HOLMES COUNTY CONSOLIDATED SCHOOL DISTRICT
REQUEST FOR PROPOSAL

Overview

1. Introduction: The Holmes County Consolidated School District (HCCSD) is located in Holmes County. School facilities consist of seven schools and one central office. The district has approximately 2,150 students.

2. Purpose of RFP: The district is requesting sealed bid proposals for a **Controlled Access Security System that includes a stand-alone video surveillance recording system at selected schools and offices in the Holmes County School District.**

3. Tentative schedule of RFP events are as follows:
   a. **Advertisement Dates: November 19, 2026 and November 26, 2026**
   b. **Pre-Bid Site Walk-Through: 9:00 am, November 30, 2026**
   c. **Deadline Date for Questions: 4:30 p.m., December 2, 2026**
   d. **Proposal Due Date: December 4, 2026 at 2:00 p.m.**
   e. **Bid Opening: December 7, 2026 at 9:30 a.m.**
   f. **Vendor Selection Notification: December 11, 2026**

4. General Specifications and Instructions to Bidders:
   a. A paper copy or an email copy of this document, including any addendums, can be obtained by a request below:

Ms. Betty Bridgeford
Holmes County Consolidated School District
Post Office Box 630
313 Olive Street
Lexington, MS 39095
(662) 834-2175 (voice)
E-Mail: bbridgeford@holmesccsd.org

   b. RFP Submission requirements: **Submit 4 copies** of the RFP response in one sealed package with **Controlled Access and Video Surveillance Security System indicated on** the outside of the package by 2:00 p.m. on December 4, 2026 to the following address:

Michelle Cage, Chief Finance Officer
Holmes County Consolidated School District
Post Office Box 630
313 Olive Street
Lexington, MS 39095

COMMUNICATIONS REGARDING THE RFP

All questions regarding the RFP are to be submitted, in writing to:

Ms. Betty Bridgeford
Holmes County Consolidated School District
Post Office Box 630
313 Olive Street
Lexington, MS 39095
(662) 834-2175 (voice)
E-Mail: bbridgeford@holmesccsd.org

The deadline for submission of written questions is December 2, 2026. All responses to written questions and changes to specification requirements will be communicated via email to all potential bidders in form of a Q & A document.

All questions, comments and requests for clarifications must be in writing. Any oral communications shall be considered unofficial and non-binding.

Only written responses to written communications shall be considered official and binding upon the School District. The School District reserves the right, at its sole discretion, to determine appropriate and adequate responses to the written comments, questions and requests for clarification.

All addendums and/or any other correspondence (general information) to this RFP will be made available **exclusively** through the Holmes County Consolidated School District's website.

Minimum Eligibility Requirements for Contract Award

1. Applicants must provide documentation of a minimum of three (3) years of experience providing similar services to business or educational organizations.

   Applicants must provide a listing of previous installs similar to the scope of this bid over the past five year.

3. Applicants must include abilities, qualifications, and experience of all persons who would be assigned to provide the required services.
4. Applicants must address and provide (if applicable) a list of any pending/past litigation or investigations that have occurred within the past five (3) years.
5. Applicants must have financial stability and adequate staff to manage the program (technical support).
6. Applicants must be in compliance with all applicable City, County, State and Federal laws, regulation codes and ordinances.

The proposal will consist of four parts:

- **Part I** is the Vendor Profile, which shall provide satisfactory evidence of the vendor's capability to manage and coordinate the types of activities and to provide the services described in this RFP in a timely manner. Special attention should be given to the qualifications listed in the minimum eligibility section of this RFP. A discussion shall include a description of the vendor's background and relevant experience as related to the described activities. A description and details of the relevant experience shall be included. A minimum of three (3) references shall be provided. Samples of previous work may be included.

- **Part II** is the Production Proposal. The Production Proposal shall provide a detailed plan describing how the services will be performed to meet the requirements of the RFP. The proposal must be prepared and organized in a clear and concise manner that is easily understandable. The proposal shall address the tasks to be accomplished, processes to be undertaken to accomplish those tasks and a proposed timeline for completion. Examples of materials that demonstrate the quality of work completed by the vendor on similar projects should be included. Offerors may designate those portions of the proposals which contain trade secrets or other proprietary data which may remain confidential in accordance with section 25-61-9 and 79-23-1 of the Mississippi Code.

- **Part III** is the Implementation Plan. The Implementation Plan shall provide a proposed timeline for the implementation of the install. .

- **Part IV** is the Budget that shall include the cost proposal and must encompass all requirements of this RFP. In order to be considered, vendors must submit a proposal that includes the budget narrative/cost proposal that addresses all costs for services, expenses, and products specified in the RFP. The budget narrative is a maximum cost. The HCCSD will not pay any costs above this amount. A detailed budget narrative shall be included. Indirect costs will not be allowed. The budget narrative should include all costs associated with the project. A unit price shall be given for each service and such unit price shall be the same throughout the proposal. The Budget Summary form shall be completed and shall accompany the proposal.

