CITY OF MT. PLEASANT
MT. PLEASANT DEPARTMENT OF PUBLIC SAFETY
804 E. High St.
Mt. Pleasant, MI 48858

ELECTRONIC ACCESS CONTROL SYSTEM (EACS) & FACILITY MANAGEMENT & CONTROL SYSTEM (FMCS) INTEGRATION PROJECT

1. PART 1 GENERAL

1.1 SUMMARY

A. This section describes the Electronic Access Control System & Facility Management & Control System scope of work for the project. This section also references the responsibilities of the Systems Integrator (Prime Contractor) and Electrical, Door Hardware trade sub-contractors pertaining to products or systems, furnished by each trade, that affect this project.

B. It is the owner's goal to implement a security& card access system that will allow products from various suppliers to be integrated into a unified system on one platform and to provide flexibility for expansion, maintenance, and service of the system.

C. It is the owner's goal to completely remove the existing American Automatrix Facility Management Control System on all existing HVAC equipment, reusing all com bus, cabling, VAV Boxes and wiring that can be reused and install a Carrier I Vue Open System. The Carrier I Vue Open system must be integrated into the Electronic Access Control and Intrusion System. Both systems must reside on the Niagara AX Framework platform.

D. The Facility Management & Control System Contractor must be the prime contractor on this project.

1.2 SYSTEM DESCRIPTION

A. The Electronic Access Control and Intrusion System (EACS) as provided shall be based on the Niagara^{AX} Framework (or "Niagara"), a Java-based framework developed by Tridium, Inc. The Niagara^{AX} Framework provides an open automation infrastructure that integrates diverse systems and devices (regardless of manufacturer, communication standard or software) into a unified platform that can be easily managed in real time over the Internet using a standard Web browser.

B. The EACS shall be a Honeywell WEBAX Security & Access System to provide a completely web-based access control and alarm monitoring system that shall be accessed through a standard Web browser. The EACS shall consist of a Network Security Controller, Door Control Modules, Cameras, DVR Video Drivers, Digital Video Recorders, Supervised Alarm Input / Output Modules, access and intrusion system peripheral devices and a standard web browser.

Please contact Mike Rosu at Cochrane Supply for a predetermined parts list for this project. Any other EACS systems will not be accepted. Variation from this list will not be accepted. 1-800-482-4894.

1. A Network Security Controller (NSC) within each facility shall regulate access, maintain historical records and alarm security personnel. The NSC shall connect to the owner's local or wide area network, as described elsewhere in this document. Secure access to the system, either locally in each building, or remotely from a central site or sites, shall be accomplished through standard Web browsers, via the Internet and/or local area network. Each NSC shall communicate to door controllers and other monitoring alarm input/output devices.

2. A Door Control Module (DCM) shall provide a physical interface for EACS door peripherals such as card readers, door position switches, request to exit devices and output to control the door locking mechanism. The DCM shall communicate directly to the NSC through a RS485 protocol.

3. A Supervised Alarm Input / Output Module (IOM) shall provide a physical interface for EACS alarm inputs such as motion detectors, glass break sensors, etc. and monitor outputs to control lighting panels, horns, etc. The IOM shall communicate directly to the NSC through a RS485 protocol.

4. The existing Edwards fire alarm panel must be tied into the Honeywell Webs Platform to monitor status.

C. The Facility Management & Control System (FMCS) shall be a Carrier I Vue Open Control System.

1. The Carrier I Vue Open system shall be installed (replacing existing American Automatrix) on all existing HVAC Equipment & VAV's with reheat. The Carrier System shall connect to the owner's local or wide area network. Secure access to the system, either locally in each building, or remotely from a central site or sites, shall be accomplished through standard Web browsers, via the Internet and/ or local area network. Each controller shall communicate to the Niagara AX platform for a seamless integration of the FMCS to the EACS platform. Please contact Scott House @ Carrier Great Lakes: 810-577-2944 for a predetermined parts list for this project. Any other FMCS will not be accepted. Variation from this list will not be accepted. A complete list of equipment is provided below:

6 – AHU's w/HWV & 6- DX condensing units
32 – VAV's with reheat
2 – Boilers w/controls
4 – HW pumps

1 – Finn Tube HTG valve
14 - Exhaust fans
1- Generator
All associated t-stats per drawings per zone to be replaced

1.3 SUBMITTAL

A. Two copies of shop drawings of the entire EACS shall be submitted and shall consist of a complete list of equipment and materials, including manufacturers catalog data sheets and installation instructions. Shop drawings shall also contain complete wiring and schematic diagrams, software descriptions, calculations, and any other details required to demonstrate that the system has been coordinated and will properly function as an integrated system. Terminal identification for all control wiring shall be shown on the shop drawings.

