INVITATION TO BID
BID NO. 9758
INTEGRATED SECURITY MANAGEMENT SYSTEM
FOR TROY SCHOOL DISTRICT

The Troy School District will receive firm, sealed bids for furnishing, delivering and installing an Integrated Security Management System for Troy Schools.

Specifications and proposal forms can be obtained online at http://www.troy.k12.mi.us. From the main page click the "Business Services" tab listed under "Departments", then click "Purchasing" and go into the "Current Bids" tab, scroll down to locate and access the bid document.

Your proposal and three copies marked **"Integrated Security Management System"** must be delivered no later than 2 p.m., Monday, April 29, 2013 to: Purchasing Department, Troy School District, 1140 Rankin, Troy, Michigan 48083, at which time all bids will be publicly opened and read aloud immediately thereafter. Bid proposals received after this time will not be considered or accepted.

All questions regarding the bid specified, or the bid terms and conditions will be accepted in writing ONLY and subsequently answered through an addendum to all interested parties. Any questions must be received no later than noon, Monday, April 22, 2013, at no other time prior to the bid opening will questions/concerns be addressed or accepted and may be faxed to: 248.823.4077, or emailed as a Word document to: PurchasingOffice@troy.k12.mi.us.

The Troy Board of Education reserves the right to accept or reject any or all bids, either in whole or in part; to award contract to other than the low bidder; to waive any irregularities and/or informalities; and in general to make awards in any manner deemed to be in the best interest of the owner.

Purchasing Department
Troy School District
1140 Rankin
Troy, MI 48083

INSTRUCTIONS TO BIDDERS

PROPOSALS

1. Firm, sealed proposals will be received by the Troy School District, for furnishing, delivering and installing an Integrated Security Management System for the District, in accordance with the attached specifications.

2. Proposals will be submitted only on the forms provided, will be enclosed in a sealed envelope marked with the name of the bidder, the title of the work and must be delivered to the Purchasing Department, Troy School District, 1140 Rankin, Troy, Michigan 48083, no later than 2 p.m., Monday, April 29, 2013, at which time all bids will be publicly opened and read aloud immediately thereafter. Bid proposals received after this time will not be considered or accepted. Oral, telephone, fax or electronic mail bids are invalid and will not receive consideration. Submit one original and three copies.

3. Proposals will be made in conformity with all the conditions set forth in the specifications. All items of furniture and equipment must conform to the specifications.

4. All questions regarding the bid specified, or the bid terms and conditions will be accepted in writing ONLY and subsequently answered through an addendum to all interested parties. Any questions regarding bid specifications must be received no later than noon, Monday, April 22, 2013, at no other time prior to the bid opening will questions/concerns be addressed or accepted and may be faxed: 248. 823.4077, or emailed as a Word document to: PurchasingOffice@troy.k12.mi.us.

5. References in the specifications to any article, product, material, fixture, form or type of construction, etc., by proprietary name, manufacturer, make or catalog number will be interpreted as establishing a standard quality of design and will not be construed as limiting proposals.

6. The Troy Board of Education reserves the right to accept or reject any or all proposals either in whole or in part; to waive any irregularities and/or informalities; and in general to make awards or cancel this proposal, if deemed to be in the best interests of the owner.

7. A completed Familial Disclosure form must be included with each proposal submitted of the proposal will not be accepted, please note this form must be notarized.

INSURANCE

Satisfactory Workers' Compensation coverage of at least $2,000,000.00 and General Liability and Property Damage Insurance of at least $2,000,000.00 per occurrence and $2,000,000.00 in Aggregate must be carried and paid for by the contractor(s) who undertakes the work on this contract. Insurance coverage must also include automobile insurance of at least $2,000,000.00. Bid number and Troy School District as additional insured must be noted on the insurance certificate. Certificate holder will be Troy Schools.

GUARANTEE BONDS

Prior to the issuance of a purchase order authorizing commencement of this project, and in all cases before beginning work under the contract, the Vendor/Contractor(s) selected will qualify for, sign and deliver to the Purchasing Office, an executed performance bond and executed labor and materials payment bond secured by the surety company. Each bond will be in the amount of 100 percent of the contract. Troy Schools requires that the bonding companies be limited to those listed on the U.S. Department of Treasury Circular 570, and must be licensed in the State of Michigan. The U.S. Department of Treasury Circular 570 can be viewed at the following web site: http://www.fms.treas.gov/c570/c570.html. Certificates of such insurance and bonds will be filed with the Purchasing Office within five working days of notification of bid award and before any work begins**.**

TAXES

State and local sales and use taxes are not applicable and will not be included in the proposal.

CONTRACT AWARD

The contract will be awarded in the form of a **PURCHASE ORDER** mailed to the Vendor/Contractor(s) selected. It is the intent to award the bid on May 7, 2013 at the regular monthly meeting of the Board of Education.

WITHDRAWAL OF BIDS

Any bidder may withdraw their bid at any time prior to the scheduled time for receipt of bids. Proposal will be held open and irrevocable for forty-five (45) days after receipt of bids.

WARRANTY

All material and equipment will be guaranteed to be free from defects in both workmanship and materials for no less than one year from date of receipt/installation. If manufacturer warranty exceeds this minimum requirement, the manufacturer warranty will prevail. Any item(s) found to be defective will be replaced or repaired within 10 working days at the Vendor/Contractor(s) expense.

PAYMENTS

Payment in full will be due and payable within thirty days after delivery, providing all goods are approved and accepted by the Troy Board of Education and the contract having been fully performed.

VENDOR LIST

Bidders not responding with a sealed bid or notification of a "No Bid" will be removed from the vendor bid list.

MSDS

COPIES OF MATERIAL SAFETY DATA SHEETS FOR ALL HAZARDOUS MATERIALS MUST BE INCLUDED WITH YOUR INVOICE.

MATERIAL SAFETY DATA SHEETS

The Troy School District expects MATERIAL SAFETY DATA SHEETS for all appropriate materials ATTACHED TO THE INVOICE and to appropriately label all products delivered according to Section 14 of Act 154, of the Public Acts of 1974 as amended. Any appropriate products not labeled will be refused and the vendor will be responsible for additional freight charges. Payment may be withheld until MSDSs are received by the school district.

Integrated Security Management System – Specifications

Bid Package 9758

PART 1 GENERATION

1.01 Work Scope

This bid package is not intended to replace or modify existing security systems and/or services already being utilized by Troy School District. Equipment specified in this bid package should not be restricted to authorized dealers only; although dealers must be trained by the manufacturer. The components to be utilized (listed on page 34) have been selected based on availability through common distribution channels, existing and future needs of the District and can be serviced/maintained by a multiple number of vendors now and in future. The bidders are to provide a modular and network-enabled access control system for security management, including engineering, supply, installation, and activation. The installation process can't interfere with the daily operations or educational programs.

- Page 32 – Estimated Cable Runs
- Page 33 – Building Addresses
- Page 34 thru 35 – Video/Intercoms and Proximity Card Readers Door Location. Small Yellow/Black number tag has been displayed on each door.
- Page 36 – Minimum Required Equipment List
    - If you are bidding alternate equipment that is equal to the equipment specified you will be required to provide a manufacturer cut-sheets and general advertisement brochures.
- Page 37 thru 53 – Google Earth Maps and Door Structures at each facility.

1.02 Reference Standard

A. Must have a minimum of 10 years' experience in the installation of projects of this scope. Systems specified in this Section shall meet or exceed the requirements of the following:

B. Standards: Systems specified in this Section shall meet or exceed the requirements of the following:

1. Federal Communications Commission (FCC):
    a. FCC Part 15 – Radio Frequency Device
    b. FCC Part 68 – Connection of Terminal Equipment to the Telephone Network
2. Underwriters Laboratories (UL):
    a. UL294 – Access Control System Units
    b. UL1076 – Proprietary Burglar Alarm Units and Systems
3. National Fire Protection Association (NFPA):
    a. NFPA70 – National Electrical Code
4. Electronic Industries Alliance (EIA):

a. RS232C – Interface between Data Terminal Equipment and Data Communications Equipment Employing Serial Binary Data Interchange

b. RS485 – Electrical Characteristics of Generators and Receivers for use in Balanced Digital Multi-Point Systems

5. Federal Information Processing Standards (FIPS):

a. Advanced Encryption Standard (AES) (FIPS 197)

1.03 Integrated Security Management System Description

A. The Integrated Security Management System (ISMS) shall function as an electronic access control system and shall integrate alarm monitoring, CCTV, digital video, ID badging and database management into a single platform. ISMS shall function as a one-stop gateway for all the access control needs. A modular and network-enabled architecture shall allow maximum versatility for tailoring secure and dependable access and alarm monitoring solutions.

1.04 Submittals

B. Manufacturer's Product Data: Submit manufacturer's data sheets indicating systems and components proposed for use.

C. Shop Drawings: Submit complete shop drawings indicating system components, wiring diagrams and load calculations.

D. Record Drawings: During construction maintain record drawings indicating location of equipment and wiring. Submit an electronic version of record drawings for the Security Management System not later than Substantial Completion of the project.

E. Operation and Maintenance Data: Submit manufacturer's operation and maintenance data, customized to the Security Management System installed. Include system and operator manuals.

F. Maintenance Service Agreement: Submit a sample copy of a maintenance service agreement, including cost and services for a two year period for Owner's review.

1.05 Quality Assurance

A. Contractor: Minimum ten years' experience in design, engineering, installation of Security Management Systems.

B. Work areas must be kept safe, clean and organized at all times.

C. Contractor will be responsible for any and all damage caused during the installation process.

D. Hours of work will require prior approval from the Director of Operations and are based on school events.

1.06 Delivery, Storage, and Handling

1.06.1 Deliver materials in manufacturer's labeled packages. Store and handle in accordance with manufacturer's requirements.

1.06.2 The District will not be responsible for providing a secured area to store or stage equipment. Loss or stolen will not be covered under this agreement.

1.07 Warranty

1.07.1 Manufacturer's Warranty: Submit manufacturer's standard warranty for the security management system.

1.08 Definitions

1.08.1 Access Card: A coded employee card, usually the size of a credit card, recognizable to the access control system and read by a reader to allow access. It can be used for photo identification of the cardholder and for other data collection purposes. Card technologies include magnetic strips, wiegand-effect, proximity (active/passive), barium ferrite, and smart/intelligent cards.

1.08.2 Abstract Device: An Abstract Device (ADV) is a logical representation of a physical device. The ADVs can be associated with any hardware device, including communication interfaces, panels, alarm points, entrances, and CCTV equipment. The ADVs help in monitoring the device status and controlling the actions of a physical device through the Control Map, Floor Plan, or Alarm View.

1.08.3 Access Control System: An interconnected set of controllers, managing the entrance and exit of people through secure areas.

1.08.4 Access Level: The door or combination of doors and/or barriers an Individual is authorized to pass through.

1.08.5 Anti-Pass back (Anti-Tailgating): This feature protects against more than one person using the same card or number. It defines each system card reader and card I.D. number as IN, OUT or other. Once a card is granted access to an IN reader, it must be presented to an OUT reader before another IN reader access is granted. Cards will continue to have access to all authorized OTHER readers.

1.08.6 Alarm input: A device that is monitored by the access control panel. An alarm signal will be generated if the device is activated.

1.08.7 Badge: Badge is a template or a design for creating a card. WIN-PAK includes a full-featured badge layout utility for designing, creating, and printing badges. Badge design includes magnetic stripe encoding, bar coding, signatures, and so on.

1.08.8 Bar Code: A method of encoding information using lines and blank spaces of varying size and thickness to represent alphanumeric characters.

1.08.9 Biometrics: A general term for the verification of individuals using unique biological characteristics (i.e. fingerprints, hand geometry, voice analysis, the retinal pattern in the eye).

1.08.10 Card and Card Holder: A card is an identity proof of a person and a card holder is a person who holds the card. Multiple cards can be assigned to a single card holder to provide different access.

1.08.11 Controller: A microprocessor based circuit board that manages access to a secure area. The controller receives information that it uses to determine through which doors and at what times cardholders are granted access to secure areas. Based on that information, the controller can lock/unlock doors, sound alarms, and communicate status to a host computer.

1.08.12 Communication Port: A hardware device that allows a computer to communicate with external devices.

1.08.13 Card Reader: A device that retrieves information stored on an access card and transmits that information to a controller.

1.08.14 Digital Video Recorder (DVR): A security system device that records the video from the surveillance cameras (IP and Analog) on a hard disk.

1.08.15 Door: A generic term for a securable entry way. In many access control applications a "door" may actually be a gate, turnstile, elevator door, or similar device.

1.08.16 Duress: Forcing a person to provide access to a secure area against that person's wishes.

1.08.17 Guard Tour: A defined route of a security guard.

1.08.18 Host Computer: The central controlling computer from which access control software applications are run.

1.08.19 Input: An electronic sensor on a controller that detects a change of state in a device outside the controller.

1.08.20 Keypad: An alphanumeric grid which allows a user to enter an identification code. A flat device which has buttons that may be pressed in a sequence to send data to a controller, and which differs from a typewriter-like computer board.

1.08.21 Online Help: A reference program within most software programs that provides basic descriptions and instructions on how to use that software program.

1.08.22 Output Relay: A device that changes its state upon receiving a signal from a controller. Typically the state change prompts an action outside of the controller such as activating or inactivating a device. The auxiliary relays found in access control panels or NODES that control external devices.

1.08.23 Reader: A device that "receives" an identification code from a card, key tag, magnetic stripe card, bar code card, or related item. Refers to the “front end” that a user must interact with to allow access. Readers can be keypads, card readers, proximity readers, and so on.

1.08.24 RS232: A serial communication protocol used for connecting data terminal devices. RS-232 is the most commonly used communication protocol.

1.08.25 Server: The host computer, which has the ISMS functions.

1.08.26 Shunt Time: The length of time a door open alarm is suppressed (shunted) after a valid card access or free egress request. This time should be just enough to allow a card user to open a door or gate, pass through, and then close it.

1.08.27 Time zones: "Schedules" that allow cards to function or not function depending on the time of day. This is used to limit access to the facility. The schedule may include not only time but which days of the week a card is valid.

1.08.28 Wiegand Card: An access control card based on the Wiegand effect. Small bits of specially processed wire are embedded in the card in a pattern that uniquely identifies the card. This identification information can then be decoded by a Wiegand reader.

1.08.29 Wiegand Reader: A reader capable of reading the information encoded on a Wiegand card.

1.08.30 Video Management System (VMS): An enterprise-class video management and storage solution.

PART 2 PRODUCTS

2.1 Manufacturer

1. Integrated Security Management System Manufacturer: WIN-PAK Access Management System by Honeywell, www.honeywellaccess.com.

   a. Standard Edition (SE) shall include the following features: Single user intrusion integration license, one communication server, un-restricted readers, un-restricted card holders, NetAXS-123, NetAXS-4, digital video integration with Fusion, RapidEye™, MAXPRO® NVR XE/SE, HRDP and HRDP H.264.

