. Include a video loss alarm function to allow an alarm event to occur when a camera loses the signal for any reason (e.g. camera power failure, cable being cut, camera damage, etc.). When a video loss event occurs, the operator shall have the option to enable an alarm output.
54. Include Alarm Monitor software to stream video across a LAN to a client PC when an alarm is detected on the unit. The operator shall have the ability to stop, play forward and backward, frame by frame or at real speed, the video that streams across. The program must constantly monitor for a signal from the digital recorder, and when an alarm signal is detected the Alarm Monitor must notify the operator of an event. The Alarm Monitor image viewer shall also allow the user to search through past events that have been recorded on the client PC.
55. The Instant Recording feature allows users to manually initiate recording on a specific camera, overriding the current schedule.
56. Provide, through the remote software, the ability to export single images in the JPG file format and save video clips in the AVI format. A digital signature must be attached to every JPG and AVI file exported by the unit for use with the bundled Digital Verifier application. This function must be unique to the unit and its verification software; and shall not interfere with viewing files using other applications.
57. Offer on screen PTZ camera control by clicking and dragging the mouse over the live video display and include play controls to play back the recorded video either forward or reverse, at multiple speeds.
58. Include the ability to search by using fast forward or rewind. Using the feature, the operator shall be able to search frame by frame using any number of cameras and have the ability to speed up or slow down the speed of playback using a slow/fast slide bar.
59. Include an index search. Using this feature the operator shall be able to search through previously recorded video based on motion detection, sensor trip or instant record.
60. Include a preview search function. Using this feature the operator shall be able to search using a 24-hour visual overview of one single camera by separating a 24-hour period into 24 images, each one representing the first second of each hour. The operator must then have the ability to drill down to the search to 10-minute increments and then 1-minute increments by simple double left clicking on a displayed image.
61. Include a panorama search function. Using this feature the operator shall be able to search one camera frame-by-frame using a 16-image grid.
62. Include an object or post motion (forensic) search. Using this feature the operator shall be able to search through previously recorded video for motion within an operator defined field.
63. Include a status search. Using this feature the operator shall be able to see a single camera on the screen and, using a split view, view each frame sequentially side by side.
64. The ability to search recorded video on the main screen by simply clicking the middle mouse scroll button and selecting rewind and fast forward options.
65. Provide simultaneous playback viewing while recording live images, and backing up recorded images in true multiplex operation.
66. Incorporate a software watchdog for restarting the system in the event of a system lock-up.

I. MULTI-SITE MANAGEMENT SOFTWARE (ENTERPRISE VMS): The digital recorder shall come with multi-site management software free of charge. The Digital Recorder Manufacturer shall provide additional copies of the Multi-Site Management software via the web at no

additional charge, along with upgrades free of charge during the product warranty period.

The MULTI-SITE MANAGEMENT SOFTWARE shall include, as a minimum, the following benefits/features/functions/specifications. The Multi-Site software shall:

1. Provide the operator, with administrator privileges, of remotely administering most of the functions that the user has locally, including administration privileges, camera/PTZ adjustments, frame setup, recording schedule, network configuration, and log file retrieval and viewing. The administrator shall also be able to add, delete, or update users when connected to the system remotely.
2. Provide configuration of user accounts with a multitude of assigned privileges that allow or deny access to different functions, therefore ensuring that only authorized personnel are allowed to log in to the Digital Recorder and perform operational functions.
3. Be able to perform remote health check of all systems connected; monitoring Warning and Failures counts on hard drive status, recording status, video loss and disk free space %. The Health check feature shall also provide:
    a. Selectable actions which include: Pop op on Failure/Warning or Voice Warning on failure.
    b. The ability to define interval checks by day (up to 7 days), hour (up to 24 hours) or minutes (minimum 10 minutes).
    c. E-mail notification options for warning and failure events.
4. Be able to send email alarms for motion detection and sensor events.
5. Use the same user accounts that the digital recorder uses locally.
6. Provide a detailed list of log events with the Log Manager.
7. Be able to support multiple digital recorder connections simultaneously and control the digital recorders using a single PC workstation with appropriate network connectivity.
8. Be capable of supporting up to 4 monitors. Shall be capable of enabling the Map Editor, Search windows and Live Display on any of the 4 monitor outputs.
9. Be capable of displaying up to 64 cameras in live view on one monitor or displaying a multitude of different live view camera divisions across 4 monitors.
10. Offer a highly configurable UI that provides user-friendly options including toolbar selections, a detailed Connection list providing individual NVR information, icon size selections, viewing pane selections and various main window selections including multiple open windows organized by tabs at the top of the Live View area.
11. Be capable of exporting AVI video and jpeg images - with a digital signature.
12. Be able to create custom interactive maps and incorporate cameras and/or sensors to locations on the map, link multiple maps, use linked internet maps (Google, etc.). Shall also provide support for AutoCAD (*.DXF, *.DWG) and Image files (*.JPG, *.BMP, *.WMF, *.EMF).
13. Allow 2-Way live audio communication with the digital recorder.
14. The Multi-Site software should provide the following Search capabilities:
    a. Multiple Search: simultaneous search from multiple NVRs on a single screen.
    b. Preview Search: allowing a single day of video to be searched by 1-hour, 10- and 1-minute blocks of time.
    c. Index Search: provides search based on sensor, motion and instant record events.
    d. Status Search: displays a timeline graph allowing recorded video to be located and instantly played from a selected time.