   The prime contractor must provide a summary of how they are going to complete the system integration between the FMCS and the EACS to reside on the Honeywell Webs AX Niagara Platform.

B. Submittal shall also include a trunk cable schematic diagram depicting operator workstations, Network Security Controller locations, Door Control Modules, Alarm Input / Output Modules, Card Readers and a description of the communication type, media and protocol.

C. Submittal shall also include a complete point list of all input and output points connected to the EACS & FMCS. EACS & FMCS contractor shall provide necessary point lists, protocol documentation, and factory support information for systems provided in this division. FMCS points list must be per piece of equipment also showing network diagrams and system architecture. FMCS must also show all points that will be available for the integration into the EACS.

D. Submittal shall also include a copy of each of the graphics developed for the EACS & FMCS Graphic User Interface including a flowchart (site map) indicating how the graphics are to be linked to one another for system navigation. The graphics are intended to be 80% - 90% complete at this stage with the only remaining changes to be based on review comments from the A/E design team and/or Owner.

E. Upon completion of the work, provide a complete set of 'as-built' drawings and application software on compact disk. Drawings shall be provided as AutoCAD™ or Visio™ compatible files. Two copies of the 'as-built' drawings shall be provided in addition to the documents on compact disk. All contractors (prime and subs) shall provide as-builts for their portions of work. All as built drawings shall also be installed into the server in a dedicated directory.

1.4 DEFINITIONS

A. Acronyms used in this specification are as follows:

EACS	Electronic Access Control System
DCM	Door Control Module
FMCS	Facility Management and Control System
IOM	Input/Output Module
LAN	Local Area Network
NSC	Network Security Controller
PICS	Product Interoperability Compliance Statement
WAN	Wide Area Network

1.5 DIVISION OF WORK

A. The EACS contractor shall be responsible for Network Security Controller, Alarm and Display Workstations (when provided), Door Control Modules, Card Readers, Remote Input/Output Devices, controller programming, controller programming software, power wiring and Controller, Module, Reader and I/O wiring.

B. The FMCS contactor shall be responsible for the integrating data and alarms into an EACS via the local or wide area network on the Niagara AX Framework.

1.6 RELATED WORK:

A. Openings- Must be fire stopped per City of Mt. Pleasant Fire Code

B. Mechanical:

1. Provide HVAC control devices and systems

2. Provide fans, dampers and other control devices

C. Electrical:

1. Provide disconnect switches (unless otherwise noted)

2. Power wiring and conduit (unless otherwise noted)

3. Integration of the generator on the Niagara AX Framework

D. Facility Management and Control:

1. Provide Network Area Controllers (NAC) per Carrier I Vue Open Protocol

2. Provide Carrier I Vue Open Server hardware and software

3. Software programming between FMCS & EACS.

E. Door Hardware:

1. Door Hardware must be included in this project

2. Magnetic strike systems are not approved

3. Electronic strike systems are approved

1.7 AGENCY AND CODE APPROVALS

A. All products of the EACS shall be provided with the following agency approvals. Verification that the approvals exist for all submitted products shall be provided with the submittal package. Systems or products not currently offering the following approvals are not acceptable.

1. FCC, Part 15, Subpart J, Class A Computing Devices

1.8 SOFTWARE LICENSE AGREEMENT

A. It is the owners express goal to implement an FMCS that will allow access and occupancy data to integrated into a EACS Niagara AX Framework in order to provide improved energy management and security. The Owner shall be the named license holder of all software associated with any and all incremental work on the project(s). In addition, the Owner shall receive use of all job specific configuration documentation, data files, and application-level software and programming tools developed for the project. This shall include all custom, job specific software code and documentation for all configuration and programming that is generated for a given project and/or configured for use with the NSC and any related LAN / WAN / Intranet and Internet connected routers and devices. Any and all required IDs and passwords for access to any component or software program shall be provided to the owner.

1.9 DELIVERY, STORAGE AND HANDLING

A. Provide factory-shipping cartons for each piece of equipment and control device. Maintain cartons through shipping, storage, and handling as required to prevent equipment damage. Store equipment and materials inside and protected from weather.

1.10 JOB CONDITIONS

A. Cooperation with Other Trades: Coordinate the Work of this section with that of other sections to ensure that the Work will be carried out in an orderly fashion. It shall be this Contractor's responsibility to check the Contract Documents for possible conflicts between his Work and that of other crafts.