2.2 ISMS Components

The ISMS shall be divided into three components: Database Server, Communication Server, and User Interface. These components shall run on a single computer or on multiple computers, allowing flexibility in configuring a networked system.

a. Database Server: The database server is used for storing the database tables. This data is accessible to communication server and user interface for retrieving and generating the reports. The database server shall be installed on the client computer or any other computer connected to the network.

b. Communication Server: The communication server routes user interface requests as well as the access transactions to the panel. The panel in-turn processes the transactions and sends the information to the database server as well as responses to the user interface through the communication server. When the communication server is sending information to the database server, it can also receive a request from the user interface. In this scenario, the communication server considers the user request as a higher priority and stops the panel-database server communication until the user request is processed. The communication server shall be installed on the client computer or any other computer connected to the network.

c. User Interface (ISMS Client): The user interface helps ISMS operators to communicate with the access control system. The user interface shall be installed on the computer where the database server or the communication server is installed or any other computer connected to the network. Several client computers can be run simultaneously and can access the single database server simultaneously. The number of client computers varies based on the licensing information of ISMS.

In addition to above three components, ISMS includes the following four components, also called as ISMS services.

d. Command File Server: A command file server provides text files containing device instructions that shall be stored in the command files database. The commands in the command files can be sent to the devices automatically on receiving, acknowledging, or clearing an alarm. The command files can also be executed manually.

e. Guard Tour server: A guard tour is a defined series of check points a guard must activate within a given amount of time. The check points are readers or input points where the guard presents the card or presses the button.

f. Tracking and Muster Server: A muster server is enabled in the event of an emergency and allows the card holders to swipe the readers. Muster areas are logical areas that contain readers to be used by the card holders, only if there is a call for muster (in the event of a disaster, for example).

g. Schedule Server: A schedule server schedules the list of events to be performed at predetermined time and intervals such as hourly, daily, or monthly.

h. Video Management Server: A video management server provides interface to connect to various DVR's/NVR's. In addition, it also provides CCTV control with live monitor display, PTZ control of cameras, video playback operations, and so on.

2.3 <u>Integrated Security Management System Operational Requirements</u>

A. The ISMS shall be a modular and network-enabled access control system capable of controlling multiple remote sites, alarm monitoring, video imaging, ID badging, paging, digital video and CCTV switching and control that allows for easy expansion or modification of inputs and remote control stations. The ISMS control at a central computer location shall be under the control of a single software program and shall provide full integration of all components. It shall be alterable at any time depending upon facility requirements. The ISMS reconfiguration shall be accomplished online through system programming. The ISMS shall include the following features:

1. Multi-User/Network Capabilities: The ISMS shall support multiple operator workstations via local area network/wide area network (LAN/WAN). The communications between the workstations and the server computer shall utilize the TCP/IP standard over industry standard IEEE 802.3 (Ethernet). The communications between the server and workstations shall be supervised, and shall automatically generate alarm messages when the server is unable to communicate with a workstation. The operators on the network server shall have the capability to log on to workstations and remotely configure devices for the workstation. Standard operator permission levels shall be enforced, with full operator audit.
2. Operating Environment: The ISMS shall be a true 32-bit or 64-bit, 3-tier client/server, ODBC compliant application based on Microsoft tools and standards. The ISMS application shall operate in the following environments: Microsoft Windows® Server 2008 R2 SP1, Microsoft Windows® 7 SP1 (64-bit).
3. Multiple Servers: The ISMS shall consist of multiple servers including, but not limited to, database server, communications server, and client workstation. The servers shall be capable of being installed on one or more computers across a network providing a distribution of system activities and processes. The ISMS shall support multiple communication servers on a LAN/WAN, to provide distributed networking capabilities, which significantly improve system performance.
4. Multi-level Password Protection: The ISMS application shall provide multi-level password protection, with user-defined operator name/password combinations. Name/password log-on shall restrict operators to selected areas of the program. The application shall allow the assignment of operator levels to define the system components that each operator has access to view, operate, change, or delete.
5. Graphical User Interface: The ISMS shall be fully compliant with Microsoft Graphical User Interface (GUI) standards, with the look and feel of the software being that of a standard Windows application, including hardware tree-based system configuration.
6. Online Help: The ISMS user interface shall include an Online Help which shall require only one click to activate. The standard special function key “F1” shall have the capability to be programmed to provide access to the help system.
7. Guard Tour: The Security Management System shall include a guard tour module, which shall allow the users to program guard tours for their facility. The tours shall not require the need for independent or dedicated readers.
8. Concurrent Licensing: The ISMS shall support concurrent client workstation licensing. The ISMS application shall be installed on any number of client workstations, and shall provide the ability for any of the client workstations to

connect to the database server as long as the maximum number of concurrent connections purchased has not been exceeded.

9. Relational Database Management System: The Security Management System shall support industry standard relational database management systems. This shall include relational database management system Microsoft SQL Server 2008 R2 Enterprise Edition. The RDBMS shall provide edit, add, delete, search, sort, and print options for records in the selected databases.
10. Database Partitioning: The Security Management System shall provide the option to restrict access to sensitive information by user ID.
11. Unicode: The Security Management System shall utilize Unicode worldwide character set standard. The Security Management System shall support double-byte character sets to facilitate adaptation of the Security Management System user interface and documentation to new international markets. Language support shall include at a minimum English and French.
12. Encryption: The Security Management System shall provide multiple levels of data encryption
    a. True 128-bit AES data encryption between the host and intelligent controllers. The encryption shall ensure data integrity that is compliant with the requirements of FIPS-197 and SCIF environments. Master keys shall be downloaded to the intelligent controller, which shall then be authenticated through the Security Management System based on a successful match.
    b. Transparent database encryption, including log files and backups.
    c. SQL secure connections via SSL.
13. Industry Standard Panel Communication: The ISMS application shall communicate with the access control panels via LAN/WAN connections utilizing industry standard communication protocols.
14. Supervised Alarm Points: The system shall provide both supervised and non-supervised alarm point monitoring. Upon recognition of an alarm, the system shall be capable of switching and displaying the video from the camera connected to the digital video recorder that is associated with the alarm point.
15. Multiple Account Support: The ISMS application shall allow support for multiple accounts allowing separate access to the card database, badge layout, operator access, and reporting. Physical hardware may be filtered by operator level into sites. Sites may reside in multiple accounts. The system shall allow control of common areas between accounts. Access levels and time zones shall be global to allow for easy administration. The global access levels and time zones shall be capable of being used by several accounts. Administrators shall have the ability to move cardholders from one account to another. When moving cardholders in such a manner, access level information shall not be transferred automatically in order to ensure proper security settings are made upon changing the status of the cardholder.
16. Logical Representation of Hardware Devices: The ISMS shall use Abstract Devices (ADV) for representing physical hardware devices in the system. The ADVs shall be used in Floor Plans to provide the user interface to control and

monitor the system, and shall also be used in the data trees to organize, display, and control system information.

17. Access Control Functions: The ISMS shall include the following access control functions: validation based on time of day, day of week, holiday scheduling, site code and card number verification, automatic or manual retrieval of cardholder photographs, and access validation based on positive verification of card type (VIP, Supervisor, Standard), card, card and PIN, card or pin, pin only and Site Code only.
18. Digital Video Recorders (DVRs) Support: The ISMS shall support live video streaming from cameras connected to supported DVRs.
19. Camera Functions: The ISMS shall include the following camera functions: pan/tilt, lens control, limits, and home.
20. Live Video Display: The ISMS shall provide an option to view live video from a camera connected to the digital video recorder on the computer screen. The live video window shall allow the user to change its size and location on the computer screen. Video controls (pan, tilt, zoom) shall be available to customize the display of live video to the user's requirements.
21. Global and Nested Anti-passback: The Security Management System shall support the use of an optional anti-passback mode, in which cardholders are required to follow a proper in/out sequence within the assigned area.
22. Alarm Events: The ISMS shall include a feature where alarm events with defined priorities shall be able to pop-up automatically in an Alarm event window for operator attention. The pop-up shall display the name of the event (reader, alarm point, cardholder, or system alarm), time, date, site, account, if a card event the card number, type of event and cardholder name. An event counter shall also display the number of times the event was reported to the Alarm event monitor prior to Acknowledgement or Clearing the event. Event instructions shall be made available by double clicking on the event. The event shall also display an icon to indicate that video is available for events so programmed. The Alarm event window shall allow the operator to initiate a physical response to the event as well as a written response. Responses shall include but not be limited to: acknowledge, clear, open a pre-programmed floor plan, energize, de-energize, pulse, time pulse, add comment, retrieve time sensitive video, bring up live video, shunt, or un-shunt.
23. Manual Panel Control: The ISMS application shall allow manual control of selected inputs, outputs, and groups of outputs. Manual panel control shall include pulse, timed pulse, and energize/de-energize or return to time zone options for output points and shunt/un-shunt, set time zone or return to time zone options for input points. For entrances and readers manual control shall include but be limited to Lock, Un-Lock, Disable, Card only, Card-Pin only, Pin only, exit only and site code only. For partitions monitored by the intrusion panel the control shall include but not be limited to arm away, arm stay, disarm, refresh, and provide a virtual keypad for the partition. For zones monitored by the intrusion panel the control shall include but not be limited to

bypass, unbypass, and refresh. Intrusion panel output control shall included activate, deactivate and refresh.

24. Levels of System Operation: The ISMS shall include a feature to define the levels of system operation for each individual operator using passwords. System operation for individual operators shall include, but not be limited to, restricted time periods for login, available accounts and default language selection at login. Operator actions range from no view or control rights to basic monitoring including the ability to block the viewing of card and or personal identification numbers, to full control of the system including programming.
25. User-Friendly Quick Start Wizard: The system programming shall be user friendly and capable of being accomplished by personnel with no prior computer experience The ISMS shall include a quick start wizard that allows an operator to easily program a system including basic time zones, access panels (IP connection, Modem Pools, or direct connections to an RS-232 port). The software shall utilize drop boxes for all previously entered system-required data. The programming shall be MENU driven and include Online Help. The Online Help shall be available by pressing the F1 key. When using the F1 help access, the help menu will provide detailed information relative to the operation that the user is performing without the need to key in additional search parameters.
26. Hardware Configuration Changes: After installation of ISMS application, the customer shall be able to perform hardware configuration changes. These hardware configuration changes shall include, but not be limited to, door open time, door contact shunt time, point and reader names, when and where a cardholder is valid, and the ability to add or modify card databases as desired; For the intrusion system, any control function that can be generated from a physical keypad shall also be available from the system's virtual keypad, without the services of the Contractor or Manufacturer.

27. Distributed Processing: All the control components of the ISMS shall utilize "Distributed-Processing" concepts. The distributed processing shall include the ability to download operating parameters to any field panel, thus allowing the field panel to provide full operating functions independent of the access control system computer.
28. Flexible Component replacement: The repair of hardware components associated to the ISMS shall be accomplished on site, by a new replacement, utilizing spare components.

B. The ISMS application shall have the major functional capabilities (considered essential for the system described in this specification) categorized as follows:

1. General

a. All the databases shall have the ability to add, delete, report, view, and edit information.

b. All the system transactions shall be saved in a retrievable file.

c. All the events shall be logged by date and time.

d. All the system transactions or selected system transactions shall be saved in a disk file.

e. The end-user shall have the provision to make any system configuration changes such as, but not limited to door open time, door contact shunt time, point and reader names, when and where a cardholder is valid, and the ability to add or modify card databases at any time.

f. Shall support “Global Anti-pass back”, feature allowing cardholder to enter/exit any such defined card reader on the same intelligent control panel or RS-485 drop-line consisting of 2 and 4 door controllers.

g. Anti-pass back modes shall include: hard (no forgiveness), soft (allows access but generates an alarm event) and timed for all readers on the intelligent controller, on specified reader or card for a definable period of time up to 32,000 seconds.

h. Shall support the “Duress” feature, where a PIN is used in conjunction with a card read; the numbers of digits are selected using the keypad where the PIN number is a value different from the normal PIN.

i. Shall support the “Two card holder” rule, where two valid, non-identical “cards” must be used within a 20-second period to grant access.

j. Shall have the option to display the time when a card holder using a reader has accessed (opened) the door or the card was used, but the door was not opened.

k. Shall support the “Latch mode” operation where the first card read unlocks the door and the second card read locks it.

l. Shall provide a mode of system operation that stores system commands not accepted by the hardware.

m. Shall provide a mode of system operation that requires the operator to enter a response to an event when acknowledging it from the alarm view window.

n. Shall provide a mode of system operation that allows acknowledged alarms to be automatically cleared.

o. Shall provide a mode of system operation where when an acknowledged, but not cleared event will be reissued requiring acknowledgement when the event changes to an alarm or trouble state.

p. Shall provide a mode of system operation that does not allow the operator to clear an alarm before prior to it being restored to normal.

q. Shall provide the ability for manual operator control of system output relays. The manual functions shall include the ability to energize, de-energize, return to time zone, or pulse the output relay. The pulse time shall be a programmable setting.

r. Shall provide the ability for manual operator control of system doors. The manual functions shall include the ability to define a time zone/schedule to change between the following modes of operation: Lock, Un-Lock, Disable, Card only, Card-Pin only, Pin only, exit only and further restrict to Escort required, Supervisor present or Standard modes.

s. Shall provide the ability to automatically display stored “video image” of cardholder, and switch real-time camera from CCTV or digital video server to card reader location for specific card usage.

t. The cardholder “video image” pop-up shall be activated based on a priority level set to the cardholder or reader. Information in the pop-up shall include, but not be limited to the card holder’s primary image a live video pop-up showing the person who initiated the pop-up, entrance name, time, date, cardholder name, and status. User shall be able to display up to 40 note fields. The size of the pop-ups shall be adjustable by the operator.

u. Shall support multiple card reader technology including: Proximity, Wiegand effect, Biometrics, Magnetic stripe, Bar Code, Keypad, Card/keypad (PIN), High-speed long range Vehicle ID, and Smart Card.

v. Shall provide an option for taking scheduled automatic backups of any or all database system files. A means to restore these files from a simple menu shall exist.

w. Shall provide the ability to address up to 255 serial communication ports per communication server, where each port can be configured for either hardwired, or dial-up. When configured for dial-up, any one port can support multiple dial-up locations.

x. Communication from the access control communication server to the remote intelligent control panels shall be selectable. Communication options shall be RS-232 directly to the intelligent control, via RS-485 converter, dial-up, leased line from a defined communication port or by LAN/WAN using an IP address for direct connection to the intelligent controller via network interface card. When using IP addressing it shall be un-acceptable to use a communication port converter device on the communication server side of the transmission. A minimum of 255 such IP connections shall be allowed per communication server. When using IP addressing both traditional static IP can be assigned to the remote device or reverse initiate IP addressing shall be allowed.