Project Scope

Secure Access Control and Video Intercom Systems
Owner: Holmes County Consolidated School District
Address: 313 Olive Street, Lexington, Mississippi

Project: School and Administrative Building Security and Controlled-Access Improvements
Holmes County Consolidated School District invites sealed bids from qualified security-system contractors. The selected contractor shall provide all labor, equipment, materials, programming, testing, training, warranty service, and incidentals required to deliver fully operational, access-control and video-intercom systems at the facilities listed in this document.

1. Project Intent
The project is intended to secure designated exterior school entrances through centrally managed electronic access control, credentialed staff entry, controlled visitor entry, video and two-way audio communication, and safe egress. Authorized District personnel must be able to administer the system remotely. The additional intent is to provide video surveillance and recording of the front and rear of identified school properties for security purposes 24/7

2. General System Requirements
The contractor shall furnish and install a complete, operational system that includes:

- Access control with remote user administration, credential management, schedules, door programming, and system monitoring through a software-based VMS with remote access through an App.
- Access-control panels with integrated or dedicated power supplies and backup batteries. Panels shall be sized for the number of controlled doors and installed in secure, accessible communications or equipment rooms.
- HID Signo readers at each controlled door. Readers shall support proximity and Bluetooth/mobile credentials.
- One hundred prox cards per school to be provided.
- Electrified locking hardware appropriate to each opening, including surface-mount electric strikes and/or 1,200-pound magnetic locks as required by the door configuration.
- Egress components for magnetically locked doors, including motion request-to-exit devices, exit buttons, and any other devices required for code-compliant operation.
- Video-intercom systems at designated front-entry visitor doors. Each system shall include an exterior door station, an interior master station, an interior expansion station, and two desk mounts. Intercoms shall provide HD video and two-way audio.
- All necessary cabling, conduits or surface raceway where needed, terminations, connectors, power components, programming, labeling, and restoration of finishes disturbed by the work.
- Equipment SHALL match the existing Monitorcast Access Control System that is currently installed at Durant Elementary School. There will be a centralized database installed in the District Office to manage the access control system at each of the schools. Video-intercom equipment shall be the Aiphone intercom system that matches the existing system at Durant Elementary School. It must provide video, audio, and door-release functionality.

3. Facilities and Scope of Work

3.1 Holmes County School Central Office Entrances:

Two—front and rear. Provide:

- One two-door access-control panel with power supply and backup batteries.
- Two proximity readers, one at each entrance.
- One motion request-to-exit device at the front door.
- Two exit buttons, one at each entrance.
- One desk door-release button for the front door.
- One 1,200-pound magnetic lock for the front door.
- One surface-mount electric strike for the rear door.
- Fifty prox cards.
- Wiring from the control panel to the front and rear doors.

Video surveillance and recording:

- One five-port PoE network switch.
- Two WV-S25500-F6L indoor/outdoor PoE cameras, each with 5MP UHD video, IR LED, color night vision, and video analytics.
- Camera placement to monitor the front parking area and the back yard/back door.
- Provide on-site recording of the cameras for a minimum of 30 days.
- Two complete CAT6 camera cable runs, including cable and connections.

3.2 S.V. Marshall Elementary/Middle School

The Elementary and Middle Schools are housed in one building. Secure eight entrances: four on the Elementary side and four on the Middle School side.

Provide:

- Two front-entry video-intercom systems: one for the Elementary entrance and one for the Middle School entrance.
- Two four-door access-control panels, each with a power supply and backup batteries.
- Eight readers and HES-type surface-mount electric strikes, or approved equivalents.
- One exit button and one motion request-to-exit device at each of the two front doors.
- One hundred (100) prox cards.
- Wiring from the control panels to all eight doors.

Video surveillance and recording:

- One five-port PoE network switch.
- Two WV-S25500-F6L indoor/outdoor PoE cameras, each with 5MP UHD video, IR LED, color night vision, and video analytics.
- Camera placement to monitor the front parking area and the back yard/back door.
- Provide on-site recording of the cameras for a minimum of 30 days.
- Two complete CAT6 camera cable runs, including cable and connections.

3.3 W.M. Dean Elementary School

An existing system is installed. The work is to restore operation and provide access control for eight selected doors.

Provide:

- Two four-door access-control panels with power supplies and backup batteries.
- One video-intercom system with an extension and two desk-mount monitors.
- Reconnection and commissioning of eight doors.
- Reuse of existing card readers and locking hardware.

Video surveillance and recording:

- One five-port PoE network switch.
- Two WV-S25500-F6L indoor/outdoor PoE cameras, each with 5MP UHD video, IR LED, color night vision, and video analytics.
- Camera placement to monitor the front parking area and the back yard/back door.
- Provide on-site recording of the cameras for a minimum of 30 days.
- Two complete CAT6 camera cable runs, including cable and connections.

3.4 W.L. Sullivan Middle School

Provide:

- One four-door access-control panel with power supply and backup batteries.
- One front-entry video-intercom system, including an exterior door station, interior master station, interior expansion station, and two desk mounts. The system shall provide HD video and two-way audio.
- Four readers and HES-type surface-mount electric strikes, or approved equivalents.
- One exit button.
- One hundred (100) prox cards
- Wiring to the panels, including outdoor-rated wiring for one rear building door.