2. PART 2 PRODUCTS

2.1 GENERAL

A. The Electronic Access Control and Intrusion System shall be comprised of all the components referenced within Cochrane Supply's Component List.

B. The Facility Management Control System shall be comprised of all the necessary items to achieve a fully functional Carrier I Vue Open Control System when complete integrated into the EACS Platform

2.2 OPEN, INTEROPERABLE, INTEGRATED ARCHITECTURES

A. The intent of this specification is to provide a fully integrated system operating on the Niagara Framework via Ethernet using one of the following protocols: BACnet IP..

B. The supplied NSC shall employ component-oriented technology (COT) for representation of all data and control devices within the system. In addition, adherence to industry standards is required to assure interoperability between all system components. For each BACnet ANSI / ASHRAE™ Standard 135-2004, system, the system supplier must provide a PICS document showing the installed systems compliance level. Physical connection of BACnet devices shall be via Ethernet using BACnet/IP. BACNet MSTP shall not be acceptable as a means to integrate the EACS with a FMCS.

C. The EACS shall not require a dedicated PC to host the security application or system database. The supplied system must incorporate the ability to access all data using standard Web browsers for

operator interface and configuration. An embedded database shall be provided at the NSC and connectivity is required for all system database parameter storage.

2.3 NETWORK CONTROLLERS

A. The NSC shall be specified by Cochrane Supply.

B. The EACS contractor shall supply Network Security Controllers (NSC) as part of this contract.

C. The Network Security Controller shall provide the interface between the LAN or WAN and the door control modules (DCM) and remote input/output devices, and provide global supervisory access control functions over the all devices connected to the NSC. The NSC shall provide multiple user access to the system. The NSC shall support standard Web browser access via the Intranet/Internet.

D. The EACS & FMCS controllers shall be capable of executing common application control programs to provide:

1. Calendar functions
2. Scheduling
3. Event and Credential database Reporting
4. Alarm monitoring and routing
5. Time synchronization
6. Integration via BACnet, Niagara^{AX} Fox, oBIX or SNMP protocols

E. The Network Security Controller shall be mounted in a key locked, tamper switch protected metal enclosure with the following requirements per the location specified by the customer:

1. The cabinet shall be suitable for wall mounting and contain a removable door for ease of installation.
2. The cabinet shall be suitably sized to allow installation of the controller and additional expansion modules if required.
3. A single tamper switch shall be incorporated into the door.
4. The enclosure shall include 4 mounting holes and sufficient knockouts on the top, bottom and sides.

2.4 DOOR CONTROL MODULE (DCM)

A. The DCM shall be specified by Cochrane Supply..

B. The DCM shall be mounted in a key locked, tamper switch protected metal enclosure with the following requirements per the location specified by owner:

1. The cabinet shall be suitable for wall mounting and contain a removable door for ease of installation.
2. The cabinet shall be suitably sized to allow installation of the controller and additional expansion modules if required.
3. A single tamper switch shall be incorporated into the door.

4. The enclosure shall include 4 mounting holes and sufficient knockouts on the top, bottom and sides.

5. The DCM shall be capable of controlling the Card Reader to provide different audible beeps for indication of either "Access granted" or "Access denied". Te Card Reader red LED shall flash red for access denied. The Card Reader green LED shall flash green for access granted and shall show solid green when there is free access.

2.5 SUPERVISED ALARM INPUT/OUTPUT MODULE (IOM)

A. The IOM shall be specified by Cochrane Supply.

2.6 CARD READER

A. Card Reader shall be specified by Cochrane Supply.

2.7 WEB BROWSER CLIENTS (EACS & FMCS):

A. The system shall be capable of supporting up to twenty five (25) simultaneous clients using a standard Web browser such as Internet Explorer™, Mozilla Firefox™, or equivalent.

B. The Web browser user interface shall support at a minimum, the following functions:

1. User log-on identification and password shall be required. If an unauthorized user attempts access, a login failed message shall be displayed. Security using authentication and encryption techniques to prevent unauthorized access shall be implemented.

2. Graphical screens shall be available, without requiring any graphics to be stored on the client machine. Systems that require graphics storage on each client PC are not acceptable. Graphics must represent real time data and show fully functioning equipment and real time movement.

3. Real-time values displayed on a Web page shall update automatically without requiring a manual “refresh” of the Web page.

4. Users to have administrator-defined access privileges. Depending on the access privileges assigned, the user shall be able to perform the following:

a. Modify, Input, Delete or Override common access control objects, such as doors, credentials, interlocks, schedules, and calendars, set points of control system.

b. View and acknowledge alarms.

c. Setup and execute queries on credential and event archive information.