y. All commands and updates to the panels shall be verified and shall automatically retry if communications fail.

z. Shall provide a system scheduler that shall automatically: Call remote locations to retrieve history transactions and update panel information, including time and date, Activate or deactivate cards locally or at remote dial-up sites, Initiate a pre-programmed command event/action, Synchronize system to intelligent controller time, Run a pre-defined (template) History report, Run a pre-defined (template) Card Holder report, Card frequency report defined by reader(s), over a defined period of time with disposition options to automatically report or report and de-activate card or change the access level of the card, Frequency shall be defined as Never, Now, Once, Hourly, Daily, and Weekly, Once per 2 weeks, and Monthly.

aa. Shall provide drop boxes for all system-required information that the user has previously entered.

bb. Shall provide the ability to initiate an email (via SMTP) or page to a paging system based on a transaction state. A transaction state shall be defined as but not limited to Normal, Alarm, Trouble, Ajar, Trace, Not Found, Anti-Pass back Violation, Escort access granted, Supervisor Authenticated, Supervisor modes, PIN Violation, Time Zone Violation, Site Code Violation, Door Used, Duress, No Second Card Presented, VIP Card, Trace Card or Expired Card, and System Alarms including, Panel Com, Panel Power Failure, Modem Pool, Guard Tour, and Tamper. Intrusion partition events including but not limited to: Alarm, Alarm Cancel, Arm Away, Arm Stay, Auto Arm, Auto Disarm, Bypass, Disarm, Early Arm, Early Disarm, Fail to Arm, Fail to Disarm, Normal, Not Ready, Part Arm, Quick Arm, Recent Close, Remote Arm, Remote Disarm, Unbypass, User Code Added, User Code Deleted, user Code Edited. Intrusion zone events including but not limited to: Alarm, Alarm Restore, Bypass, Fault, Fault Restore, Normal, Trouble, Trouble Restore, and Unbypass. Intrusion output events including but not limited to: Alarm, Communication Loss, Normal, Tamper, and Tamper Restore. Intrusion panel events including but not limited to: Access Denied, Automatic Test, Comm Fail, Comm Restore, Faults, Faults Restore, Line Restore, Line Trouble, Manual Test, Pager Restore, Pager Trouble, AC Restore, AC Trouble, Alarm, Battery Low, Battery Low Restore, Disarm, Normal, Recent Close, Reset, Panic Alarm, Power Up, Program begin, Program Changed, Program End, System Shutdown, System Shutdown Restore, Tamper Alarm, Tamper Restore, Test End, Test Start, Time/Date changed. Video events including but not limited to: Camera Blind, Camera Blur, Car parked in handicapped zone, Clear Storage, Clear Stream, Configuration Modification, Counted as entering, Counted as exiting, Counted in lane, Entered lot, Entered restricted zone, Entered target zone, Excessive System Clock Drift, Exited lot, Exited restricted zone, Input Alarm, Input Normal, Left unattended, Loitering in restricted zone, Made illegal U-turn, Motion Detected, Needs assistance, No Synchronization in 24 Hours, No Video Recording, On fence line, Output, People converged, People passed by, Possible theft, Pulled off the road, Reboot, Recorder Connected, Removed, Rule Engine Action Triggered, Running, Running in the wrong direction, Runtime Failure, S.M.A.R.T. Disk Failure, Security Modification, Self Restart, Session Connected, Speeding, Started moving in wrong direction, Staying in target zone, Stopped moving in wrong direction, Stopped running, Storage Devices Missing, Synchronize Time, System Files Modification, Time Server Unusable, Trespassing line, Video Boost Record, Video CSD Moved and Video Signal Lock.

cc. Shall include a “host grant” mode of operation that requires the host computer to grant accesses to “valid” cards. An alternate host grant mode shall allow the card access information to be downloaded along with unlocking the door for “valid” cards.

2. Cards

a. Shall provide a simple card and card holder database import utility. The utility shall be password protected and accessible only to administrators of the access control system. Information that can be imported shall include but not be limited to: First Name, Last Name, Card Number, Activation Date, De-activation Date, Status, up to 40 note fields and Photo Images. A simple CSV (comma separated value) file shall be used for the importing of data and image file names.

b. Cardholder information shall include unique card number up to 20 digits and optional Personal Identification Number up to 6 digits.

c. Shall allow multiple cards per cardholder.

d. Shall allow 32 access levels to be assigned to a card, or a single “precision” access level. When using “precision” access levels it shall be possible to create a unique access level per card using an existing access level as a baseline template. This customized card access level shall have both beginning and ending dates.

e. Shall provide 40 user defined fields.

f. Each card holder note filed shall allow the option to be entered as free form data or structured data. Structured data shall be by use of a template or drop list. The template and drop list shall be created by the operator. The capacity of the template shall allow for up to 65,000 characters.

g. Provides special card options that shall include, but are not limited to: Time zone reference, which defines valid time, visitor use, which provides a specified activation date and expiration date (spanning years), Trigger control value, which can initiate a predefined procedure at the intelligent control independent from any control function from the system computer.

h. Shall provide a card “Trace” function. The Trace function shall allow normal access control, but will provide a tracking alarm at the system monitor.

i. Shall provide the ability to store digital images of cardholder or other digital images such as property or family members. Up to 99 such images shall be associated with the cardholder.

j. Shall provide the ability to store a written signature of the cardholder or other signatures such as family members. Up to 99 such signatures shall be associated with the cardholder.

k. Shall provide the ability to prioritize specific card usage from 1 to 99 with separate priority options shall included but not be limited to Anti-pass back, Trace, PIN Violation, Normal, Not Found, Expired, Host Grant, Site Code and Time Zone card activities or violations.

l. Shall allow the user the ability to send an e-mail message, selectable per card event type.

m. Upon editing card information, the updated information shall be sent automatically to the appropriate access control panel, when hardwired, with no other user intervention. If the port is dial-up, the entry will be stored on disk and shall be updated when connection is made to the remote loop. If the scheduler is used, then card updates shall be sent based on scheduling.

n. In a traditional (Wiegand) 5 digit card database, the numbers 0 and 65,535 shall not be valid card numbers as some devices transmit these numbers on an improper read.

o. Cards shall have the ability to be allowed to access one or selected accounts up to all available accounts.

3. Access Levels

a. Shall provide an option to define specific access times.

b. Shall provide an option to define specific readers for access.

c. Shall provide an option to select a defined grouping of relays to associate to a reader for elevator control applications.

d. Shall provide a template of a defined access level detail, where changes can be made to the template and saved as a new access level detail.

e. Shall provide an access control tree structure that allows groupings of entrances. User shall have the ability to group program all entrances on the branch or make specific changes to individual entrances.

4. Video Management Server

a. Shall provide an option to configure the DVRs to a communication server.

b. Shall provide an option to configure the cameras, inputs, and outputs to a DVR.

c. Shall provide an interface to a network of digital video servers.

d. Shall provide an option to discover all the cameras connected to the digital video servers.

e. Shall provide the ability to manually access live video from any camera on any defined digital video server.

f. The viewer windows shall allow at least 16 live videos to be displayed at one time.

g. The viewable size of the viewer salvo window shall be adjustable by using the common “click and drag” method. When adjusting height or width, the image shall retain the correct aspect ratio.

h. Shall provide the ability to automatically pop-up any camera in the system based on any alarm point, system alarm or cardholder video image pop-up.

i. Shall provide the ability to manually control the pan, tilt, and lens functions (zoom, iris, and focus) of cameras so equipped.

j. A “live view” from the Digital Video Server shall be displayed on the system computer without the use of any add in video capture card.

k. Live views shall allow for the change in image resolution or aspect ratio to optimize the viewing quality to the native video.

l. The ability to change the size and location of the view shall exist.

m. The digital video server window shall also supply the ability to select a digital video server, camera, live, from stored video using user defined time and date.

n. A filter option shall allow the operator to define a date, time, transaction type, device(s), card holder, card number, note field, card event type and alarm status. Once filtered all events will be displayed in a listing. The listing shall include on the same event line if the event has an associated video clip. By clicking on the event, the time, date, camera, and digital server shall be preloaded in the manual selection boxes allowing the operator to simply click on the sorted event and then click on “show” to display the recorded event.

5. Camera control

a. Shall provide an option to configure the settings of cameras connected to the respective DVRs.

b. Shall provide an option to manually control the pan, tilt, and lens functions (zoom, iris, and focus).

c. Shall provide an option to automatically switch any camera in the system to any monitor in the system based on any alarm point or system alarm.

d. Shall display the live and recorded video in salvo window.

e. Shall provide a set of options such as color correction, sync playback, flip, playing speed, remove text overlay and soon to customize the display of live and recorded video.

f. Shall provide an option to configure the Video Motion, Video Loss, and PTZ loss events to cameras associated to all the DVRs.

6. Alarm Monitoring – Alarms Only View

a. Shall report alarm point activity.

b. Shall provide color for each specific alarm point action, “Alarm”, “Normal”, and “Trouble”, conditions.

c. Shall provide the ability to access the default floor plan graphic for any active alarm point by a right click option.

d. Live video pop-up from the digital video server(s) shall follow the alarm event pop-up. A single alarm event shall allow up to 4 different cameras to be presented in a pop-up. If these cameras are equipped with PTZ, preset positions can be programmed per event. The number of live camera views in the pop-up window shall be no less than 16. The live pop-up window shall allow the user to define the quantity of views from 1 – 16. The ability to adjust the size of the live pop-up window shall exist.

e. Shall provide ability to bypass alarms in the system.

f. Shall execute alarm notification in all modes of operation.

g. Shall provide ability to acknowledge any intrusion alarm, event alarm, system alarm, card, or reader activity based on priority.

h. Shall provide display of system activity with the higher priorities displayed at the top of the list with identical points stacked with a frequency count of each point’s change of state.

i. Shall provide a video icon for events that have video associated with it. Right-clicking on such an event shall allow the option to retrieve recorded video or view “live”. The stored video clip shall playback by default a minimum of 2 seconds before the actual event without any adjustment.

j. Viewable alarms shall include but not be limited to access control related events such as Door Normal, Door Alarm, Door Trouble, Door Ajar; Card events such as Trace, Not Found, Anti-Pass back Violation, PIN Violation, Time Zone Violation, Site Code Violation, Door Used, Duress, No Second Card Presented, Trace Card or Expired Card, and System Alarms including, Panel Com, Panel Power Failure, Modem Pool, Guard Tour, and Tamper. Intrusion partition events including but not limited to: Alarm, Alarm Cancel, Aram Away, Arm Stay, Auto Arm, Auto Disarm, Bypass, Disarm, Early Arm, Early Disarm, Fail to Arm, Fail to Disarm, Normal, Not Ready, Part Arm, Quick Arm, Recent Close, Remote Arm, Remote Disarm, Un-bypass, User Code Added, User Code Deleted, user Code Edited. Intrusion zone events including but not limited to: Alarm, Alarm Restore, Bypass, Fault, Fault Restore, Normal, Trouble, Trouble Restore, and Un-bypass. Intrusion output events including but not limited to: Alarm, Communication Loss, Normal, Tamper and Tamper Restore. Intrusion panel events including but not limited to: Access Denied, Automatic Test, Comm. Fail, Comm. Restore, Faults, Faults Restore, Line

Restore, Line Trouble, Manual Test, Pager Restore, Pager Trouble, AC Restore, AC Trouble, Alarm, Battery Low, Battery Low Restore, Disarm, Normal, Recent Close, Reset, Panic Alarm, Power Up, Program begin, Program Changed, Program End, System Shutdown, System Shutdown Restore, Tamper Alarm, Tamper Restore, Test End, Test Start, Time/Date changed. Video events including but not limited to: Camera Blind, Camera Blur, Car parked in handicapped zone, Clear Storage, Clear Stream, Configuration Modification, Counted as entering, Counted as exiting, Counted in lane, Entered lot, Entered restricted zone, Entered target zone, Excessive System Clock Drift, Exited lot, Exited restricted zone, Input Alarm, Input Normal, Left unattended, Loitering in restricted zone, Made illegal U-turn, Motion Detected, Needs assistance, No Synchronization in 24 Hours, No Video Recording, On fence line, Output, People converged, People passed by, Possible theft, Pulled off the road, Reboot, Recorder Connected, Removed, Rule Engine Action Triggered, Running, Running in the wrong direction, Runtime Failure, S.M.A.R.T. Disk Failure, Security Modification, Self Restart, Session Connected, Speeding, Started moving in wrong direction, Staying in target zone, Stopped moving in wrong direction, Stopped running, Storage Devices Missing, Synchronize Time, System Files Modification, Time Server Unusable, Trespassing line, Video Boost Record, Video CSD Moved and Video Signal Lock.

k. Shall provide the ability for an operator to acknowledge and clear alarms from display. Prior to acknowledgment, the user shall be allowed to enter a response per alarm. The system shall offer a means to require acknowledgement of an alarm before it can be cleared.

l. Shall provide a display of the most current transactions in real time.

m. Shall provide the ability for dynamic alarm monitoring of alarm points in real time on the system computer’s video display terminal.

n. Shall provide an alarm view filter that is structured as a tree allowing the operator to select individual devices or groups of devices to be viewed.

o. Shall provide a “System” alarm upon a loop integrity violation.

p. Shall provide a “Panel Not Responding” alarm if communication to a panel is lost.

q. Shall provide real time printing of alarms as they occur by line printing with a dot matrix printer or provide printing of alarms, one page at a time, using typical Windows page printing.

7. Alarm Monitoring/System Control – Tree View

a. Shall provide the ability for dynamic alarm monitoring of alarm points in real time on the system computer’s video display terminal.

b. Shall provide color and icon shapes for each specific alarm point action of “Alarm”, “Normal”, “Trouble”, and “Shunted”.

c. Access control panels in the alarm tree, like alarm points, shall also indicate if they are in the buffered mode of operation as well as any “system” related alarm such as “Tamper” or “Primary Power Loss” or Loss of communication.

d. Devices connected to the communication server shall provide additional popup information as to the communication port or IP connection the device is programmed for.

e. Shall provide an option to launch a Virtual keypad from an intrusion panel partition to monitor the physical keypad remotely and to administer programming changes via the Virtual keypad.

f. The control tree shall be created by the user and allow for manual control of all system devices. By right clicking on a device in the tree the operator is able to initiate the appropriate action from a pick list. Actions shall include but not be limited to: Acknowledge All Alarms, Clear All Alarms, Send Time & Date, Send Camera Titles, Camera to Monitor Switch, Control Camera P/T/Z, Focus, Iris, Live Video, Retrieve Video from Clip, Run Command File, Lock, Unlock, Unlock Time Zone, Shunt, Shunt Time Zone, Un-shunt, Pulse, Timed Pulse, Restore to Time Zone (Door Mode), change Time Zone control of door modes (Lock Down/Disable, Lock Out, Card+PIN, Card or PIN, PIN only, Card only, Supervisor or Escort required), Initialize, Cancel Initialization, Buffer, Un-buffer, Connect Remote and Disconnect Remote from remote site. For partitions monitored by the intrusion panel the control shall include but not be limited to arm away, arm stay, disarm, refresh, and provide a virtual keypad for the partition. For zones monitored by the intrusion panel the control shall include but not be limited to bypass, un-bypass and refresh. Intrusion panel output control shall included activate, deactivate and refresh.