Video surveillance and recording:

- One five-port PoE network switch.
- Two WV-S25500-F6L indoor/outdoor PoE cameras, each with 5MP UHD video, IR LED, color night vision, and video analytics.
- Camera placement to monitor the front parking area and the back yard/back door.
- Provide on-site recording of the cameras for a minimum of 30 days.
- Two complete CAT6 camera cable runs, including cable and connections.

3.5 Career and Technical Education Center

Provide:

- One front-entry video-intercom system, including an exterior door station, interior master station, interior expansion station, and two desk mounts. The system shall provide HD video and two-way audio.
- One access-control panel with power supply and backup batteries.
- One proximity reader.
- One HES Slimline surface-mount electric strike, or approved equivalent.
- One hundred (100) prox cards.

Video surveillance and recording:

- One five-port PoE network switch.
- Two WV-S25500-F6L indoor/outdoor PoE cameras, each with 5MP UHD video, IR LED, color night vision, and video analytics.
- Camera placement to monitor the front parking area and the back yard/back door.
- Provide on-site recording of the cameras for a minimum of 30 days.
- Two complete CAT6 camera cable runs, including cable and connections.

3.6 GWR Academy

Provide controlled entry, exterior video surveillance, and recording.

Access control and intercom:

- One front-entry video-intercom system, including an exterior door station, interior master station, interior expansion station, and two desk mounts. The system shall provide HD video and two-way audio.
- One access-control panel with power supply and backup batteries.
- One proximity reader.
- One HES Slimline surface-mount electric strike.
- One hundred (100) prox cards.
- All required wiring from the panel to the access door.

Video surveillance and recording:

- One five-port PoE network switch.
- Two WV-S25500-F6L indoor/outdoor PoE cameras, each with 5MP UHD video, IR LED, color night vision, and video analytics.
- Camera placement to monitor the front parking area and the back yard/back door.
- Provide on-site recording of the cameras for a minimum of 30 days.
- Two complete CAT6 camera cable runs, including cable and connections.

3.7 Durant Elementary School

Video surveillance and recording: (Only)

- One five-port PoE network switch.
- Two WV-S25500-F6L indoor/outdoor PoE cameras, each with 5MP UHD video, IR LED, color night vision, and video analytics.
- Camera placement to monitor the front parking area and the back yard/back door.
- Provide on-site recording of the cameras for a minimum of 30 days.
- Two complete CAT6 camera cable runs, including cable and connections.

4. Installation and Performance Requirements
The contractor shall:

- Verify existing site conditions, door construction and handing, hardware compatibility, wiring routes, electrical capacity, and network connectivity before beginning installation.
- Coordinate work to minimize disruption to instruction and school operations and to protect student safety.
- Complete all wiring, terminations, mounting, configuration, testing, and commissioning necessary for the systems to operate as specified.
- Use outdoor-rated wiring wherever wiring is exposed to outdoor conditions or routed underground or to an outbuilding.
- Label all panels, power supplies, cables, readers, doors, and associated components.
- Integrate access-controlled doors with visitor-intercom release functions where indicated.
- Configure schedules, user roles, credentials, door groups, and District administrative access before final acceptance.
- Test every reader, credential, lock, exit device, intercom station, video feed, audio path, door-release function, battery backup, and remote-management function.
- Correct all deficiencies before final acceptance.

5. Training, Documentation, and Closeout
Before final acceptance, the contractor shall provide:

- Administrator training for designated District personnel covering user enrollment and removal, credential assignment, door schedules, remote locking and unlocking, reporting, and basic troubleshooting.
- A complete equipment list organized by facility and door.
- Panel locations, wiring diagrams, system-programming information, and manufacturer documentation.
- A credential inventory and transfer to the district of all administrative access, accounts, passwords, licenses, and ownership rights.

6. Warranty and Service
The contractor shall provide a minimum two-year parts-and-labor warranty covering all new equipment and installation work. Warranty service shall include repair or replacement of defective equipment, labor, programming, and return service necessary to restore normal operation.

Bidders shall separately identify all recurring cloud-management, communication, licensing, or monitoring charges. Bidders shall clearly disclose any loss of functionality that would result from discontinuation of a required recurring service.

7. Bid Submission Requirements
Bids shall include:

- The Access Control and Video cameras MUST match the existing i-PRO Video Insight/Monitorcast System (Specs Attached) that was installed at Durant Elementary School in 2025. The school district intends to utilize that system as the design for each of the schools in the district. There will be a centralized database in the District Office to manage all Video & Access Control in the future.
- A lump-sum base bid itemized by facility and major equipment category.
- The manufacturer, model number, quantity, and technical specifications for all proposed equipment.
- An installation schedule and estimated duration for each site.
- A description of the bidder's relevant experience with K–12 access-control and video-intercom installations.
- Proof of required Mississippi licensing, insurance, and qualifications.
- Warranty terms, service-response procedures, and all recurring costs.
- A statement identifying all exclusions, assumptions, alternates, or deviations from these specifications.

8. Basis of Award

The district intends to award the contract to the responsible and responsive bidder whose proposal is determined to be in the best interest of Holmes County Consolidated School District. Evaluation may consider compliance with these specifications, total cost, equipment quality, installation approach, warranty, recurring costs, relevant experience, and the ability to complete the work within the required schedule.