5. The system shall provide the capability to specify a user's (as determined by the log-on user identification) home page. Provide the ability to limit a specific user to just their defined home page. From the home page, links to other views, or pages in the system shall be possible, if allowed by the system administrator.

6. Graphic screens on the Web Browser user interface shall support hypertext links to other locations on the Internet or on Intranet sites, by specifying the Uniform Resource Locator (URL) for the desired link.

C. Local or Remote connections shall be via an Ethernet LAN/WAN.

2.8 SYSTEM CAPACITIES

A. The system software shall support the following features and be configured for a minimum of the following:

1. 2,500 Personnel Records

2. 5,000 Buffered Transactions of System Events

3. 16 Programmable Wiegand Card Formats

4. 250 Access Levels

5. 250 Weekly Schedules

6. 32 Holidays

7. 32 Special Holidays

2.9 ACCESS CONTROL

A. Each door (9 total) shall be comprised of one (1) card reader pre Cochrane Supply, a door position status point, a request to exit device, and a door lock control output point designator.

B. The system shall allow a reader to operate using the following functions:

1. Readers shall read cards while the door is in the open position.

2. The software shall allow the following door relock configurations:

a. Unlock the door for a user definable period of time. Valid range for access unlock time shall be from 0 seconds to 1 hour.

b. Relock the door on door open. If the door is never opened after a valid request, the system shall relock the door when the access unlock time expires.

c. Relock the door on door closed. If the door is never closed after a valid request, the system shall relock the door when the access unlock timer expires. The system shall report a door held open alarm, if the door remains open after the access unlock and alarm sense timer expires.

3. There shall be separate timers for the operation of the door lock and the software shunting of the door switch monitor alarm point. The shunting of the door contact following the presentation of a valid access card or activation of the request to exit device shall be accomplished by software control. The use of a hardware shunt shall not be accepted. The system shall operate according to the following with the door shunt time:

    a. Door Held Open - If the door fails to close prior to the expiration of the shunt period, a "door held open" alarm shall occur at the NSC.

    b. Door Forced Open – If door position switch is armed and an intrusion occurs (door open without authorization), a “door forced open” alarm shall be annunciated.

C. The system shall allow each door to be configured to cause a variety of alarms to occur based upon activity at that door. These shall include as a minimum:

1. Door forced open
2. Door held open
3. Badge does note exist
4. Badge is lost
5. Badge is disabled
6. No active schedule
7. No access right
8. Granted but not used
9. Invalid PIN number
10. Anti Passback violation
11. Door position switch supervision
12. Request to exit supervision

D. The system shall provide the ability for the user to configure a global offset to the system badge holder's PIN number. The system shall allow a person at a keypad reader to signal the system operator that they are entering the area under duress using the PIN duress value. This duress alarm should not be evident at the card reader. The access controls normally executed by the system, person is authorized for that door, at that time and that day of the week, shall still be enforced for a duress access event.

E. The system shall provide configuration options to control the card reader's Red LED, Green LED and Beeper functions during both a valid and invalid access request. The minimum configurations for these auxiliary reader outputs shall include:

1. Use access unlock time
2. Define custom time
3. Pulse output on and off for a definable period of bursts

F. Area Control Strategies

1. Manual Control – With the appropriate password level, a user shall be able to manually control all doors and control points via the browser based user interface. Control points are defined as any door strike or any other relay output point of a NSC, DCM or I/O module. All system outputs shall be overridden by initiating a mouse "right click" and selecting the command action from a list. All manual control commands shall be recorded into the Event log for viewing by any user given proper privileges to do so. Manual control for doors, or any relay output, shall allow the user to:

a. Unlock the door/output (leaving the door strike unlocked)

b. Pulse the output open

c. Return the door/output to a pre-defined automatic setting.

2. The Timed Anti-Passback feature shall enable a software timer that prevents a second access at the same reader for an adjustable period of time after a cardholder has already gained access. This helps prevent multiple swipes by an individual to allow access to others through turnstile doors.

G. The system shall support time and attendance based functionality. The software shall provide the ability to designate a card reader to be used as a "clock in" or "clock out" reader. The resulting access traffic through the time and attendance reader shall be logged in a separate report. The system should allow the OWNER to manually insert records into the log to capture missed user transactions (ie, the user forgot to swipe their badge to either clock in or clock out).

2.10 CREDENTIAL MANAGEMENT

A. It shall be the responsibility of the EACS Contractor to enroll all personnel and badge records. The EACS shall consist of equipment and devices placed at predetermined locations to ensure that only cardholders who are authorized to enter secured areas through certain doors or gates can do so.