e. Point of Sale search: allowing search on information transmitted during POS transactions.

15. Provide detailed Search functions that include multiple Search methods, individual camera or screen division selections, Bookmarks for quickly marking video clips for later review or backup, JPG or AVI save file options, increase/decrease playback speeds, zoom in/out options, hour/minute control bars and the ability to Sync the playback of multiple cameras.
16. Be able to backup video data in proprietary format, AVI and/or JPEG. AVI backup shall provide the operator with an AVI duration selection and Quality selection.
17. Be capable of automatically transferring live images via TCP/IP to an emergency client workstation in the event a sensor is activated. The emergency agent software shall be capable of automatically opening without assistance from the operator.
18. Be capable of alarm monitoring, keeping track of all incoming motion, alarm input and video loss alarms in real time. Filter options shall be included providing the operator with the ability to select a status level of the alarms. Alarm event indicators shall be color coded and include Video Loss, Motion, Sensor, Relay, No Signal, Write Fail, Connected and Disconnected.
19. Provide a shortcut list in the main screen that displays the following:
    a. Server List: Displays all added NVRs and allows users to connect to NVRs and their associated cameras quickly
    b. User Screen: Provides list of customized screens, allows adding new screens and editing existing screens.
    c. Window List: Organizes open windows into categories – Live Windows, Search Windows and other active windows.
    d. Hot Spot: Feature allowing users to zoom in on an AOI (area of interest).
20. Provide a Right-Click Live Camera option that allows for pausing Live Video, starting Live Video (after pause), Capturing a JPG snapshot, Full screen option, setting resolution and control of video screen display options.
21. Provide a Right-Click DVR option that allows for instant DVR and Camera connect/disconnect, Search feature, POS On/Off, Device Configuration, and Network/Clip backups.
22. Provide a Live Camera Tool bar that provides Full Screen options, ability to drag live cameras from one screen to another, options to enable an on-screen PTZ compass, Cloning Live View in another window and Screen division options.
23. Provide a Lock List function that locks specific functions based off a user-defined waiting period. The list includes, but is not limited to:
    a. DVR configuration
    b. Map editing
    c. Log Viewer access
    d. Health Check status
    e. Search
    f. Shutting down VMS software
24. Provide a rich Network Backup feature that allows the operator to backup any or all cameras on a selected NVR to a local or network drive. Functions shall allow for specific day selection and hour to minute selection blocks within each day. No Data, Existing Data and Selected Data blocks shall be color coded for easy to identify backup options. A download status bar shall provide Total and Current percentage completion times along with a Total overall file size (indicated in KB/s) indicator.