The district reserves the right to reject any or all bids, waive informalities, negotiate permitted changes, and award the project in whole or in part, as permitted by applicable law.

9. Pre-Bid Conference

A job walk for this bid will begin at GWR Academy in Tchula at 9am on Monday, Nov. 30th. We will then visit each of the sites listed in the specs. The Location of the GWR Academy is 32 School Street, Tchula, MS.

SCORING METHODOLOGY

Holmes County Consolidated School District will use any or all of the following categories in developing a scoring mechanism for this bid prior to the receipt of proposals. All information provided by the Vendors, as well as any other information available to Holmes County Consolidated School District staff, will be used to evaluate the proposals.

1. Experience — 20 Points

Variables considered in evaluating this category will include, but not be limited to the following:

a) Applicant's experience and success in conducting similar work
b) Experience in fulfilling contract of similar nature
c) Quality and completeness of proposal
d) Number of years in business

2. Project Design — 20 Points

Variables considered in evaluating this category will include, but not be limited to the following: overall approach and the Applicant's grasp of the project as shown by the depth, breath, and clarity of the proposal.

3. Cost Efficiency — 40 Points

a. Total cost of proposed services
b. Service and support;
c. Cost is itemized separately

4. Program Operations — 20 Points

a. Adequacy of resources, including personnel, equipment, financial stability and other related factors
b. Management, planning, and technical support: The quality of procedures and organizational structures proposed for completion of the work

Possible Score: 100 Points

The Applicants should submit its best and final cost offer in the proposal. The district, at its sole discretion, may open negotiations with responsible applicants after submission of proposals and prior to award. The district specifically reserves the right to award without negotiations based upon written proposals only.

A. The evaluation process will include contact with individuals or organizations identified by the Applicant as a current/former customer or reference. The evaluation process also includes a status check with the Mississippi State Comptroller to ensure that the Applicant is in good standing.

B. Proposals received after the specified date and time will not be accepted or considered. To guard against premature opening, sealed proposals shall be submitted, plainly marked with the proposal title, vendor name, and time and date of the proposal opening. Evaluation of the proposals is expected to begin shortly after the proposal due date. To document compliance with the deadline, the proposal will be date and time stamped upon receipt.

C. HCCSD will receive proposals until the date and time shown in this RFP. Proposals will be opened only in the presence of HCCSD personnel. There will be no public opening of proposals but a public log will be kept of the names of all vendor organizations that submitted proposals.

D. The HCCSD reserves the right to reject any and all proposals, to negotiate with the best proposed offer to address issues other than those described in the proposal, to award a contract to other than the low offer, or not to make any award if it is determined to be in the best interest of the HCCSD.

2. PRODUCTS

2.1 GENERAL

1. The security management system shall be deployed through IP network infrastructure with a two-tiered hardware hierarchy. The IP Door Controller shall be capable of running on an existing TCP/IP network and shall be accessible, configurable, and manageable from any network-connected PC with a browser.
2. Browser access for configuration and administration of the system shall be possible from a PC on the same subnet, through routers and gateways from other subnets, and from the Internet. Control and management of the system shall therefore be geographically independent.
3. The top hardware tier shall be the MonitorCast v4 Server based platform. Installed applications on the MonitorCast v4 Server is to be an operating system, a web MonitorCast v4 Server, security application software, and the database of personnel and system activity.
4. The bottom hardware tier shall be the IP Door Controller. The IP Door Controller shall make and manage access control decisions with data provided by the MonitorCast v4 Server, and it shall control the communication between the IP Door Controller and door hardware connected to the IP Door Controller inputs, outputs, and readers. This modular design shall make it possible for the system to continue to manage access control and store system activity logs, even during network downtime. When network connectivity is re-established, the system activity logs shall be automatically re-integrated to the host MonitorCast v4 server.

A. The system shall integrate, within a browser interface; access control and video monitoring. These applications shall be a fully bi-directional integrated software architecture.
   1. The database tier shall use Microsoft SQL Server residing on the MonitorCast v4 Server. Microsoft SQL Server on the MonitorCast v4 Server shall be a full featured, high performance database management system. This shall provide a small footprint, low administration, and a high reliability relational database that is embedded without requiring the use of a separate PC MonitorCast v4 Server.
   2. The MonitorCast v4 Server tier shall be based on a Microsoft™ MonitorCast v4 Server 2008 R2 or 2012 MonitorCast v4 Server. This application shall provide a graphically rich security management application through a standard web browser.

B. All equipment and materials used shall be standard components, regularly manufactured, and regularly utilized in the manufacturer's system.

C. All systems and components shall have been thoroughly tested and proven in actual use.

D. All systems and components shall be provided with a manufacturer warranty of one year for software and two years for hardware.

2.2 OVERALL SYSTEM CAPABILITY

A. The security management system shall meet the requirements of business and government access control systems. The system shall monitor and control facility access and shall perform alarm monitoring and integration to camera and video monitoring. The system shall also maintain a database of system activity, personnel access control information, and system user passwords and user role permissions. The system shall be controlled from a web browser and require no software installation or client licenses. The system shall provide control and access to users on Local Area Networks (LAN), Wide Area Networks (WAN),

wireless networks, and the Internet. The system shall provide email and/or text message alerts for all alarm conditions and threats.