B. The NSC shall generate and store up to 2,500 personnel records, and monitor badge/credential use throughout the facility. The credentials database shall be populated by the user, based on data that is input and captured at the time of enrollment.

C. The user shall be able to create personnel records either through the use of direct input into the personnel record or via an import feature. Each personnel record shall be tabular in design for easy navigation through the fields. The credential data screen shall allow for multiple credentials to be enrolled in an efficient manner. The user shall have the ability from the personnel record to easily:

1. Add, delete, or modify personnel data and shall consist of a minimum of the following data fields:

a. Record ID Number (System Defined)

b. Last Name

c. First Name

d. Middle Name

e. Employee ID

f. Tenant Designation

g. Department Type

h. Person Type

i. Personal Identification Number (PIN)

2. Add, delete, or modify personnel data in up to 10 custom defined data fields.

3. Assign and manage the cardholder's facility access rights.

4. Assign badges to personnel records by selecting badges from the un-assigned list, input new badge, or enroll new badge from system reader.

5. Enable or disable the cards - the user shall be able to mark the card as enabled or disabled by selecting that control button.

6. Define expiration date - the expiration date shall be determined by date. It shall be possible to program future start and end dates for a new cardholder's access or any specific part of their access.

7. Define the card number and facility code.

8. Mark the card as lost - the user shall be able to mark the card as lost by selecting that control button. This shall disable the card, create a stored record with the associated card number and cardholder and generate an alarm on future access attempts.

D. The user shall be able to create badge records either through the use of direct input into the badge record, mass creation through badge enrollment, bulk badge creation by defining credential number range, or via an import feature. Each badge record shall be tabular in design for easy navigation through the fields. The OWNER shall have the ability from the badge record to easily:

1. Add, delete, or modify personnel data and shall consist of a minimum of the following data fields:

a. Record ID Number (System Defined)

b. Credential Number

c. Facility Code

d. Wiegand Format

e. Status

f. Tenant Designation

g. Description

h. Activation Date

i. Expiration Date

j. Owner

2. Remove badge from personnel record

E. In addition to manual input of credential information, the EACS shall allow operator to input credential records from a properly structured CSV file. The import data screen shall allow for multiple credentials to be enrolled and edited in an efficient manner.

F. After a badge is created it shall be possible to assign access privileges to the personnel record. If a user also has proper authorization, access privileges can be overwritten. When an individual's access

privileges are modified, that change shall be effective immediately upon completion of the change. Changes of access privileges shall affect only the modified record, and shall not require a download of the entire cardholder database.

G. The user with proper authorization shall be able to initiate the call-up of a cardholder record. This feature shall be provided via browser to assist the user in determining access rights for an employee who may have forgotten his or her badge. Utilizing a database search via the input of the cardholder's name, or other key search fields, the EACS shall access the employee's personnel file, and containing pertinent information for identification by the user. This operation shall not restrict the operation of monitoring alarms.

2.11 ACCESS RIGHTS

A. Access Privileges - All cardholders shall have facility access based on privileges assigned by controlled area, time and date. For example, some badges shall only allow access to the facility on weekdays between 8:00 a.m. and 5:00 p.m., while others allow access on weekends between 1 p.m. to 5 p.m. and so on. These time zones for each day are to be pre-defined by user and shall be able to be modified quickly by authorized employees without vendor intervention. The systems shall provide the following minimum user-definable features for access privileges. The FMCS shall have access rights assigned to the system per owner's direction.

1. Description
2. Schedule
3. Tenant
4. Collection of Readers

2.12 TENANTS

A. The EACS software shall support logical database filtering based on tenant record designations. The system shall support the creation of multiple tenant types; EACS access based on users with specific tenant designations, and provide ability to assign tenants to personnel records, badge records, and access rights. For example, EACS users assigned to tenant A shall only have access to personnel, badges, access rights, reports and alarms designated as tenant A data. While employing tenant methodology, the user shall have the ability to do the following:

1. Distribute credential management responsibilities to building tenants.
2. Display data based on EACS user assigned tenant designation.
3. Add, delete, and modify personnel records, badges and access rights of same tenant data.

2.13 SYSTEM DATE / TIME: EACS & FMCS

A. Time / Date - The time and date of the system shall be set by the Network Security Controller (NSC). Dates for Daylight Savings Time shall automatically take effect. Holiday schedules input by OWNER shall be capable of overriding normal schedules in effect. The system shall support the new daylight savings rules implemented in 2007.