8. Operator Database

a. Shall allow the assignment of operator levels to define the system components that each operator has access to view, operate, change, or delete.

b. Shall have the ability to view, edit, or delete cardholder sensitive information such as note fields, card number, and PIN shall be definable by field per operator.

c. Shall provide the ability to define the accounts that the operator has access to.

d. Shall provide the ability to define if Alarm or Video pop-ups are allowed.

e. Shall provide the ability to log operator actions in the history files.

f. Shall provide the ability to select the default language during operator logon.

g. Shall provide specified time periods for the operator to logon

9. Control Panels

a. Shall provide ability to program Action Messages and assign an alarm event priority. A specific action message may be displayed for each alarm, system alarm (communication, ground fault, power, panel reset, low voltage, and panel tamper), card, or reader usage state. States shall include but not be limited to: Incorrect Password, Panel Configuration Error, Panel Remote Dial-up Failed, Panel Remote Dial-up Successful, Poll Response Alarm, Poll Response Normal, Primary Power Failure, Primary Power Normal, Tamper Switch Alarm, Tamper Switch Normal, Unsupported Panel Version, Anti-Pass back Violation, Anti-Pass back Violation Door Not Used, Anti-Pass back Violation Door Used, Card Not Found, Door Normal, Door Alarm, Door Trouble, Door Ajar, Door Locked, Door Unlocked, Duress Request Denied, Duress Request Door not Used, Duress Request Door Used, Forced Open, Free Egress Door Not Used, Free Egress Door not Verified, Free Egress Door Used, Host Grant Card Downloaded, Host Grant Door Unlocked, Invalid Format, Invalid Format Reverse Read, Invalid Pin, Invalid Site Code, Invalid Time zone, Issue Code, Never Allowed at this Door, No Second Card Presented, Site Code Verified Door Not Used, Site Code Verified Door Used Trace Card, Valid Card Door Not Used, Valid Card Door Used.

b. Intrusion partition events including but not limited to: Alarm, Alarm Cancel, Aram Away, Arm Stay, Auto Arm, Auto Disarm, Bypass, Disarm, Early Arm, Early Disarm, Fail to Arm, Fail to Disarm, Normal, Not Ready, Part Arm, Quick Arm, Recent Close, Remote Arm, Remote Disarm, Un-bypass, User Code Added, User Code Deleted, user Code Edited.

c. Intrusion zone events including but not limited to: Alarm, Alarm Restore, Bypass, Fault, Fault Restore, Normal, Trouble, Trouble Restore, and Un-bypass.

d. Intrusion output events including but not limited to: Alarm, Communication Loss, Normal, Tamper, and Tamper Restore.

e. Intrusion panel events including but not limited to: Access Denied, Automatic Test, Comm Fail, Comm Restore, Faults, Faults Restore, Line Restore, Line Trouble, Manual Test, Pager Restore, Pager Trouble, AC Restore, AC Trouble, Alarm, Battery Low, Battery Low Restore, Disarm, Normal, Recent Close, Reset, Panic Alarm, Power Up, Program begin, Program Changed, Program End, System Shutdown, System Shutdown Restore, Tamper Alarm, Tamper Restore, Test End, Test Start, Time/Date changed.

f. Video DVR events including but not limited to: Camera Blind, Camera Blur, Car parked in handicapped zone, Clear Storage, Clear Stream, Configuration Modification, Counted as entering, Counted as exiting, Counted in lane, Entered lot, Entered restricted zone, Entered target zone, Excessive System Clock Drift, Exited lot, Exited restricted zone, Input Alarm, Input Normal, Left unattended, Loitering in restricted zone, Made illegal U-turn, Motion Detected, Needs assistance, No Synchronization in 24 Hours, No Video Recording, On fence line, Output, People converged, People passed by, Possible theft, Pulled off the road, Reboot, Recorder Connected, Removed, Rule Engine Action Triggered, Running, Running in the wrong direction, Runtime Failure, S.M.A.R.T. Disk Failure, Security Modification, Self Restart, Session Connected, Speeding, Started moving in wrong direction, Staying in target zone, Stopped moving in wrong direction, Stopped running, Storage Devices Missing, Synchronize Time, System Files Modification, Time Server Unusable, Trespassing line, Video Boost Record, Video CSD Moved and Video Signal Lock.

g. Shall provide the ability to program descriptions, shunt times, and momentary shunt times for all access system alarm points.

h. Shall provide ability to program descriptions, pulse times, and energize times for all system output relays used for door control and other auxiliary functions.

i. Shall provide the ability to program descriptions for all system card readers.

j. Shall monitor both supervised and non-supervised access alarm points with the ability to select by point which point shall be supervised and define if the point is a normally closed or normally open point contact.

k. Shall provide the ability to interlock any alarm point condition to an output relay.

l. Shall provide the ability to interlock any alarm point condition to another alarm point.

m. Shall provide the ability to interlock any alarm point to switch a camera to a system monitor.

n. Shall provide ability to program alarms and associate incoming alarms with related outputs.

o. Shall provide a programmable “delay” setting of 255 seconds for all access system alarm points. The system shall not report the alarm condition until the delay setting has expired.

p. Shall allow 8 different site codes to be used in the system.

q. System shall allow various access control panel configurations to allow 1-16 readers per control panel.

10. Reports

a. Shall provide reporting capability for printing of selected system transactions from the disk files by specific time and date selection, range from time and date to time and date, or from start time to end time each day of the selected date range.

b. Shall provide a feature to generate a history report for an alarm point(s) state. An alarm point state shall be defined as Normal, Alarm, Trouble, or Ajar.

c. Shall provide a feature to generate a history report of system alarms. A system alarm state shall be defined by panel and include any of the following information: communication, ground fault, power, panel reset, low voltage, panel tamper, and loop communication.

d. Shall provide a feature to generate an ADV actions report, which provides information on how the system ADVs are configured including detailed/advanced video configurations.

e. Shall provide a feature to generate a history report for a card(s) state. A card state shall be defined as Normal, Trace, and Not Found, Anti-Pass back Violation, PIN Violation, Time Zone Violation, Site Code Violation, or Expired card. Additional search criteria shall include cardholders that meet up to at least 3-note field restriction and filter the report with defined reader location(s).

f. Shall provide a feature to generate a history report for system operator(s) activities. The report shall include time, date, operator name the device associated with the action and the type of action performed by the operator. Activities shall include but not limited to: acknowledged and cleared transactions, camera control, door mode, door and relay control such as unlock, lock; door and input control such as shunt, Un-shunt; login, logout, panel initialization, panel buffer and panel Un-buffer.

g. Shall provide complete database reporting of all data programmed into the system data files.

h. Shall provide an option to define how long a card holder has been in a defined area. This report shall allow the time to be accumulated representing an attendance report. The definable filters shall include time/date range, reader(s) definition, card number, card holder and note field. The output of the report shall allow sort options to include First Name, Last Name, Event Time, and Card Number. The sorted data shall be selectable as Alpha or Numeric sorting and Ascending or Descending.

i. Shall provide feature to generate a report based on the frequency of usage of a card. The report shall allow the operator to define a time/date period, a minimum and maximum usage limit, a means to define which reader or readers should be used to filter the report and the ability to further define the type of card to be reported on based on note field selections. This report shall also provide a disposition function. The cards meeting the filtering criteria shall be acted upon based on the disposition setting. Disposition settings shall include but not be limited to: Report only, De-activate the card or Re-assign to a specified an access level. This report shall be available in the event scheduler. When defining when to run the report an option to select the number of previous days to run the report against shall be provided. As an example a scheduled weekly report for the last 14 days could generate allowing for an overlap of time if desired.

j. Shall provide an option to create report templates. Report templates shall include, but not be limited to, History and Card Holder information. The templates shall be able to be assigned to a scheduler to run automatically per the scheduler settings.

11. Tracking/Muster Report

a. A tracking feature shall allow the system operator to identify an area and the person(s) in that area.

b. Areas shall be defined by readers representing an IN or OUT read status.

c. Defined areas shall provide an automatic update of how many cardholders are in the area.

d. An area defined as an exit shall remove the person from the tracking area.

e. A view displaying all card holders in a defined tracking or muster area shall have the ability to be sorted in columns where by clicking on the column the data in the column shall be sorted. At a minimum, the columns can be sorted by: Card Number, Status, Card Holder, Reader, and Time/Date.

f. A Muster area shall be defined by a reader(s) used to “muster” individuals in the event of an emergency.

g. Reports can be generated for the defined muster or tracking area.

h. Reports shall be generated for all muster or tracking areas in the system.

i. Reports shall be sorted on time and date, card number, card holder name or matching note field. When sorted on note field, a page break between fields shall allow the report to be easily handled for departmental uses.

j. Tracking areas shall include “nested” areas. Nesting allows for various reports from a large area to smaller areas within the large area.

k. A Tracking and Muster area screen shall be continually updated with the most recent card activity, therefore minimizing the time required generating a report.

l. A history priming feature shall load history activities for the defined amount of hours when the software is started. This priming feature shall be implemented in the event that the system computer is offline when a muster call is initiated, thereby allowing the implementation of the tracking and muster features of the software. The history priming time shall be operator selectable in 1-hour increments up to 99 hours.

12. Time Zones

a. Time zone definitions shall include Starting time, Ending time, Days of the week, and Holiday override.
b. Time shall be defined in either AM/PM or 24-hour (military) time.
c. The minimum time zone that shall be assigned to a panel is 63.
d. The maximum time zones that shall be defined in a system is unlimited.
e. Holidays shall be defined in three different time zones allowing different time schedule to be programmed for each holiday type.
f. Holidays shall be grouped in a Holiday Group.

13. Floor Plan Graphic

a. Shall provide the ability to import floor plan graphics stored in a WMF format.
b. Shall provide the ability to associate all ADV's (access, intrusion, and video) to floor plan graphics allowing the user to control and monitor the system.
c. Shall provide the ability to link floor plan graphics together in a hierarchy fashion.
d. Shall allow multiple floor plan views to be displayed simultaneously.

14. Remote Locations

a. Shall provide the ability to place remote control panels in an offline mode. In the offline mode, the remote control panels shall retain all panel history events. The amount of historical events shall be limited to the panels’ buffer capacity.
b. Shall provide the ability to place remote control panels in an offline mode where the remote panel will automatically call to the communications computer to report system alarms or upload buffered events.
c. Shall provide the ability to manage at least 250 remote locations.
d. Shall provide a user-defined schedule that will automatically add cards to any number of sites.

e. Shall provide system time schedules that the computer will use to automatically start uploading or downloading information to the remote sites. Information to be sent to the panel shall include, but not be limited to, card database changes, time, date, and buffer condition. Information received from the panel shall include all buffered events. While connected to the remote site, the system software shall poll, verify, and report any loss of panel communication. If a site's communication time is longer than expected, the system will automatically adjust the time schedule to allow all selected sites to be updated.

f. Attaching a site to an auto dial schedule shall allow the system to automatically dial the remote site at a predetermined time. The auto dial schedule is programmed with the ability to dial Once, Now, Hourly, Daily, Weekly, Two Weeks, Monthly, or Never to the remote site.

g. Shall provide the ability for an operator to program when the next scheduled update will occur, based on time and date.

h. Communication to remote dial up sites shall be accomplished through the use of password protection. The remote site provides the system with a site ID; the system responds with the appropriate password. No commands or transactions occur until the communication link is verified.

i. The System shall be able to receive or send information to remote access control panels on demand.

j. Shall have the ability to configure how many redial attempts from the remote location shall be defined from 1 to 5.

k. Shall have the ability to pause between redial attempts shall be programmable from 1 to 120 seconds.

l. Shall have the ability to pause before disconnecting shall be programmable from 1 to 30 seconds.

m. Communication rates shall be 38.4k baud.

15. Guard Tour

a. Guard Tour shall allow the operator to program a series of guard check points that must be activated to accomplish the task of a Guard Tour.

b. The check point shall be either reader points or alarm contact points or a mixture.

c. The Guard Tour shall be timed sequential allowing travel time between points with +/- tolerance. This type of tour shall allow alarms to be generated for early, missed, or late events.

d. The Guard Tour shall be un-sequenced with no time parameters.

e. The Guard Tour shall be started by two methods, Manual or Scheduled by the access control system scheduler.

16. Networking

a. Shall provide networking capabilities (LAN or WAN) as allowed by the computer's operating system license.

b. The access control software shall support two networking methods. By default, Domain controlled networks shall be the standard configuration providing secure networking communications. The ability to work on less secure peer-to-peer (Workgroup) networks shall be allowed for lower security installations. The functionality shall be one or the other and not run in both modes at the same time.

c. Shall provide the ability for a network system to support concurrent users up to the license limit (one station adding cards and making badges, another station monitoring alarms, yet other running data base reports, another controlling door openings and alarm shunting, and so on).

d. The workstation shall have the same user interface functionality as the Server, except the workstation shall not be able to perform database maintenance functions.

2.4 ISMS Computer Requirements

A. The ISMS shall be installed in a computer that supports more than 100 readers, 50,000 cards:

1. The computer will be provided by Troy School District

2.5 Hardware Requirements

A. Intelligent Controllers

1. Distributed architecture shall allow controllers to operate independently of the host. The architecture shall place key access decisions, event/action processing, and alarm monitoring functions within the controllers, eliminating degraded mode operation.

2. Flash memory management shall support firmware updates and revisions to be downloaded to the system. Upgrades to the hardware and software shall occur seamlessly without the loss of database, configurations, or historical report data.

3. Manufacturer: Subject to compliance with requirements, provide Field Controllers or comparable product:

a. Honeywell NetAXS Controller (NetAXS-123 and NetAXS-4 are the two types of NetAXS controllers)

B. Field Hardware

1. The security management system shall be equipped with access control field hardware required to receive alarms and administer all access granted/denied decisions. All field hardware shall meet UL requirements.
   a. Proximity Card Reader

   b. Request to Exit Motion Detector

   c. Door Monitor Switch

   d. Heavy Duty Door Strike (HES9600 or Equivalent)

   e. HID 1346 ProxKey lll

2.6 System Interfaces

A. Future Digital Video Recording Systems

1. The Security Management System shall provide fully integrated support for a powerful digital video recording and transmission system. The Security Management System shall record, search and transmit video, and shall provide users with live, pre and post- event assessment capabilities. The DVRs shall be seamlessly integrated with existing video equipment and incorporated into any TCP/IP network. The DVRs shall provide multiple levels of integration with the Security Management System software, providing control of the digital video system from the access control application.