B. System Partitioning: The system administrator shall have the ability to divide the system into partitions, allowing subsets of the overall population and/or resources to be managed separately.
   1. From the default Master partition, one or more additional partitions shall be able to be created.
   2. Each partition shall contain some number of administrators, card holders with their credentials, and resources.
   3. When performing administrative functions, the administrator of a partition shall have the ability to create or modify only the cardholders and resources in that partition. However, resources shall be able to be shared across partitions through the mapping of access levels from one partition to another.
   4. System partitioning shall have a precision feature that allows administrators in one or more partitions to view and perform edit functions on person records that belong to another partition.
   5. Administrators shall have the ability to search for person records across all partitions to which they have access. The system administrator shall have the ability to make such cross-partition searches the default for users who have access to multiple partitions.
   6. After finding a personnel group record located in another partition, an administrator shall be able to click a button to switch to that partition directly from the personnel group record—and possibly edit the record, depending on his or her access rights in that partition. Alternatively, an option for making every person record seamlessly visible across all partitions shall be provided.

C. The system shall provide the following Access Control capabilities:
   1. Integrated photo ID creation capability with video verification.
   2. User interface secured access under encrypted password control.
   3. Multiple Site Control.
   4. System-wide timed anti-pass back function.
   5. "First-in-unlock" rule enforcement.
   6. Multiple access levels and cards per person.
   7. Detailed time specifications.
   8. Simultaneous support for multiple card data formats.
   9. Compatibility with various input devices, including biometric readers.
   10. Activation/expiration date/time by person with one-minute resolution.
   11. Access level disable for immediate lockdown.
   12. Multiple holiday schedules.
   13. Timed unlock schedules.
   14. Dual-reader portal support.
   15. Wiegand Reader support.
   16. Magnetic-stripe reader support.
   17. Wiegand keypad PIN support for 4-digit or 6-digit PINs.

D. The system shall provide the following native or VMS integrated monitoring capabilities:
   1. The Home page shall allow users to view a full system summary, including an Activity Log, Auto-Monitor, and dashboard functions.
   2. Common alarm panel integration for disarm on access, and arm on egress.
   3. Integrated real-time IP-based NVR systems with stored video replay for events.
   4. Provides alarms on communication loss.
   5. Provides the ability to record video and link to video for alarm events.
   6. A monitoring desktop that integrates video, system activity logs, floorplans, ID photos, and alarm notifications.
   7. Graphic floorplans with active icons of monitor and access control points.

8. Secure access to the user interface under encrypted password control.
9. Delivery of alerts via VMS Rules Manager or Automation and email.
10. Remote logging of system messages to local host.

E. The system shall provide the following integrated VMS Video Management capabilities:
1. Playback of event-related video.
2. Integrated alarm inputs from the video management system.
3. Digital playback of video events.
4. Linking of video and events based on triggers provided by the system or video system.
5. Support for multiple NVRs.
6. Multiple pre-programmed supported cameras.
7. Monitoring and control through a web browser interface.

F. The system shall provide the following Security Database capabilities:
1. Maintain data of system activity, personnel access control information, system user passwords and custom user role permissions for whole or partial access to system resources and data.
2. LDAP integration for single-user logon authentication.
3. Network-secure API for external application integration.
4. Easy to use custom report generator.
5. Record recall by vehicle tag, name, or card.
6. An API for adding to, deleting from, and modifying the database.
7. Storage of system user passwords and permissions.
8. Storage and recall of ID photos and emergency personal information.
9. Pre-defined reports on system configuration, system activity history, and people.
10. Custom report writer interface that allows the interactive creation of custom reports. Reports may be saved for later reuse. No third-party software (such as Crystal Reports) shall be necessary.
11. Selectable custom report output formats, including PDF & CSV.
12. Custom report repository location. Users shall be able to review, cancel and delete reports from this data storage location.
13. Email and text messaging (SMS) alert notifications.

2.3 HARDWARE REQUIREMENTS

A. The security management system shall employ a modular hardware concept that enables simple system expansion and utilizes a two-tiered hardware hierarchy:
1. At the top tier shall be a MonitorCast v4 Server, which shall contain the database engine, web MonitorCast v4 Server, application software, and configuration data. It is at this level that System Users, through a browser interface, shall interact with the system, set configurations, monitor activities, run reports, and manage alarms.
2. At the bottom tier shall be the IP Door Controller, an intelligent device with native TCP/IP & PoE support, which shall make and manage access control decisions, a set of inputs, outputs and readers.
3. The network device shall run on existing building TCP/IP PoE networks and shall be configurable for access from separate subnets, through gateways and routers, and from the Internet.