2.14 ALARM MANAGEMENT (EACS & FMCS)

A. Alarm Notification and Actions

1. The NSC shall be capable of displaying and routing alarms directly from Door Controller Modules, or from Input/Output Modules.

   Any alarm (regardless of its origination) shall be integrated into the overall alarm management system and shall appear in all standard alarm reports, be available for user acknowledgment.

2. Alarm generation shall be selectable for annunciation type and acknowledgement requirements including but limited to:

   a. To alarm

   b. Return to normal

   c. To fault

3. Provide for the creation of a minimum of 255 alarm priorities to be assigned to individual alarms.

4. NSC equipment external power fail/low battery detection and network failures shall be treated as alarms and annunciated. Door Control Module (DCM) cabinet tamper and external power fail/low battery detection shall be treated as alarms and annunciated.

B. Alarms Annunciation

1. Alarm Console message

   a. The alarm Console manages alarms on a per-point basis. Each row in the alarm console is the most recent alarm from a point. To view all the current alarms from a particular security point, the user shall double click the row.

   b. To acknowledge an alarm, the owner shall select the desired alarm and click the Acknowledge button. An alarm is cleared from the alarm console when both of the following conditions exist:

      1. Alarm is acknowledged

      2. The point is in a "normal" state

   c. The user shall also be able to add notes to the alarm record using the notes dialog box.

2. Email of the complete alarm message up to eight recipients. Provide the ability to route and email alarms based on:

   a. Individual Day of week

   b. Time of day range

   c. Recipient – include the ability to cc and bcc others in the organization

   d. Type of alarm – systems shall allow user to individually assign types of alarms to go to a particular recipient including:

1. To Off Normal
2. To Normal
3. To Alert
4. To Fault
5. Equipment failure

e. Graphic with flashing alarm object(s). The background color for each alarm notification level shall be customizable to allow easy identification of certain alarm types or alarm states.

f. Sounding of an audible beep or playing an audio file on alarm initiation or return to normal.

3. The following shall be recorded by the Front end for each alarm (at a minimum):

a. Time and date

b. Location (building, floor, zone, office number, etc.)

c. Equipment (reader #, IOM point #, etc.)

d. Acknowledge time, date, and user who issued acknowledgement.

4. A log of all alarms shall be maintained by the Front End server (if configured in the system) and shall be available for review by the user.

2.15 EVENT NOTIFICATIONS AND ACTIONS LOG (EACS & FMCS)

A. A separate log for System Event Transactions shall be provided and available for review by the user.

B. Every System Event shall be time stamped with the time of occurrence and shall be recorded in the Event Log. Time stamping shall include the date, and be to the nearest second

C. All operator initiated actions shall be recorded in the Event Log. Each operator action event logged to Event Log shall be stamped with time of day and operator ID. The Event Log shall include all details of any change that an operator has carried out.

D. Provide and maintain an Event Log that tracks all activities performed. Provide the ability to specify a buffer size for the log and support a minimum of 5,000 transactional system events.

2.16 APPLICATION HELP (EACS & FMCS)

A. The system software shall have on-line help available at any point requiring operator input. The help screen shall be accessible by clicking on the Help button located on the page in view. This help screen shall provide detailed information about every property on the screen. Examples and screen captures will be available to assist in operator comprehension.

B. The on line help shall be context sensitive and automatically direct the user to the appropriate help section based on current location within the application software.

2.17 GUIDED WIZARD SETUP (EACS & FMCS)

A. The system shall provide an easy to use guided wizard setup to assist the user with initial product setup. The guided setup shall step the user through hardware setup, personnel database creation, and other pertinent system administration functions. The wizard shall be available by default on initial connection to the NSC and will remain available until completed. The system shall allow the guided wizard to be manually restarted at a later time if reconfiguration is required.

2.18 APPLICATION USER PROFILES (EACS & FMCS)

A. Each operator shall be given a profile as part of the operator definition. Profiles consist of a group of web pages that determine the look and feel of the user interface and the functionality that is to be assigned to each operator. Standard profiles shall include as a minimum:

1. System Administrator – Shall have full control to entire application.

2. Maintenance User – Shall have access to all sections of the application but cannot access or make changes to the system administrator account.

3. Badge Operator – Shall have access to the reports and personnel sections of the application.

4. Console Operator – Shall have access to the alarm console and reports sections of the application.

B. When an operator logs out of a workstation and a new operator logs on, the profile displayed on the workstation screen shall be automatically updated to the setting for that new operator.