2. ISMS shall support the following Digital Video Recorders (DVRs).

   a. Rapid Eye
   b. Fusion
   c. HRDP Performance Series
   d. MAXPRO NVR

3. Manufacturer(s) and products:

   a. Honeywell Rapid Eye™ Multi-Media series digital recorders
   b. Honeywell Fusion IV series digital recorders
   c. Honeywell MAXPRO® NVR SE/XE series recorders

B. Access Control Panels(Controllers)

1. NetAXS Panels shall have the following capabilities:

a. Types of NetAXS panels available are: NetAXS-4 panel and NetAXS-123 panel.

b. Panels (NetAXS-123 and NetAXS-4) are called as Gateway panels when added directly to the communication server.

c. NetAXS-4 Gateway panel supports the downstream devices feature. This feature shall extend the input and output capabilities of the NetAXS-4 panels.

d. Supports only the WIEGAND card format. The NetAXS panel allows multiple sets of card numbers and site codes embedded in a card format. These multiple embedded sets will be represented as A, B, C, and D sets of card numbers and site codes. The A set shall be used as the default / primary card and site code numbers. The resulting maximum length of the card number will be 64-bits in length (20-digit card number). This is the reason that the system defaults will incorporate the ability to select a 20-digit card number size in addition to the existing 5, 12 and 16 digit

e. Supports 128 time slots and 256 holidays (per holiday group). Holidays shall be definable in three different holiday types thus allowing for different operational time definitions for each holiday type. The NetAXS panels shall have a provision to add a new time zone while within the panel database. After creating the new time zone, it shall be added to the Time Zones database and applied to the panel's database.

f. Panel options such as Anti-passback, Groups (NetAXS-4 only), Forgiveness, Continuous Card Reads, Reverse Read LEDs, Host Grant, Site Codes, and Command File can be set for providing access to the readers, input points, and output points attached to the NetAXS panels.

g. NetAXS-4 panel shall allow configuring of 14 inputs with default values. NetAXS-123 panel shall allow configuring 15 inputs with default values.

h. NetAXS-4 panel shall support 4 readers controlling 4 entrances. NetAXS-123 shall support 6 readers controlling 3 doors where the "A" reader is the primary reader for the door and the "B" reader is the Out reader for the door when so used. The B Reader can be programmed separately regarding name, Advanced Options, Anti-Passback configuration, and Intrusion support. The B Reader cannot work alone as a Reader only. When used, the B reader will be tied to the A reader in terms of the interlock relationships pertaining to Door operation. The Advanced Options selection shall provide several advance features not normally used in the typical system and thus the reason they are accessed separately to reduce confusion for typical installations. For the NetAXS-123, Reader A and Reader B shall support their own settings.

i. The Groups option shall be supported only by the NetAXS-4 panels. A maximum of 64 groups shall be defined with a maximum of 72 relays.

C. Existing Intrusion Detection Panels:

1. Honeywell VISTA-128FBP, VISTA-250FBP Controllers, Honeywell VISTA -128BPT, and Honeywell VISTA-250BPT.

   a. General Requirements: The Security Management System shall support hardwired and TCP/IP communication for the VISTA 128FBP/VISTA-250 FBP panel. Each panel can have 8 partitions and 15 zone lists. Zones, partitions, and the top-level panel shall have an events page, with all supported events present. Features:

      1) Disarm and unlock a door on card swipe.
      2) Arm and lock a door on card swipe.
      3) Common area arm/disarm.
      4) Access denied if intrusion system is in alarm or armed.
      5) Monitor and log intrusion system events and alarms in the Security Management System.
      6) Associate intrusion system events and alarms to video surveillance integrations.

   b. Security Management System users are able to control and monitor Group and zone status using the Security Management System client, and control the individual zones and groups using Security Management System Access control credentials. Depending on the combined user profiles and access permissions defined in Security Management System, Security Management System cardholder is allowed or denied permission to arm/disarm zones and groups. The access control functionality of the intrusion panel is disabled when the integration is operational. Features:

      1) Disarm a zone on a card swipe.
      2) Arm a zone on consecutive card swipes. Security Management System will support definition of quantity of swipes required and the timeout time in seconds to recognize consecutive swipes.
      3) Security Management System supports linking of intrusion panel users with Security Management System cardholders.
      4) Security Management System operators may be given control permissions for intrusion input and output alarms.
      5) Security Management System can associate alarm events with video commands to look at current or historic footage.
      6) Security Management System stores and reports on intrusion events.

PART 3 EXECUTION

3.1 Examination

A. Examine site conditions to determine site conditions are acceptable without qualifications. Notify Owner in writing if deficiencies are found. Starting work is evidence that site conditions are acceptable.

3.2 Installation

A. Integrated Security Management System, including but not limited to access control, alarm monitoring, CCTV, and ID badging system shall be installed in accordance with the manufacturer's installation instructions.

B. Supervise Installation to appraise ongoing progress of the other trades and contracts, make allowances for all ongoing work, and coordinate the requirements of the installation of the Security Management System.

- Troy School District will not furnish any more materials like beam clamps, bridle rings, fire stop, conduit, connectors, cabling, etc. It will be up to the contractor to look at each job site and determine what additional components and/or hardware will be required. ***Note***: Installation must be incompliance with NFPA, International Fire Codes, ASTM Standards and any other federal or local codes required for the installation/upgrade of this security system.
- Remove all debris (packing, waste, etc.) from district property in accordance with local and state regulations.
- Make sure to take every precaution to safely perform the installation without harming humans or surrounding environment. Any damage to structures, walls, flooring, ceiling tile, etc will be repaired or replaced with like materials at the contractor's expense.
- All debris must be removed and the area cleaned up at the end of each work day. No debris should be left in the corridors, teaching spaces or entranceways.

3.3 Field Testing and Certification

A. Testing: The access control, alarm monitoring, CCTV, and ID badging system shall be tested in accordance with the following:

1. Conduct a complete inspection and test of all installed access control and security monitoring equipment. This includes testing and verifying connection to equipment of other divisions such as life safety and elevators.
2. Provide staff to test all devices and all operational features of the Security Management System for witness by the Owner's representative and authorities having jurisdiction as applicable.
3. Correct deficiencies until satisfactory results are obtained.
4. Submit written copies of test results.

PART 4 SAFETY

4.01 Guidelines

A. It is **highly recommended** that you walk each project to verify scope of work. Arrangement for visiting the facilities must be first approved by:
   - **Kenneth D. Miller – Executive Director (248 823-4050)**

B. During normal school hours all contractors are requires to check in with the main office at each of the sites before entering school district property. Your visit should not interfere with the staff or students educational process. All questions concerning the project must be in written format and emailed to the purchasing department.

C. Ladders, lifts and scaffolding must meet OSHA requirements and in good working condition. School district equipment is off-limit to vendors.

D. You will be required to check with the Executive Director prior to the start of this project for approval to store or create a staging area for equipment, trailers and materials.

E. The contractor will be solely responsible and abide by all federal, state, and local laws pertaining to the safety of all employees and observers and will maintain workers compensation as required.

Troy School District

	Estimated Cable Footage for Each Drop						
Facility	1	2	3	4	5	Main Office	Total
Barnard Elementary	128	224	100	196	60	160	868
Bemis Elementary	128	224	100	196	60	160	868
Costello Elementary	120	210	264	126	80	70	870
Hamilton Elementary	128	224	100	196	60	160	868
Hill Elementary	180	236	60	60	85	150	771
Leonard Elementary	260	328	336	328	60	280	1592
Martell Elementary	120	264	210	126	80	70	870
Morse Elementary	168	296	284	170	60	156	1134
Schroeder Elementary	256	292	328	240	100	196	1412
Troy Union Elementary	160	320	300	140	110	212	1242
Wass Elementary	128	224	100	196	60	160	868
Wattles Elementary	88	194	168	112	70	110	742
Boulan Park Middle School	288	280			200	224	992
Larson Middle School	288	280			200	224	992
Smith Middle School	252	172			50	212	686
International Academy East	295	305	255		80	330	1265
Administration Building	66	88	62		60	65	341

1 thru 4 - Readers to MDF

5 - Video/Intercom Door Station to Main Office

Main Office to MDF

1. Estimated cable distances are based on utilizing the corridors, low level ceilings and the path of least resistance that would reduce the requirement for specialized equipment or multiple penetrations through firewalls or educational spaces (i.e. classrooms, conference, etc.). I also factored in 20 additional feet to cover drops to the control panel and readers/stations.
2. All cabling below the ceiling level must be in-cased (Wiremold) to protect it from damage. The casing must not only be designed to protect the wiring, it also must be of the same color scheme so it blends in and is not obtrusive.
3. All cable runs are to be properly secured above the ceiling to prevent the cable from sagging. All penetrations will require to be sealed with fire retardant material.
4. **Note:** Due to District "Security Policies" blueprints of the facilities will not be issued as part of the bid package. Once a contractor is selected a copy of the "Code Compliance" plans will be issued (must be signed for by an administrator of the organization) to the company so they can document the location of each device and cable run. Once the project is completed the blueprints are to be returned to the Executive Director.

Building Locations

Administrative Building **4400 Livernois** **Troy, Michigan 48098** **Built – 1973 Sqft – 12,000**	**International Academy East** **1291 Torpey** **Troy, Michigan** **Built – 1952 (A) Sqft – 81,311**
Barnard Elementary **3601 Forge Drive** **Troy, Michigan 48083** **Built – 1978 (A) Sqft – 64,192**	**Bemis Elementary** **3571 Northfield Parkway** **Troy, Michigan 48084** **Built – 1978 (A) Sqft – 64,192**
Costello Elementary **1333 Hamman** **Troy, Michigan 48085** **Built – 1972 (A) Sqft – 52,055**	**Hamilton Elementary** **5625 Northfield Parkway** **Troy, Michigan 48098** **Built – 1983 (A) Sqft – 64,192**
Hill Elementary **4600 Forsyth** **Troy, Michigan 48085** **Built – 1967 (A) Sqft – 54,336**	**Leonard Elementary** **4401 Tallman** **Troy, Michigan 48085** **Built – 1959 (A) Sqft – 59,220**
Martell Elementary **5666 Livernois** **Troy, Michigan 48098** **Built – 1972 (A) Sqft – 52,799**	**Morse Elementary** **475 Cherry** **Troy, Michigan 48083** **Built – 1956 (A) Sqft – 54,636**
Schroeder Elementary **3541 Jack Drive** **Troy, Michigan 48084** **Built – 1970 (A) Sqft – 61,896**	**Troy Union Elementary** **1340 E. Square Lake** **Troy, Michigan 48085** **Built – 1925 (A) Sqft – 66,929**
Wass Elementary **2340 Willard** **Troy, Michigan 48085** **Built – 1978 (A) Sqft – 64,192**	**Wattles Elementary** **3555 Ellenboro** **Troy, Michigan** **Built – 1967 (A) Sqft – 59,150**
Boulan Park Middle School **3570 Northfield Parkway** **Troy, Michigan 48084** **Built – 1971 Sqft – 110,830**	**Larson Middle School** **2222 E. Long Lake Road** **Troy, Michigan 48085** **Built – 1971 Sqft – 110,830**
Smith Middle School **5835 Donaldson** **Troy, Michigan 48085** **Built – 1967 (A) Sqft – 100,734**	

The following locations below are “Sister Buildings” and internal floor plans are almost identical:

- Barnard Elementary – Bemis Elementary – Hamilton Elementary – Wass Elementary
- Costello Elementary – Martell Elementary
- Boulan Park Middle School – Larson Middle School