B. A MonitorCast v4 Server shall contain a processor, flash memory, and storage. External battery backup shall be used to provide uninterrupted operation in the event of external power loss. The IP Door Controller shall contain IIS for communication with the IP Door Controllers and a network interface port. A MonitorCast v4 Server shall have the following capabilities:
1. Door Controller: (Mercury EP/LP boards) (AD-400/AD-300 Wireless locks) 512
2. Access cards: No Limit

3. Card formats: 15 per Controller
4. Alarm input points: 2,048 per Controller
5. Control point outputs: 2,048 per Controller
6. Ethernet ports: 1
7. Time specifications 512 per Controller
8. Holidays 255 per Controller
9. Access levels per person 15 per person (32,000 per Controller)
10. Cards per person No Limit
11. Concurrent system users Unlimited

C. The IP Door Controller shall make and manage access control decisions with data provided by the MonitorCast v4 Server, and it shall manage the communication between the IP Door Controller connected to the system's inputs, outputs, and readers. The IP Door Controller shall be powered with PoE power input 12.95 W (802.3af or 12V DC 900mA power supply) protocol. Each IP Door Controller shall have the following capabilities:

1. Access control doors 1
2. Readers 2
3. Supervised Inputs 2
4. General Input 2
5. Relay Outputs 2
6. Connectivity 10/100 Ethernet
7. Credential storage 20,000
8. Activity Log records 27,000

D. The IP Door Sub-Controller single door shall make and manage access control decisions with data provided by the MonitorCast v4 Server through the IP Door Sub-Controller, and it shall manage the communication between the IP Door Sub-Controller connected to the system's inputs, outputs, and readers. The IP Door Controller shall be powered with PoE power input 12.95 W (802.3af or 12V DC 900mA power supply) protocol. Each IP Door Controller shall have the following capabilities:

1. Access control doors 1
2. Readers 1
3. Supervised Input 4
4. Relay Outputs 2
5. Connectivity 10/100 Ethernet

E. The Door Sub-Controller single door shall make and manage access control decisions with data provided by the MonitorCast v4 Server through the IP Door Controller, and it shall manage the communication between the IP Door Sub-Controller connected to the system's inputs, outputs, and readers. The IP Door Sub-Controller shall be connected to IP Door Controller using RS-485 protocol. Each IP Door Sub-Controller shall have the following capabilities:

1. Access control doors 1
2. Readers 1
3. General Input 2 (programmable)
4. Dedicated Input 1
5. Relay Outputs 2
6. Connectivity RS-485

F. The Door Sub-Controller two door shall make and manage access control decisions with data provided by the MonitorCast v4 Server through the IP Door Controller, and it shall manage the communication between the IP Door Sub-Controller connected to the system's inputs, outputs and readers. The IP Door Sub-

Controller shall be connected to IP Door Controller using RS-485 protocol. Each IP Door Sub-Controller shall have the following capabilities:

1. Access control doors 2
2. Readers 1
3. General Input 8 (programmable)
4. Dedicated Input 2
5. Relay Outputs 6
6. Connectivity RS-485

G. The Serial Input Sub-Controller shall make and manage access control decisions with data provided by the MonitorCast v4 Server through the IP Door Controller, and it shall manage the communication between the IP Serial Input Sub-Controller connected to the system's inputs and outputs. The IP Serial Input Sub-Controller shall be connected to IP Door Controller using RS-485 protocol. Each IP Serial Input Sub-Controller shall have the following capabilities:

1. General Input 16 (programmable)
2. Dedicated Input 2
3. Relay Outputs 2
4. Connectivity RS-485

H. The Serial Output Sub-Controller shall make and manage access control decisions with data provided by the MonitorCast v4 Server through the IP Door Controller, and it shall manage the communication between the IP Serial Output Sub-Controller connected to the system's inputs & outputs. The IP Serial Output Sub-Controller shall be connected to IP Door Controller using RS-485 protocol. Each IP Serial Output Sub-Controller shall have the following capabilities:

1. General Output 16
2. Dedicated Inputs 2
3. Connectivity RS-485

2.4 HARDWARE PACKAGING REQUIREMENTS

The security management system shall have various hardware enclosures and configurations available to support different installation requirements. Enclosures shall be available for wall or rack mounting. The wall-mount enclosures shall have a lock requiring a key.

2.5 MONITORCAST V4 SERVER AND IP DOOR CONTROLLER SPECIFICATIONS

A. The MonitorCast v4 Server shall be powered by platinum efficiency hot plug redundant 495 W or 750 W power supply.

1. OS Windows Server 2008 R2/2012
2. Storage 200 GB (minimum)
3. Processor Intel I5 class processor or higher
4. RAM 8 GB
5. Ethernet Ports 1
6. Warranty 3 Years

B. Each IP Door Controller shall be powered by PoE in accordance with IEEE 802.3af standard. With PoE as the power source the total power available for all external outputs is 12V DC @ 650mA. IP Door Controllers shall have the following characteristics:

1. TTL reader connectors 2

2. RS-485 reader connectors 1
3. Power available for output 650 milliamps
4. Input connectors 2
5. Output connections 2

C. Each IP Door Sub-Controller shall be powered by PoE in accordance with IEEE 802.3af standard. With PoE as the power source the total power available for all external 12V. IP Door Controllers shall have the following characteristics:
1. TTL reader connectors 1
2. Power available to readers 150 milliamps
3. Input connectors 4
4. Output connections 2