C. Each profile shall provide operators with the ability to perform manual operations consistent with their area (s) of responsibilities. Manual operations available to profiles shall include as a minimum:

1. Running or printing reports
2. Locking/unlocking of doors
3. Adjusting time schedules
4. Setting / resetting control outputs
5. Creating system objects including cardholders, doors, and monitoring points

D. For each manual operation by the operator, the Activity Log will automatically record the action for display by the System Administrator or other authorized user.

2.19 GRAPHICS (EACS & FMCS)

A. The system shall provide a graphic subsystem that allows for the creation of real time graphic displays through the addition of animations over an imported background image. The output of each graphic will display and operate in any browser workstation. Animations will be used to display real time information (point status, alarms, etc.), to control system devices (doors, outputs, etc.). Standard graphics shall include as a minimum:

   1. Floor plans
   2. Maps
   3. Building views (internal and external)
   4. Readers
   5. Inputs
   6. Outputs

B. The system shall permit the use of standard background formats including .BMP, JPEG, and .GIF. The system must have ability to upload images and stored.

C. The system shall include an editor to build run time graphics. The graphics editor shall be executed and no 3rd party software shall be required to add/delete/modify graphics. The editor shall include tools for adding and formatting text, adding and formatting backgrounds, and creating animations. All functions are to be performed with a mouse.

D. Completed graphics may be selected from an object tree, menu, or in response to an alarm event. Upon display, the graphic will automatically poll its associated data points and refresh the data at user specified intervals.

E. All graphics will be stored on the embedded web server and served up to each browser workstation upon demand.

2.20 REPORTS (EACS & FMCS)

A. The system shall provide standard reports for all system transactional data and the means to create custom reports. Reports shall be accessed from the navigation tree within the application. Standard reports required at a minimum shall include:

   1. Access History
   2. Audit History
   3. Log History
   4. General Activity
   5. Attendance History
   6. Hardware Reports

B. The system shall allow the user to review reports in a variety of methods including:

1. Display report results on screen

2. Export results to .CSV file format

3. Export results to .PDF format.

C. The system shall allow the user to customize the .PDF report file properties. At a minimum, the user shall be able to modify the title bar image, modify font size, style, and color.

D. Depending upon the type of report being generated by the system operator, the system shall provide a listing of previously defined reports. The operator shall be able to pick an existing report, modify an existing report or generate and save a new report.

E. The system shall allow an operator to define and save reports and the contents contained within the report. There shall be no limit to the number of user defined reports. Based upon the type of report being created, the system shall provide a pick list of items that may be included within the report. This list shall include all possible attributes defined for each report (i.e. controller, doors, personnel, etc.).

2.21 DATABASE BACKUP AND STORAGE (EACS & FMCS)

A. The NSC shall have the ability to backup its database.

B. Copies of the current database and, at the most recently saved database shall be stored in the NSC or on designated network PC. The age of the most recently saved database is dependent on the user-defined database save interval.

C. The NSC database shall be stored in XML format to allow for user viewing and editing, if desired. Other formats are acceptable as well, as long as XML format is also supported.

2.22 SYSTEMS INTEGRATION (EACS & FMCS)

A. The EACS shall include objects to support the integration of FMCS (Carrier I Vue Open) data to a BACNet TCP/IP based EACS. The connection to the BACNet system shall be via an Ethernet IP as required by the NSC. At a minimum, define the following BACNet TCP/IP data points as part of the standard EACS and a complete points list must be provided in the bid documentation:

1. Door Status:

   a. Door Open and Door Closed

2. IOM data Status:

   a. Status of all Inputs

   b. Status of all Outputs

3. The NSC supplier shall provide a BACNet TCP/IP system communications driver. The FMCS vendor utilizing BACNet shall provide documentation of the system's BACNet interface to the EACS and shall provide factory support at no charge during system commissioning

4. Equipment & IOM Status:
   a. Equipment on or off
   b. Status of all inputs

c.Status of all Outputs
d. Outside Air Temperature
e. Thermostat Set Point
f. Alarms

3. PART 3 EXECUTION

3.1 INSTALLATION & PAST PERFORMANCE (EACS & FMCS)

A. All work described in this section shall be performed by system integrators or contractors that have a successful history in the design and installation of integrated security and control systems. The installing office shall have a minimum of five years of integration experience and shall provide documentation in the submittal package verifying the company's certification in Honeywell Web's AX and Carrier Controls. A list of 3 references where the installing company has successfully integrated control systems to the Honeywell Web's AX platform must be provided. Prime Contractor must have a certified energy manager on staff that is fully knowledgeable in the programming of control systems and how to best optimize the FMCS to ensure energy savings. Certification of the Energy Manager must be provided.