Video/Intercom Systems and Proximity Card Readers
Troy School District

Administrative Building

Door Number 1 – Main Entrance

- Video/Intercom System
- Honeywell OP30HON Omniprox Reader

Door Number 2

- Honeywell OP30HON Omniprox Reader

Door Number 3

- Honeywell OP30HON Omniprox Reader

International Academy

Door Number 1 – Main Entrance

- Video/Intercom System
- Honeywell OP30HON Omniprox Reader

Door Number 2

- Honeywell OP30HON Omniprox Reader

Door Number 3 – Grow Entrance

- Video/Intercom System
- Honeywell OP30HON Omniprox Reader

Barnard Elementary

Door Number 1 – Main Entrance

- Video/Intercom System
- Honeywell OP30HON Omniprox Reader

Door Number 2

- Honeywell OP30HON Omniprox Reader

Door Number 3

- Honeywell OP30HON Omniprox Reader

Door Number 4

- Honeywell OP30HON Omniprox Reader

Bemis Elementary

Door Number 1 – Main Entrance

- Video/Intercom System
- Honeywell OP30HON Omniprox Reader

Door Number 2

- Honeywell OP30HON Omniprox Reader

Door Number 3

- Honeywell OP30HON Omniprox Reader

Door Number 4

- Honeywell OP30HON Omniprox Reader

Costello Elementary

Door Number 1 – Main Entrance

- Video/Intercom System
- Honeywell OP30HON Omniprox Reader

Door Number 2

- Honeywell OP30HON Omniprox Reader

Door Number 3

- Honeywell OP30HON Omniprox Reader

Door Number 4

- Honeywell OP30HON Omniprox Reader

Hamilton Elementary

Door Number 1 – Main Entrance

- Video/Intercom System
- Honeywell OP30HON Omniprox Reader

Door Number 2

- Honeywell OP30HON Omniprox Reader

Door Number 3

- Honeywell OP30HON Omniprox Reader

Door Number 4

- Honeywell OP30HON Omniprox Reader

Hill Elementary

Door Number 1 – Main Entrance

- Video/Intercom System
- Honeywell OP30HON Omniprox Reader

Door Number 2

- Honeywell OP30HON Omniprox Reader

Door Number 3

- Honeywell OP30HON Omniprox Reader

Door Number 4

- Honeywell OP30HON Omniprox Reader

Leonard Elementary

Door Number 1 – Main Entrance

- Video/Intercom System
- Honeywell OP30HON Omniprox Reader

Door Number 2

- Honeywell OP30HON Omniprox Reader

Door Number 3

- Honeywell OP30HON Omniprox Reader

Door Number 4

- Honeywell OP30HON Omniprox Reader

Martell Elementary

Door Number 1 – Main Entrance

- Video/Intercom System
- Honeywell OP30HON Omniprox Reader

Door Number 2

- Honeywell OP30HON Omniprox Reader

Door Number 3

- Honeywell OP30HON Omniprox Reader

Door Number 4

- Honeywell OP30HON Omniprox Reader

Morse Elementary

Door Number 1 – Main Entrance

- Video/Intercom System
- Honeywell OP30HON Omniprox Reader

Door Number 2

- Honeywell OP30HON Omniprox Reader

Door Number 3

- Honeywell OP30HON Omniprox Reader

Door Number 4

- Honeywell OP30HON Omniprox Reader

Schroeder Elementary

Door Number 1 – Main Entrance

- Honeywell OP30HON Omniprox Reader

Door Number 2

- Honeywell OP30HON Omniprox Reader

Door Number 3

- Honeywell OP30HON Omniprox Reader

Door Number 4

- Honeywell OP30HON Omniprox Reader

Troy Union Elementary

Door Number 1 – Main Entrance

- Video/Intercom System
- Honeywell OP30HON Omniprox Reader

Door Number 2

- Honeywell OP30HON Omniprox Reader

Door Number 3

- Honeywell OP30HON Omniprox Reader

Door Number 4

- Honeywell OP30HON Omniprox Reader

Wass Elementary

Door Number 1 – Main Entrance

- Video/Intercom System
- Honeywell OP30HON Omniprox Reader

Door Number 2

- Honeywell OP30HON Omniprox Reader

Door Number 3

- Honeywell OP30HON Omniprox Reader

Door Number 4

- Honeywell OP30HON Omniprox Reader

Wattles Elementary

Door Number 1 – Main Entrance

- Video/Intercom System
- Honeywell OP30HON Omniprox Reader

Door Number 2

- Honeywell OP30HON Omniprox Reader

Door Number 3

- Honeywell OP30HON Omniprox Reader

Door Number 4

- Honeywell OP30HON Omniprox Reader

Boulan Park Middle School

Door Number 1 – Main Entrance

- Video/Intercom System
- Honeywell OP30HON Omniprox Reader

Door Number 2

- Honeywell OP30HON Omniprox Reader

Larson Middle School

Door Number 1 – Main Entrance

- Video/Intercom System
- Honeywell OP30HON Omniprox Reader

Door Number 2

- Honeywell OP30HON Omniprox Reader

Smith Middle School

Door Number 1 – Main Entrance

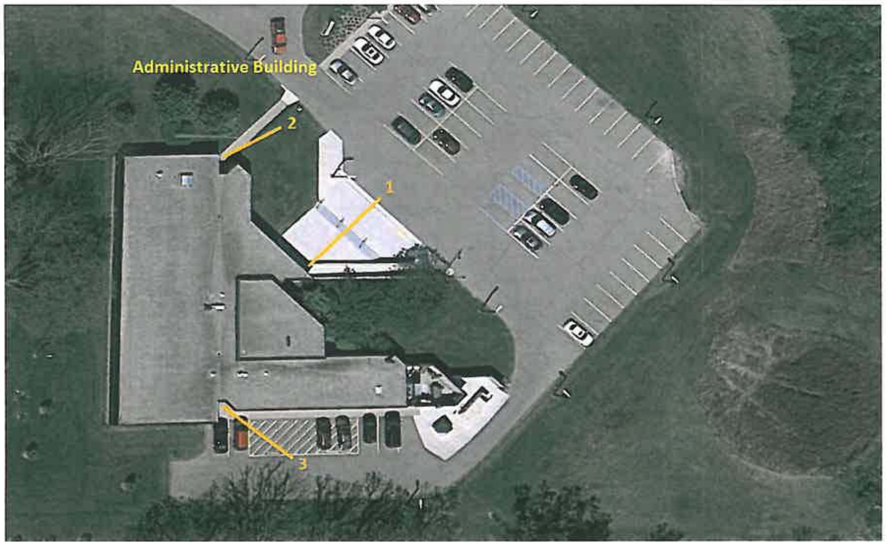
- Video/Intercom System
- Honeywell OP30HON Omniprox Reader

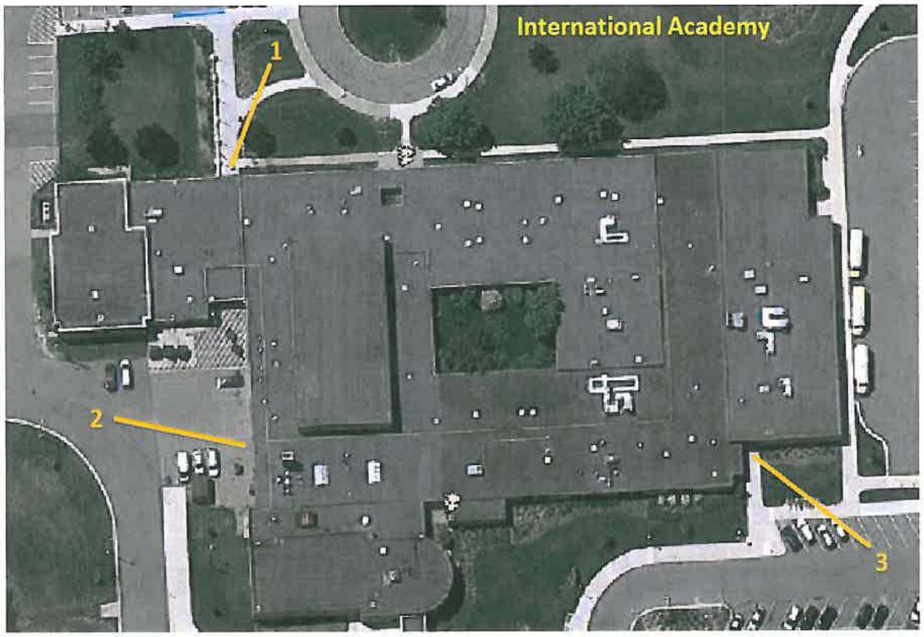
Door Number 2

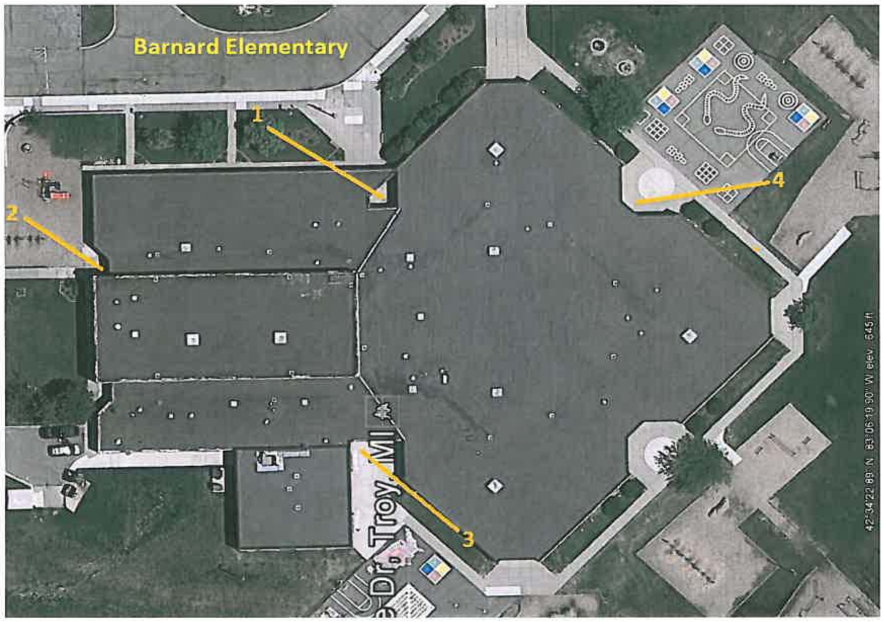
- Honeywell OP30HON Omniprox Reader

MINIMUM REQUIRED EQUIPMENT LIST

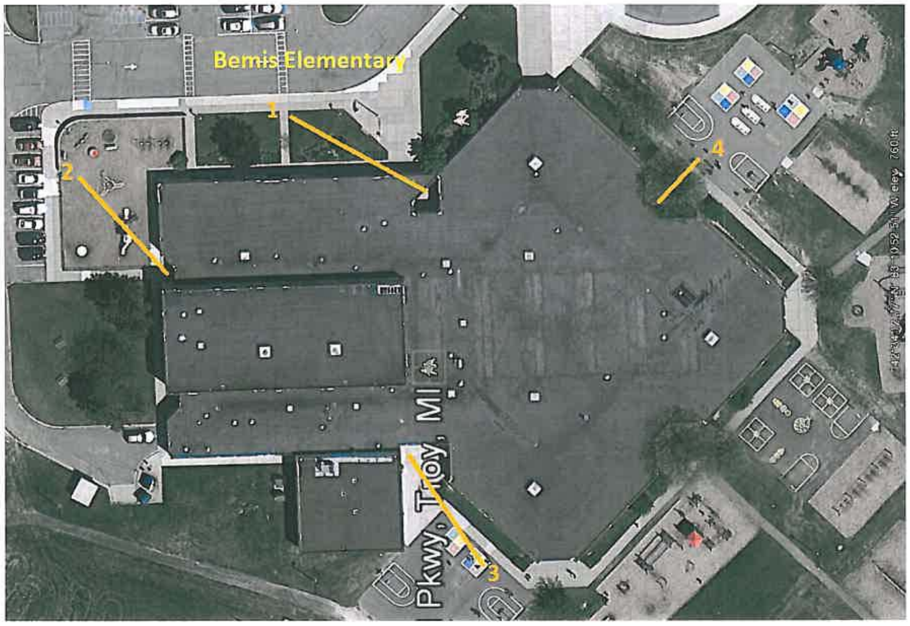
	AIPHONE VIDEO ENTRY SYSTEM PKG (18)
1	JKW-IP, IP VIDEO/INTERCOM ADAPTER
1	JKS-1ADV, VIDEO/INTERCOM SYSTEM
1	CONNECTION TO ACCESS CONTROLLER “REX” INPUT (TO RELEASE DOOR STRIKE)
1	MCW S/A DESK STAND
1	CAT5P W/RJ45 JACKS, CABLE RUN TO NEAREST MDF ROOM
*	AIPHONE 871802P10C MID CAP CABLE 18/2, TO DOOR STATION
*	AIPHONE 871804P10C MID CAP CABLE 18/4, TO IP ADAPTER
*	INSTALLATION HARDWARE
	HONEYWELL INTEGRATED SECURITY MANAGEMENT SYSTEM
1	WINPAK SE 3.0 ACCESS MANAGEMENT SYSTEM (ONE FOR THE DISTRICT)
1000	HID 1346 Prox Key III
	EACH ELEMENTARY BLDG/AND ADMIN BLDG (13)
1	HONEYWELL NX4L1, FOUR DOOR CONTROLLER
2	12V 7ah RECHARGEABLE BATTERIES FOR NX4L1
4	HONEYWELL OP30HON OMNIPROX READER
4	HONEYWELL IS320BL/WH, REQUEST TO EXIT DEVICE
4	DOOR MONITOR SWITCH
4	HES9600, RIM STYLE ELECTRIC STRIKE
1	CAT5P W/RJ45 JACK CABLE RUN TO DESIGNATED SWITCH IN MDF ROOM
*	NECESSARY PLENUM CABLE FOR ABOVE DEVICES
*	NECESSARY INSTALLATION HARDWARE
	EACH MIDDLE SCHOOL & INTERNATIONAL ACADEMY (4)
1	HONEYWELL NX4L1, FOUR DOOR CONTROLLER
2	12V 7ah RECHARGEABLE BATTERIES FOR NX4L1
2	HONEYWELL OP30HON OMNIPROX READER
2	HONEYWELL IS320BL/WH, REQUEST TO EXIT DEVICE
2	DOOR MONITOR SWITCH
2	HES9600, RIM STYLE ELECTRIC STRIKE
1	CAT5P W/RJ45 JACK CABLE RUN TO DESIGNATED SWITCH IN MDF ROOM
*	NECESSARY PLENUM CABLE FOR ABOVE DEVICES
*	NECESSARY INSTALLATION HARDWARE
*	NECESSARY QUANTITY FOR EACH SYSTEM
	03/23/13 3:05pm