25. Provide a Clip Backup feature allowing the operator to backup one or more cameras to a local drive, CD/DVD or USB device. Functions shall include individual camera selection, backup target device, backup start and end time selections, clip information options including name/memo, and the option to include the backup viewer software with the data clip. Packet size configuration shall also be available providing the operator with the ability to lower the clip size for low bandwidth transmission environments.
26. Be capable of displaying POS text overlay on POS data within the live video display. Shall provide multiple options for searching POS data recorded on DVRs. POS search should be defined through a user defined item name or selectable from a predefined item list. Search filter options should provide a value definable selection based off specific value conditions.
27. Provide the ability to Customize Screens by allowing the user to create groups of cameras called screens and customize the organization of the cameras. Each screen should allow up to 64 different cameras.
28. Have the ability to auto Save settings on log-off and auto Load settings on log-on.
29. Have a configurable alert sound setting for DVR disconnections from the VMS software.
30. Have the option to enable a Map Alarm Sound on an associated event.
31. Have the option to enable the Live Video window as a top-most application.
32. Have the ability to enable “pop up” live video of recorder associated with an alarm or event.
33. Provide the option to Auto-Switch the time between camera sequencing.
34. Have the ability to enable a full screen channel when live mode display is double-clicked.
35. Provide the user ability to hide the following on screen display text (OSD):
    a. Hide all OSD
    b. Hide channel number
    c. Hide server name
    d. Hide camera name
    e. Hide 64 division to disable the 64-channel screen division option
    f. Hide PTZ overlay
    g. Hide Time/Date
36. Provide the option to enable PTZ ACP in advance mode on screen.
37. Allow screen ratio configurations of None, Original, 4:3 & 16:9 (Widescreen).
38. Provide an option for Full Screen Channel on motion and sensor alarms. Shall allow for user defined Full Screen durations of up to 100 (seconds) and an option to Ignore alarm events after Full Screen configurable in seconds up to 100.
39. Have the ability to define schedules to discard alarms. Shall provide a user configurable setting to filter, by category, including Motion, Sensor, Sensor (Camera) and Relay.
40. Offer the operator a user-friendly DVR Site List page displaying a list of all added recorders. Shall provide sections to add all DVR information including:
    a. Server Name
    b. IP/URL
    c. Port #’s

d. User ID

e. Password

f. DVR Group

g. Additional information: Contact information including Manager Name, Telephone #, Police and Fire department information.

41. Provide the operator the ability to edit all information of any DVR in the list of connected recorders within the DVR Site List page.

42. Provide an option to custom name Sensors and Relays of any DVR in the list of connected recorders within the DVR Site List page.

J. MULTI-SITE SYSTEM HARDWARE for the NVR

Single / Multi-site software: The recommended hardware and operating system configuration for a PC workstation shall have:

1. Intel Quad Core i7 processor (or equivalent)
2. 4 GB System Memory
3. DirectX 9 or Higher
4. ATI 7770 Video Card (or equivalent) / Intel HD2000 onboard graphics (or newer)
5. 512k Network Connection
6. TCP/IP Installed
7. Microsoft Windows® 10, Windows Server 2012/2016
8. 1280 x 1024 Optimal Display Resolution

---------- END OF NETWORKED NVR SECTION ----------

PART 3 EXECUTION

3.1 INSPECTION AND PREPARATION WORK

A. This contractor shall examine the conditions under which the system installation is to be performed and notify the Owner's Representative or Design Professional in writing of unsatisfactory conditions. Do not proceed with the work until unsatisfactory conditions have been corrected in a manner acceptable to provide a workmanlike installation.

B. Review areas of potential interference and resolve conflicts before proceeding with the work. Coordinate ceiling layout and wall layout and other work that penetrates or is supported throughout the space of the building. All work shall be flush and workmanlike in all finished areas.

3.2 INSTALLATION

A. Install materials and equipment in accordance with manufacturer's printed instructions to comply with governing regulations and industry standards applicable to the work and as shown on approved shop drawings.

B. Arrange and mount all equipment and materials in a manner acceptable to the Design Professional and Owner.

C. Installation shall conform to the basic guidelines.

1. Use of approved wire, cable, raceways, wiring, devices, hangers, supports and fastening devices.
2. Separation of high and low voltage wiring is required throughout the installation.
3. All wiring shall be thoroughly tested for grounds and opens.

D. All power wiring shall be in metallic conduit. The maximum conduit fill shall not exceed 40% of rated capacity. Refer to NFPA 70-NEC for additional requirements.