D. Each Single Door Sub-Controller shall be powered by may be supplied with 12-24V DC at 3 amps. With a 12V DC 3A power supply the total power available for all external output shall be 1100mA (13 watts). IP Door Controllers shall have the following characteristics:
1. TTL reader connectors 1
2. Power available to readers 150 milliamps
3. Input connectors 3
4. Output connections 2
5. Communication protocol RS-485

E. Each Two Door Sub-Controller shall be powered by may be supplied with 12-24V DC at 3 amps. With a 12V DC 3A power supply the total power available for all external output shall be 1100mA (13 watts). IP Door Controllers shall have the following characteristics:
1. TTL reader connectors 2
2. Power available to readers 150 milliamps
3. Input connectors 10
4. Output connections 6
5. Communication protocol RS-485

F. Each Serial Input Sub-Controller shall be powered by may be supplied with 12-24V DC at 3 amps. With a 12V DC 3A power supply the total power available for all external output shall be 1100mA (13 watts). IP Door Controllers shall have the following characteristics:
1. General Inputconnectors 16
2. Dedicated Input connectors 2
3. Output connections 2
4. Communication protocol RS-485

G. Each Serial Output Sub-Controller shall be powered by may be supplied with 12-24V DC at 3 amps. With a 12V DC 3A power supply the total power available for all external output shall be 1100mA (13 watts). IP Door Controllers shall have the following characteristics:
1. General Output connectors 16
2. Input connections 2
3. Communication protocol RS-485

2.6 SOFTWARE REQUIREMENTS

A. Operating System and Application Software shall have the following characteristics:
   1. The MonitorCast v4 Server operating system shall Windows Server 2008 R2 or Windows Server 2012 operating system.
   2. The system database shall be SQL Server Express requiring a small footprint and providing high reliability. The MonitorCast v4 Server shall provide users with access and operate the system using a standard web browser.
   3. The system shall support the following web browsers:
      a. For the security management system, the listed browsers shall include Internet Explorer, Firefox, Chrome and Safari.

B. Software Licensing shall have the following characteristics:
   1. Software licensing shall be based upon the number of cameras licenses you have per server and individual lifetime licensing in situations where doors out number cameras at the project site.
   2. Licensing shall be controlled by a Serial Key and an Activation Code. The Serial Key shall contain the licensed system limits. System upgrade licensing to enable more cameras or more doors shall require a Serial Key re-activation. The key shall be locked to the system license number.

C. Software upgrades shall be possible from a browser on any network-connected PC, by uploading a software update to the IP Door Controller. No client software installation shall be necessary.

D. Online Help and Documentation - The system shall be provided with complete online documentation. The online documentation shall include:
   1. Technical Support Notes - These documents shall be in PDF format, shall be printable, and shall be linked to from the Help system table of contents, index, and related topics.
   2. Installation Guides - These documents shall be in PDF format, shall be printable, and shall be linked to from the Help system table of contents, index, and related topics.
   3. Video Integration Guides - These documents shall be in PDF format, shall be printable, and shall be linked to from the Help system table of contents, index, and related topics.
   4. End-User Task Guide - This document shall be in PDF format, shall be printable, and shall be linked to from the Help system table of contents, index, and related topics.

E. Language Support - The system shall be provided with multiple language support. The ability to switch from one language to another shall be accomplished through the user interface. Translation of the user interface, online help and documentation into other languages shall be available. The languages supported shall include:
   1. English

F. Date Formats - The system shall support global date formats as follows:
   1. mm/dd/yyyy
   2. dd/mm/yyyy
   3. yyyy/mm/dd

G. Floor plans - The system shall provide graphic floorplan capability including graphic display of door status and entry direction. Floor plans shall have the following characteristics:
   1. The Network Administrator shall be able to graphically configure device icons onto the floorplan images, and to upload additional floorplan images. JPEG images shall be supported, and the maximum size for a floorplan image shall be 256K.

H. Personnel Data - The system shall maintain person data relating to access control, system user privileges, photo identification, system activity, and contact information.
   1. All person data in the system shall be integrated onto one page for viewing, editing, and deletion by system users.

2. A system user holding at least an "Administrator" user role shall be able to create, delete, and modify person records, including access levels, schedules & resource groups.
3. A system user holding at least a "Administrator" user role shall be able to configure the display of person records.

I. Access Control:
1. The system shall be able to make access control decisions, define a variety of access levels and time specifications, write system activity into a log file, maintain a personnel enrollment database, receive signals from input devices such as door switch monitors, card readers and motion detectors, energize devices such as door locks and alarms via outputs.
2. Card Formats - The system shall support the use of readers that use the Wiegand Reader Interface. The system shall also support the use of the Magnetic Stripe ABA track 2 card data formats.
    a. It shall be possible to create new card formats, designate start bits and bit lengths for facility codes and card ID numbers, as well as designate parity bits. The system shall support up to 32 different card formats.
3. Access Levels - The system shall be capable of storing unlimited access levels in each partition.
    a. The definition of an access level shall require the assignment of a reader or reader group, and a time specification.
4. First-in Unlock Rule - The system shall support the use of a First-in unlock rule. It shall be possible to use this rule to control the unlock behavior of portal groups with assigned unlock time specs.
    a. The First-in unlock rule shall require a card read of a specified access level. The portals in the group shall unlock only when the rule is satisfied and the unlock time spec is valid.
5. Holidays - The system shall be capable of storing up to 5 holidays per system. Each holiday shall be assigned a unique alphanumeric name. The definition of a holiday shall require a start date and an end date. Holidays shall have the ability to span several days using only one holiday slot. Holiday definitions shall support the designation of a start time and an end time. If no start time is designated, then the system shall default to 00:00 (start-of-day). If no end time is designated, then the system shall default to 24:00 (end-of-day). Holidays shall require the use of 24-hour time format, e.g. 17:00 is 5:00PM.