B. Install system and materials in accordance with manufacturer's instructions, and as detailed on the project.

C. Drawings of EACS network are diagrammatic only and any apparatus not shown, but required to make the system operative to the complete satisfaction of the owner shall be furnished and installed without additional cost.

D. Line and low voltage electrical connections to control equipment shown specified or shown on the control diagrams shall be furnished and installed by the Electrical contractor in accordance with the specifications.

E. The FMCS Contractor must be the prime contractor on the project as the City of Mt. Pleasant will only issue one purchase order for this integration work. The prime contractor must provide a list of sub contractors they are using on the job as well as the sub contractors references and certifications in accordance with section A. above.

3.2 WIRING

A. All wiring shall be in accordance with the Project Electrical Specifications the National Electrical Code and any applicable local codes. All EACS wiring shall be installed in the conduit types specified in the Project Electrical Specifications unless otherwise allowed by the National Electrical Code or applicable local codes. Where EACS plenum rated cable wiring is allowed it shall be run parallel to or at right angles to the structure, properly supported and installed in a neat and workmanlike manner.

3.3 WARRANTY

A. Equipment, materials and workmanship incorporated into the work shall be warranted for a period of one year from the time of system acceptance. During this time the prime contractor is responsible for tracking energy use and consumption and will provide two reviews of FMCS programming to continually reduce energy costs at the public safety building.

B. Within this period, upon notice by the Owner, any defects in the work provided under this section due to faulty materials, methods of installation or workmanship shall be promptly (within 48 hours after receipt of notice) repaired or replaced by the contractor at no expense to the Owner

3.4 WARRANTY ACCESS

A. The Owner shall grant to the Prime contractor, reasonable access to the system during the warranty period. The owner shall allow the contractor to access the system from a remote location for the purpose of diagnostics and troubleshooting, via the Internet, during the warranty period.

3.5 ACCEPTANCE TESTING (EACS & FMCS)

A. Upon completion of the installation, the prime contractor shall load all system software and start-up the system. The contractors shall perform all necessary calibration, testing and de-bugging and perform all required operational checks to insure that the system is functioning in full accordance with these specifications. When appropriate, sub contractors are to coordinate the checkout of the system when interlocks between systems are present. Ensure that each contractor has a representative present during the portion of system checkout that affects them.

B. The contractors shall perform tests to verify proper performance of card access and intrusion alarm strategies. Repeat tests until proper performance results. This testing shall include a point-by-point check out to validate 100% of the input and output points and each of the card access strategies, area groupings and reporting/logging.

C. Upon completion of the performance tests described above, repeat these tests, point by point in presence of Owner's Representative, as required. Properly schedule these tests so testing is complete at a time directed by the Owner's Representative. Do not delay tests so as to prevent delay of occupancy permits or building occupancy.

D. System Acceptance: Satisfactory completion is when the prime contractor has performed successfully all the required testing to show performance compliance with the requirements of the Contract Documents to the satisfaction of the Owner’s Representative. System acceptance shall be contingent upon completion and review of all corrected deficiencies.

3.6 OPERATOR INSTRUCTION, TRAINING (EACS & FMCS)

A. During system commissioning and at such time acceptable performance of the hardware and software has been established the Temperature Control sub-contractor shall provide on-site operator instruction to the owner's operating personnel. Operator instruction shall be done during normal working hours and shall be performed by a competent representative familiar with the system hardware, software and accessories.

B. The contractors shall provide 8 hours of instruction to the owner's designated personnel on the operation of the EACS and describe its intended use with respect to the programmed functions specified. Operator orientation of the systems shall include, but not be limited to; the overall operation program, credential management, alarm management, interlocking, area control, systems integration, card access strategies, reporting and appropriate operator intervention required in responding to the System's operation.

C. The training shall be a one day session (or as specified) after system is started up and at least one week before first acceptance test. Manual shall have been submitted at least one week prior to training so that the owners' personnel can start to familiarize themselves with the system before classroom instruction begins.

Mandatory Pre-Bid Walk: Tuesday January 22, 2013 at 9:00 AM at 804 E. High Street Mt. Pleasant, MI 48858

Bid Due Date: Sealed bids must be received in the office of the Mt. Pleasant City Clerk, 320 W. Broadway, Mt. Pleasant, MI 48858 no later than 1:30 PM on Tuesday February 5, 2013.

Questions will only be accepted in writing to Gregory L. Walterhouse, Fire Chief gwalterhouse@mt-pleasant.org