E. Cabling and Wire Requirements:

1. Low voltage signal and/or control wiring shall run in separate conduit/raceway from electric power cables. Cables for door locks are power cables. Provide separation from lighting fixtures and other electrical appurtenances. Provide electrical interference protection circuits as required to maintain the signal quality specified herein and required by system manufacturers.
2. The individual systems low voltage cabling shall use separate junction boxes and enclosures.
3. The minimum low voltage cabling for security, communications and safety systems shall be as required by the manufacturers without cost increases to owner for the full function intended. The systems cabling shall meet the requirements of NFPA 70/NEC Articles 725, 760 and 800 as applicable for each type of system specified.
    a. All dimensions and conditions shall be verified in the field. The Contractor shall notify the Architect of any discrepancies before proceeding with the work.
    b. Card reader cables shall be NFPA 70, Article 725 compliant.
    c. Electrified mortise and door strike power cabling shall be NFPA 70, Article 725 compliant.
    d. Touch sensor bar power cabling shall be NFPA 70, Article 725 compliant.

e. Door control/door monitoring power cabling shall be NFPA 70, Article 725 compliant.

f. Elevator and fire alarm interfacing cabling shall be NFPA 70, Article 725 compliant.

g. Card Readers to Control Panel: maximum length shall not exceed 500 feet.

h. Extended Reader Line Drivers: may be used between the Central Unit and the Remote Unit for a maximum length not to exceed 10,000 feet (3050 m). Cabling between the Central unit and the control panel shall be as specified for a reader, request to exit and a relay. Cabling between the Remote Unit shall be as specified for a reader, request to exit and a door strike.

i. Alarm Point and Request to Exit Point to Control Panel: maximum length shall not exceed 500 feet (150 m).

j. Relay to Device: maximum distance shall not exceed 1,000 feet (300 m).

k. Refer to the riser diagram located on the Contract Drawings.

4. The minimum bend radius of all security, communication conduits provided under this project shall be 6 inches (150 mm). Provide and maintain pull strings/tapes/ropes in all conduits for future installation of additional fiber optic cabling.

F. Fire Stopping:

1. Provide code required fire stopping at all fire rated wall, floor and partition penetrations with UL listed fire-stopping materials.

G. Junction Boxes, Enclosures/Cabinets, Equipment Racks:

1. The junction and pull boxes shall be securely attached to the structural members of the building at locations accessible for servicing. Provide access doors at locations accessible for servicing. Provide access doors at locations where access is not readily available.

2. The equipment enclosures shall be installed at approved locations and be typically ventilated as required to maintain the environmental conditions specified by the electronic equipment manufacturers.

3. All junction boxes and pull boxes shall be labeled. The box label shall state the system and use of cabling. The labeling shall be made with markers which are indelible when and after in contact with water and oil.

4. Each box and enclosure shall contain a cabling and wiring log identifying all cabling accessible whether is connected or is passing by.

H. Grounding and Surge Protection:

1. Provide single point grounding of the individual systems as recommended by IEEE and system manufacturers. Provide all cabling, bonding and insulation materials as required. Provide surge protection and clamping for all circuits. Coordinate all grounding, surge protection and clamping circuit requirements with the system manufacturers.

2. Coordinate grounding requirements with other trades and contractors to preclude closing of ground loops via peripheral equipment supplied from different electrical power sources. Provide isolation transformers and other equipment as required.

3.3 FIELD QUALITY CONTROL

A. A project manager shall be appointed during the course of the installation. This shall assure complete coordination and technical information when requested by other trades. This person shall be responsible for all quality control during installation, equipment set-up and testing. This

individual shall have training to provide firsthand knowledge of the installation.

3.4 ADJUSTING, TESTING AND CLEANING

A. Contractor shall be required to perform complete testing and verification of the following:

1. Card Reader maximum access time shall be 0.75 seconds under all system loads, i.e. regardless of number of cards presented simultaneously.
2. Proper operation of electric door strikes, egress switching (where required), door position monitor switches and exit hardware.
3. Proper operation of electro-magnetic locks and strikes, including full interface, control and override by the Card Access System.
4. Proper operation of magnetic door switches.
5. Proper operation of keyed EML bypass / override stations.
6. Proper operation of the intercom system(s) and their door release pushbuttons.

3.5 ADDITIONAL MATERIALS

A. Contractor shall provide the following spare equipment for items scheduled:

1. Two (2) card readers.
2. One (1) PIR egress device.
3. One (1) DRM Board(s) (Dual Reader Module).
4. Two (2) door position contacts.
5. 200 cards - one side printed/one side blank, as directed by the Owner.

3.6 DEMONSTRATION

A. Provide system demonstration.

1. Demonstrate normal and abnormal modes of operation and required response to each.
2. Provide system training.

3.7 PROTECTION

A. Protect installed products until completion of project.

B. Touch-up, repair or replace damaged products before substantial completion.

END OF SECTION