J. Reports:
1. The system shall be capable of producing a variety of predefined reports regarding software and security hardware configuration, event history, and the administration of people within the system.
2. The system shall support a graphic interface for interactively building custom reports from either historical or personnel data. These reports shall be savable for later reuse. Parameters shall be inserted into reports to prompt for data input at report runtime. Report results shall be printed, output to a PDF file or put into a spreadsheet.
3. The system shall be capable of sorting users by various criteria, including email address, and allow for email groups to be selected for auto-distribution.
4. Report generation shall not affect the real-time operation of the system.
5. The specific reports provided shall include the following:
    a. Configuration Reports
        i. Access History - Displays access history based on an entered query. The system user can specify the query using either the keyboard or point-and-click selection.
        ii. Custom Report - This provides the capability to create custom reports of historical data.
        iii. General Event History - Displays time, type of activity, and activity details for a variety of event types. The system user can select the specific event types for the report.

iv. Audit Trail: Displays an audit trail of system changes and the name of the system user that made the changes. It shall be possible to specify the dates and times covered in the report.

b. People Reports

i. Access Levels - Displays all access levels entered into the system including time specification, reader/reader group, and floor group.

ii. Credential Audit - Lists existing credentials by their current status settings (such as Active, Damaged, Lost, or Not Used). Before running the report, users can filter the data to see only credentials with a particular status setting, or only credentials that were not used with a specific number of days from the date they were issued.

iii. Current Users - Displays a list of all security system users currently logged in to the security system website.

iv. Custom Report - This provides the capability to create custom reports of personnel data. A graphic interface provides the user with the ability to interactively create and save reports for later use. Parameters can be inserted into reports to prompt for data input at report runtime. Custom report configuration shall include page size, orientation, column width and shall automatically notify the user if the selected configuration exceeds the selected page size.

K. Administration - The system shall provide for the performance of system administration tasks from any network-connected computer with a browser. These administrative tasks shall include but not be limited to:

1. Generating reports:
   a. The system shall be capable of producing a variety of predefined reports regarding software and security hardware configuration, event history, and the administration of people within the system.
   b. Alternatively, the system shall support a graphic interface for interactively building custom reports from either historical or personnel data. These reports shall be savable for later reuse. Parameters can be inserted into reports to prompt for data input at report runtime. Report results can be printed, output to a PDF file or put into a spreadsheet.
   c. A system user holding "Administrator" permissions shall be able to view and create reports.
2. Database backups:
   a. It shall also be possible for the system users to create such database backups at any time. Any database backups onboard the MonitorCast v4 Server may also be downloaded to IP Door Controller storage by the system user at any time.
3. System restore:
   a. The system shall be able to restore its database, or the full system data, from a backup. Restoration of the system shall only be possible from a backup copy onboard the MonitorCast v4 Server. It shall, therefore, be possible to upload a copy of a database backup from any network attached storage.
4. Software updates:
   a. Software updates, upgrades and patches shall be provided from time to time. The system shall be able to update its software from these files. Update of the application software shall only be possible from an update file onboard the Server. It shall, therefore, be possible to upload a copy of the software update from any network attached storage or from any PC drive or desktop.

b. Software updates may involve the Server only or may include updates for the IP Door Controller also. The monitoring of the security system may be unavailable for several minutes during this process.

5. Enrolling new people - All person data entered into the system shall be held in the system database and shall be available only to system users holding at least the Administer user role. Person data can be added, deleted, and edited by such system users.
6. Configuring network resources:
    a. DNS - The system shall support setting IP addresses for up to two domain name MonitorCast v4 Servers.
    b. Email settings - The system shall support the use of email notifications of alarm events. The system user must setup the email MonitorCast v4 Server IP address or DNS name and the email address of the Network Controller. A network administrator must setup the network mail MonitorCast v4 Server to relay email for the IP address of the Network Controller.
    c. Time MonitorCast v4 Servers - The system shall support the use of network time MonitorCast v4 Servers. Up to three MonitorCast v4 Servers can be designated. Use of a network time MonitorCast v4 Server ensures that the Network Controller and its nodes will be regularly synchronized with the exact time used by all other network resources.
    d. A system user holding "Setup" permissions shall be able to configure network resources.
7. LDAP - It shall be possible to configure an Active Directory MonitorCast v4 Server with the system.
    a. This shall provide single user-login capability.
    b. Password rules and authentication shall be governed by the LDAP MonitorCast v4 Server.

2.7 CERTIFICATIONS

A. UL 294 listed.
B. ISO 9000 listed.
C. CE Compliant.
D. RoHS.