Administrative Building
2
1
3

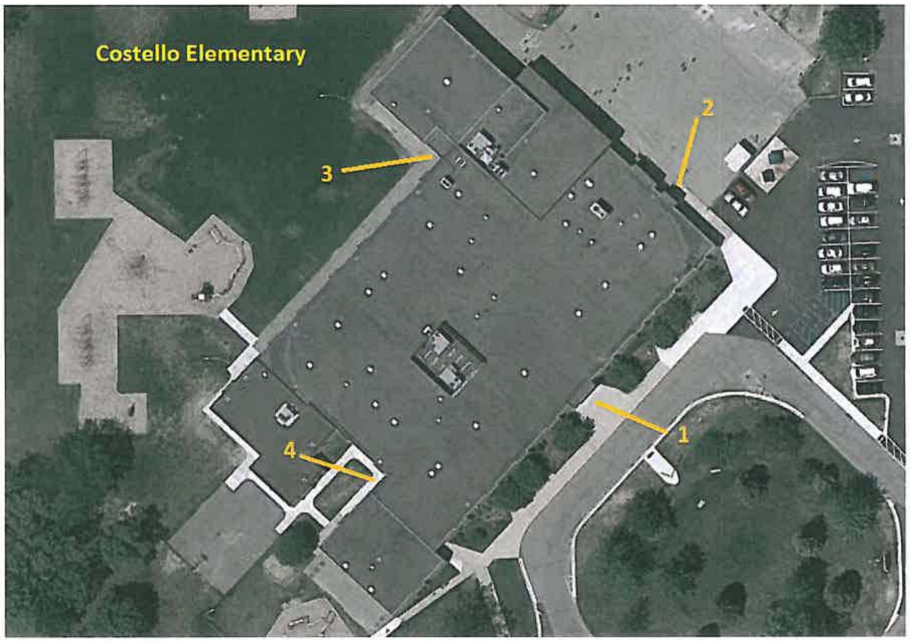

International Academy
1
2
3

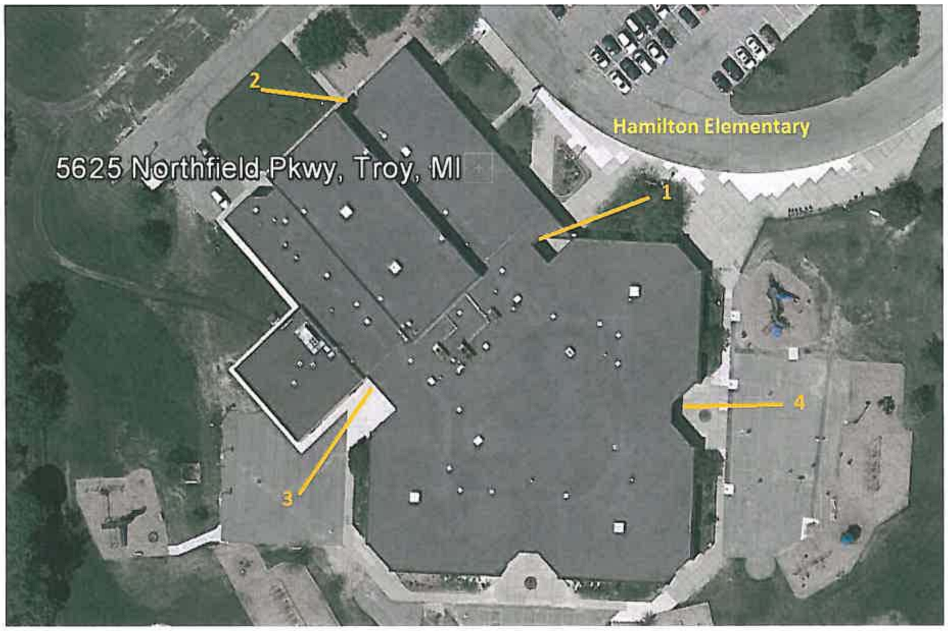

Barnard Elementary
1
2
3
4
Troy, MI
42°34'22.89" N 83°06'19.90" W elev. 645 ft

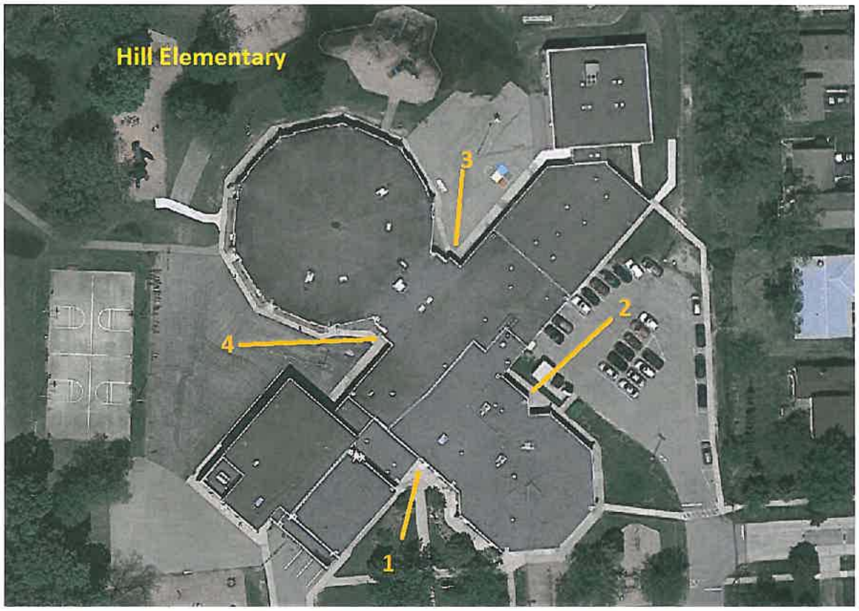
Welcome

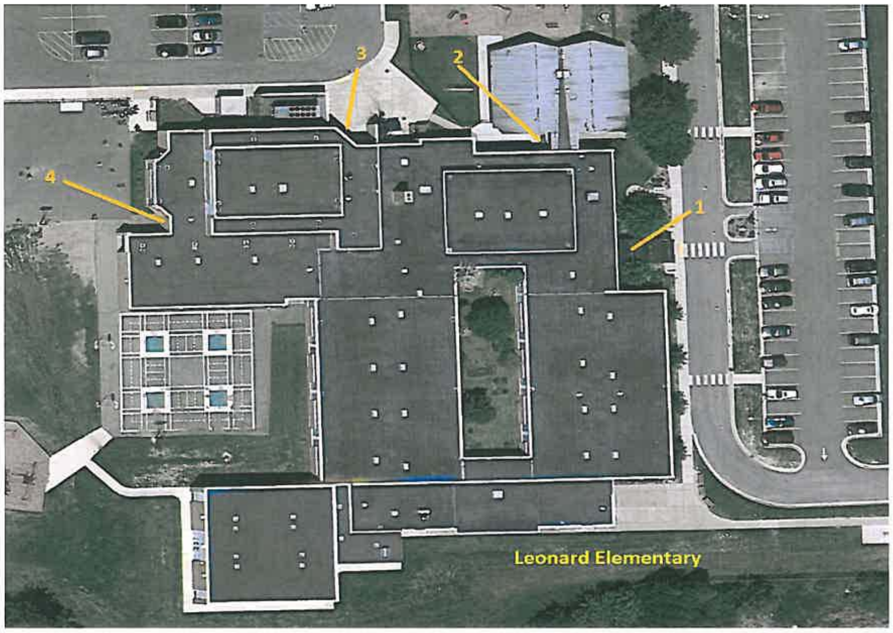

Bemis Elementary
1
2
3
4
Pkwy, Troy, MI

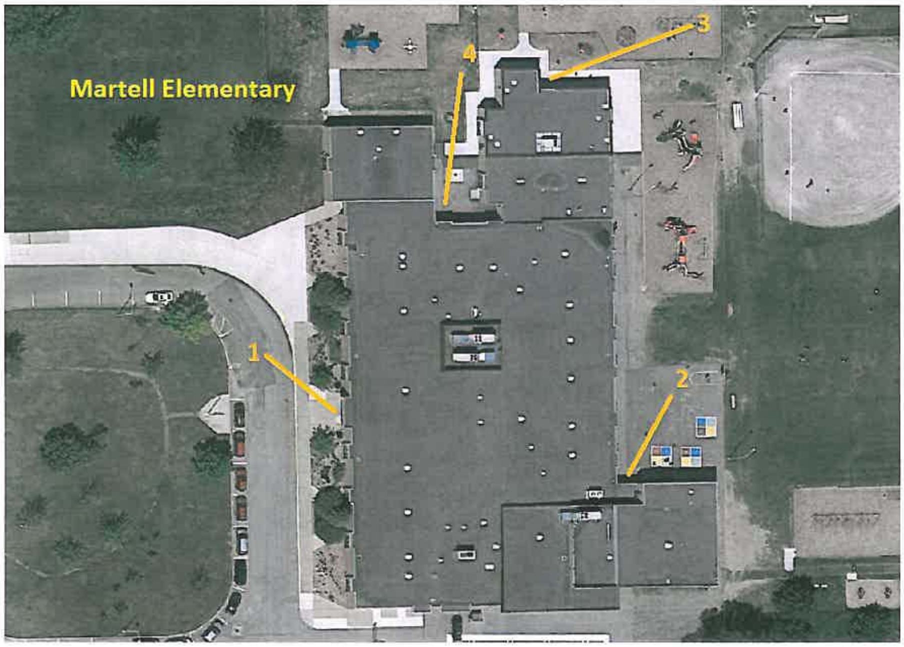
C A R E
O

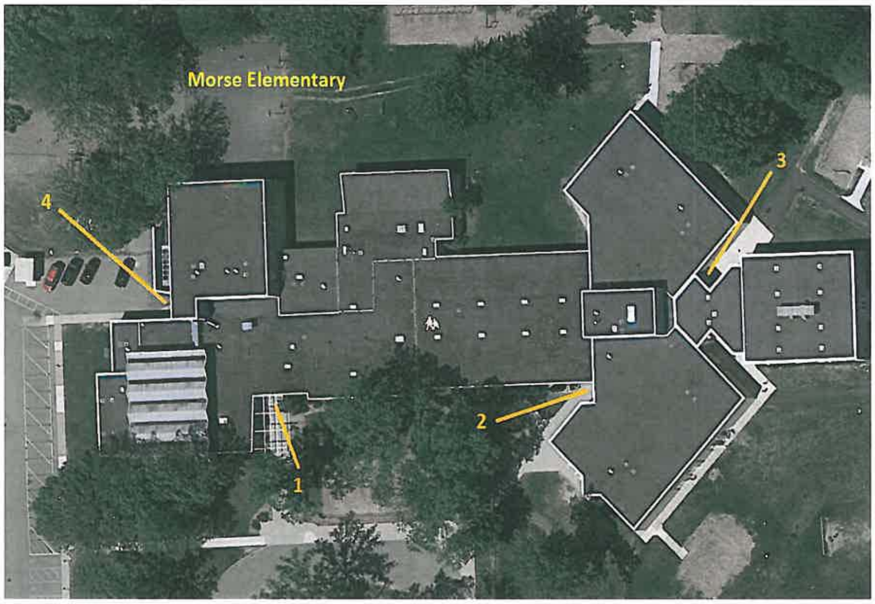

Costello Elementary
1
2
3
4


2
Hamilton Elementary
5625 Northfield Pkwy, Troy, MI
1
4
3

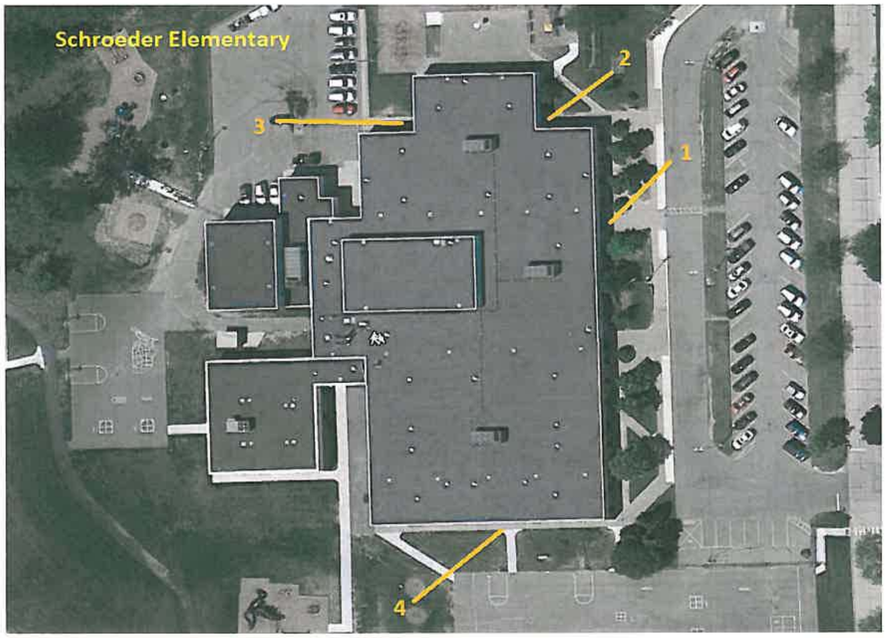

Hill Elementary
3
2
4
1


3
2
4
1
Leonard Elementary

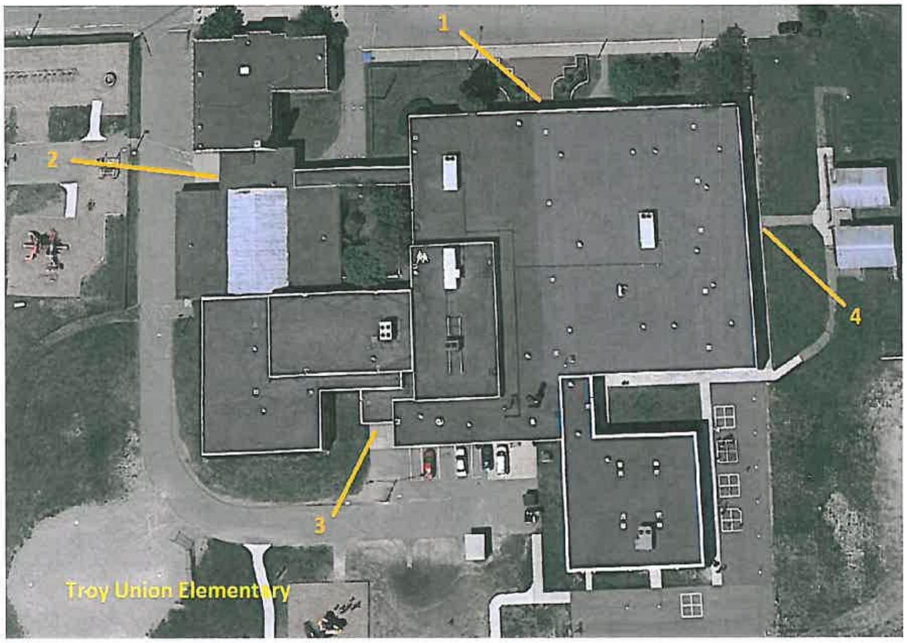

Martell Elementary
1
2
3
4

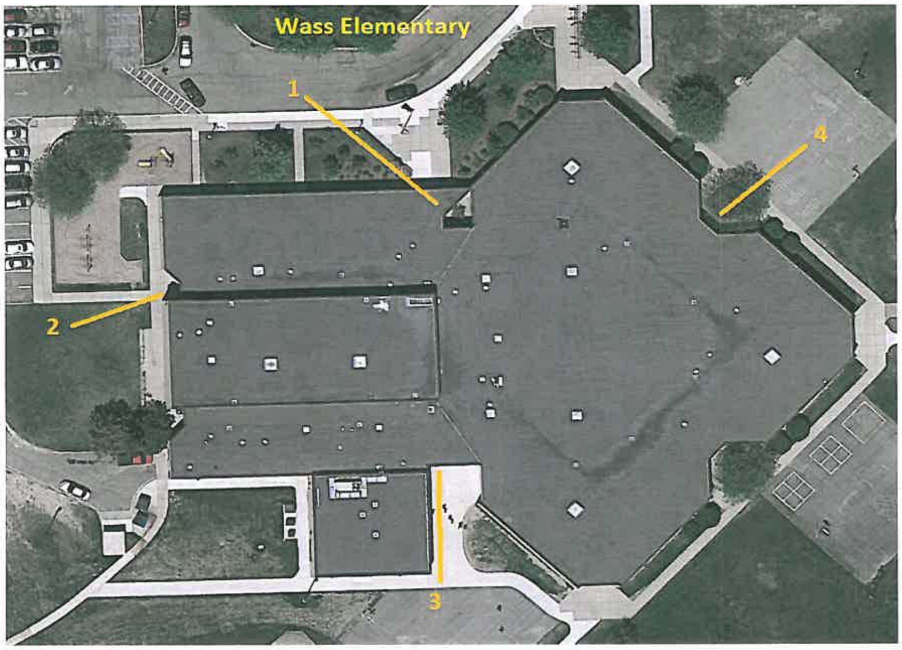

Morse Elementary
4
3
2
1

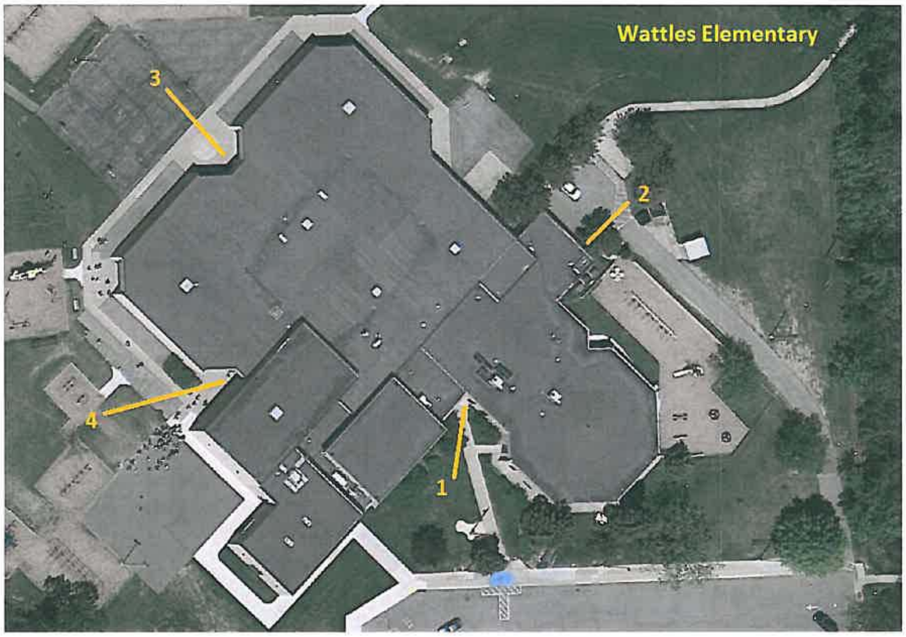
2nd Grade Line Up
1st Grade Line Up

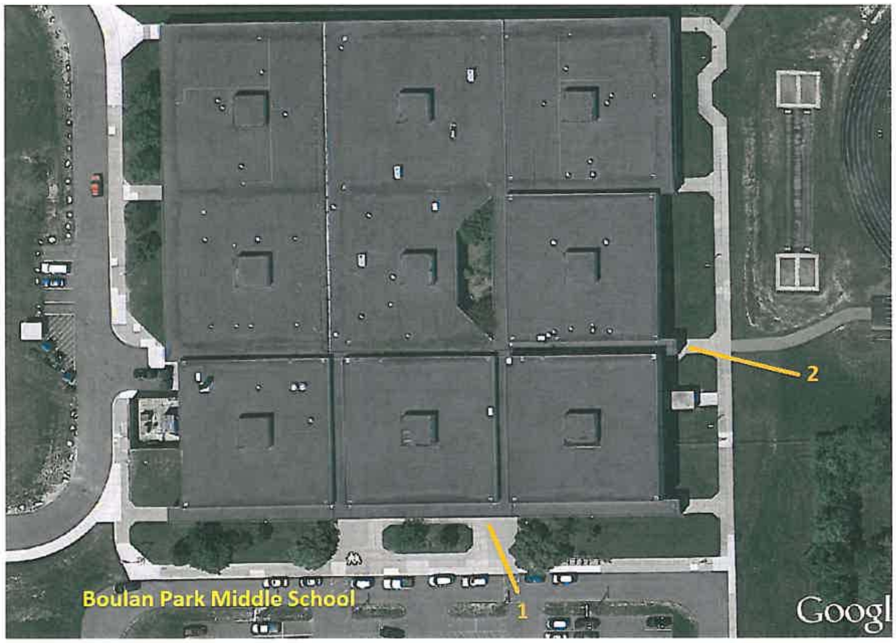

Schroeder Elementary
2
3
1
4

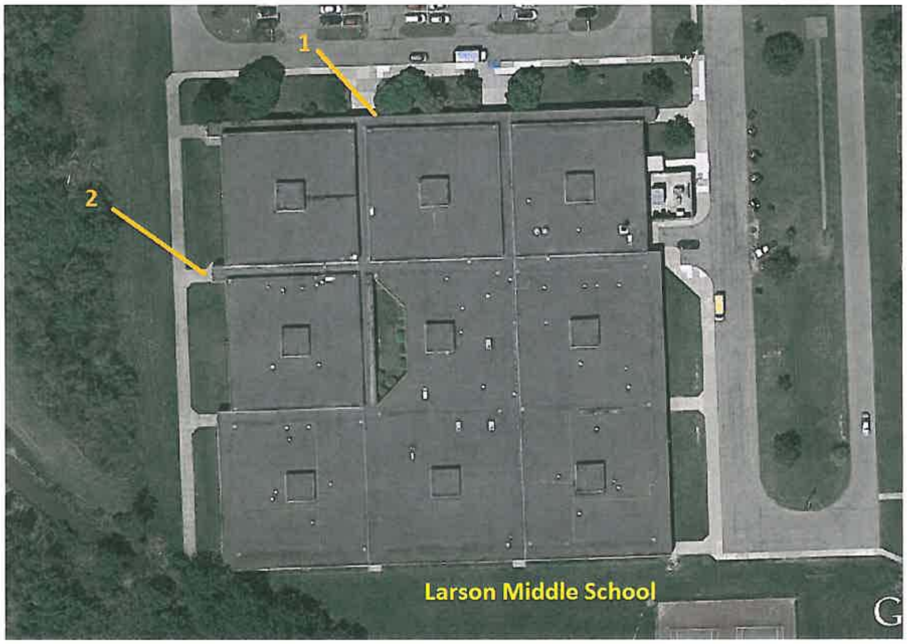
.A.R.E.
CO.

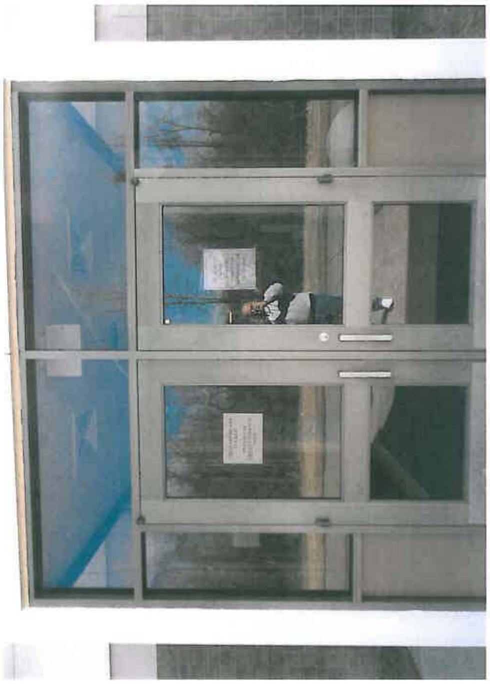

1
2
3
4
Troy Union Elementary

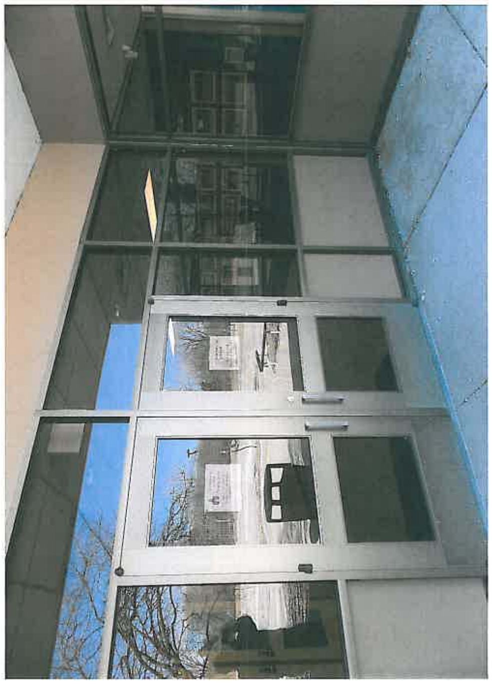

Wass Elementary
1
4
2
3

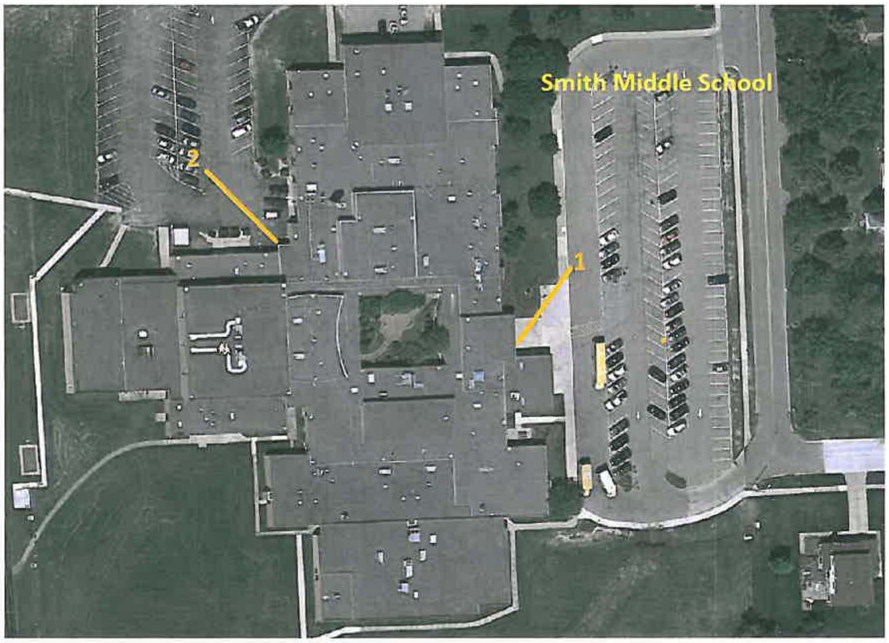

Wattles Elementary
3
2
4
1


2
Boulan Park Middle School
1


1
2
Larson Middle School
G






Smith Middle School
2
1

TROY
SCHOOL DISTRICT

DUE: 2:00 p.m**.,** Monday, April 29, 2013
PROPOSAL: BID NO. 9758 Integrated Security Management System

PROPOSAL FORM

We propose to furnish, deliver and install an Integrated Security Management System for the Troy School District in accordance with the specifications:

Facility	Material Cost	Labor Cost	Total
Administrative Building			
Barnard Elementary			
Bemis Elementary			
Costello Elementary			
Hamilton Elementary			
Hill Elementary			
Leonard Elementary			
Martell Elementary			
Morse Elementary			

Facility	Material Cost	Labor Cost	Total
Schroeder Elementary			
Troy Union Elementary			
Wass Elementary			
Wattles Elementary			
Boulan Park Middle School			
Larson Middle School			
Smith Middle School			
International Academy East			

Total ______

BIDDER'S FIRM NAME ______________________________

ADDRESS ______________________________

CITY/STATE ______________________ ZIP __________

TELEPHONE NUMBER ______________________ FAX # __________

SIGNED BY ______________________ TITLE __________

TYPED NAME ______________________ DATE __________

E-MAIL ADDRESS ______________________________

SWORN AND NOTARIZED FAMILIAL DISCLOSURE STATEMENT

All Vendor/Contractor(s) submitting proposals must provide familial disclosure and attach this information to the proposal. The proposal will be accompanied by a sworn and notarized statement disclosing any familial relationship that exists between the owner or key employee of the vendor submitting a proposal and any member of the Troy School Board or the Troy School Superintendent. The District will not accept a proposal that does not include this sworn and notarized disclosure statement.

The members of Troy School Board are: Nancy Philippart, Todd Miletti, Paula Fleming, Ida Edumunds, Wendy Underwood, Gary Hauff and Karl Schmidt. The Troy Schools Superintendent is Barbara A. Fowler.

□ **The following are the familial relationship(s):**

_____Owner/Employee Name____ **_ ____Related to:_____** **__ __Relationship_____**

1. ______________________________ ____________________ _____________________

2. ______________________________ ____________________ _____________________

3. ______________________________ ____________________ _____________________

Attach additional pages if necessary to disclose familial relationships.

□ **There is no familial relationship that exists** between the owner or key employee of the Vendor/Contractor(s) submitting a proposal and any member of the Troy School Board, or the Troy Schools Superintendent.

INDIVIDUAL/FIRM NAME ____

BY (SIGNATURE) ____

PRINTED NAME AND TITLE ____

Subscribed and sworn before me, this _________ Seal:

day of ____________, 20 ____, a Notary Public

in and for _____________ County, __________

____
(Signature)
NOTARY PUBLIC

My Commission expires ____________________

CERTIFICATION OF COMPLIANCE – IRAN ECONOMIC SANCTIONS ACT

Michigan Public Act No. 517 of 2012

The undersigned, the owner, or authorized officer of the below-named Company, pursuant to the compliance certification requirement provided in Troy School District's Request For Proposal, the "RFP", hereby certifies, represents, and warrants that the Company and its officers, directors and employees, is not an "Iran Linked Business" within the meaning of the Iran Economic Sanctions Act, Michigan Public Act No. 517 of 2012 (the "Act"), and that in the event the Company is awarded a contract by Troy School District as a result of the aforementioned RFP, the Company is not and will not become an "Iran Linked Business" at any time during the course of performing any services under the contract.

The Company further acknowledges that any person who is found to have submitted a false certification is responsible for a civil penalty of not more than $250,000.00 or two (2) times the amount of the contract or proposed contract for which the false certification was made, whichever is greater, the cost of Troy School District's investigation, and reasonable attorney fees, in addition to the fine. Moreover, any person who submitted a false certification shall be ineligible to bid on a request for proposal for three (3) years from the date the it is determined that the person has submitted the false certification.

____

Name of Company

____

Name and Title of Authorized Representative

____

Signature

____

Date

Acceptance of Proposal

The undersigned agrees to execute a Contract for work covered by this Proposal provided that he is notified of its acceptance within thirty days after the opening of the Proposal.

It is agreed that this bid will not be withdrawn until after forty-five (45) days after receipt of bids.

The undersigned affirms that the bid was developed without any collusion, undertaking, or agreement, either directly or indirectly, with any other bidder(s) to maintain the prices of indicated work or prevent any other bidder(s) from bidding the work.

BIDDER’S FIRM NAME ____

BUSINESS ADDRESS ____

____

TELEPHONE NUMBER ____

FAX NUMBER ____

BY (SIGNATURE) ____

PRINTED NAME ____

TITLE ____

SIGNED THIS ____________ DAY OF _____________, 20 _______

E-MAIL ADDRESS ____

TROY
SCHOOL DISTRICT

Purchasing Department
Facility Operations

BID 9758

RE: Integrated Security Management System

ADDENDUM #1 – April 23, 2013

The Bidding Documents are modified, supplemented or augmented as follows, and this Addendum is hereby made a part of the proposed Contract Documents.

Question #1

In Lieu of the Honeywell Equipment specified, Based on the last approved TSD bond issue the Andover System was upgraded to allow for the Bid No. 9758 expansion. MCMI is requesting the bid allow the expansion of the current Andover Controls system installed throughout the District that is already integrated with the Specified Honeywell Ademco Intrusion Detection System to be bid.

Answer #1

The District encourages all bidders to quote alternates and include anything in their proposals that would promote better quality product that meets or exceeds the specifications listed.

Troy School District
BID 9758 - Integrated Security Management System
Bid Tabulation

Vendor	Total	Alternate
Audio Sentry Corporation	$ 154,855.00	
Mechanical Controls & Maintenance, Inc.		a) $ 197,166.00
Midstate Security Company, LLC	$ 209,634.00	
a) Alternate Bid - Using Andover Controls		

Vendors Solicited

Audo Sentry
Huffermaster
Ingersoll-Rand Company
Mechanical Controls & Maintenance, Inc. (MCMI)
SBD Security
Tyco Integrated Security