`

CITY OF DEL CITY AND/OR
DEL CITY MUNICIPAL SERVICES AUTHORITY (DCMSA)

REQUEST FOR PROPOSAL

Mail proposals to: FINANCE DEPARTMENT
PURCHASING DIVISION
3701 SE 15TH ST, DEL CITY, OK 73115

Proposal for:	**RFP 1807**	**Electronic Access Control and Intrusion Detection System for the new City of Del City Central Fire Station and Fire Administration Building**

Due / Opening Date: Tuesday, Oct 10, 2017 Time: 10:00 AM

Vendor Name: _____

Mailing Address: _____

City, State, Zip: _____

Area Code, Phone: _____ Fax:_____ FEI#: _____

E-mail Address: _____ Website: _____

The City of Del City ("City") and/or Del City Municipal Services Authority ("DCMSA") is requesting Proposals for the attached specified products and/or services. The following document contains the terms and conditions which constitute the contract for the specified product and or service, including the minimum specifications. The contract will be awarded to the lowest and best bidder, as determined by the City of Del City and/or Del City municipal Services Authority. Submit all documents requested to the PURCHASING DIVISION at the above address. Place of opening Municipal Building 3701 SE 15TH ST , Del City, OK.

`

NONCOLLUSION AFFIDAVIT

PROPOSAL INVALID IF AFFIDAVIT NOT SIGNED AND NOTARIZED

State of _____

County of _____

I _____ of lawful age, being first duly sworn, on oath says that:

1. (s)he is the duly authorized agent of _____ the Bidder/Contractor ("Contractor") submitting the proposal which is attached to this statement, for the purpose of certifying the facts pertaining to the existence of collusion among contractors and between contractor and city officials or employees, as well as, facts pertaining to the giving or offering of things of value to government personnel in return for special consideration in the letting of any contract pursuant to the proposal to which this statement is attached; 2. (s)he is fully aware of the facts and circumstances surrounding the making of the proposal and/or the procurement of the contract to which this statement is attached and has been personally and directly involved in the proceedings leading to the submission of such proposals; and 3. Neither the contractor nor anyone subject to the contractor's direction or control has been a party; a. to any collusion among contractors in restraint of freedom of competition by agreement to proposal at a fixed rate or to refrain from proposing, b. to any collusion with any city official or employee as to quantity, quality or price in the prospective contract, or as to any other terms of such prospective contract, nor c. in any discussions between contractors and any city official concerning exchange of money or other thing of value for special consideration in the letting of a contract, d. to paying, giving or donating or agreeing to pay, give or donate to any officer or employee of the City of Del City and/or the Del City Municipal Services Authority, any money or other thing of value, either directly, in procuring the contract to which his/her statement is attached.

Signature: _____ Title: _____ Subscribed

& sworn before me this _____ day of _____, 20 _____

Notary Public _____ My commission expires _____

PROPOSAL/CONTRACT

TERMS AND CONDITIONS

1. PROPOSAL: Proposals must be submitted by the Bidder/Contractor ("Contractor") on and in accordance with the PROPOSAL/CONTRACT. All sheets bid on and this form must be executed and submitted in a sealed envelope. DO NOT INCLUDE MORE THAN ONE PROPOSAL PER ENVELOPE. The face of the envelope shall contain the City's address, the date and time of the bid opening and the contract number. Proposals not submitted on attached bid form shall be rejected. All Proposals are subject to the conditions specified herein. Proposals which do not comply with said conditions specified herein are subject to rejection. Proposals will be considered only on first quality products.

2. PROPOSAL ACCEPTANCE PERIOD: Proposals received after the opening date and time will not be considered.

3. EXECUTION OF PROPOSAL: Proposal must contain an original signature of authorized representative in the spaces provided. Proposal must be typed or printed in ink. Use of erasable ink and penciled proposals will not be accepted. ANY AND ALL CORRECTIONS MADE BY PROPOSER TO HIS/HER PROPOSAL MUST BE INITIALED.

4. NO PROPOSAL: If not submitting a proposal, respond by returning page 1, Request for Proposal, marking it "NO PROPOSAL", Failure to respond three (3) times in succession without justification shall be cause for removal of the vendor's name from the proposal mailing list. NOTE: To qualify as a respondent, proposal must submit a "NO PROPOSAL" and it must be received no later than the stated proposal opening date and time.

5. OPENING: Proposals will be opened by the Purchasing Officer and distributed to the requesting department for review and recommendation for award and submitted to the City Council for award. It is the contractor's responsibility to assure that his/her proposal is delivered at the proper time, date and place as specified in the documents. Proposals, which for any reason are not so delivered, will not be considered. NOTE: Proposal files may be examined during normal working hours by appointment. PROPOSAL TABULATIONS WILL NOT BE PROVIDED BY TELEPHONE OR MAIL. TABULATIONS MAY BE OBTAINED BY VISITING www.DemandStar.com ON THE INTERNET OR AT OUR WEBSITE www.cityofdelcity.com.

6. PRICES, TERMS AND PAYMENT: Firm prices shall be bid F.O.B. requesting agency and include packing, handling and shipping charges fully prepaid by the vendor.

A. PROPOSAL PRICE/MISTAKES: The proposal shall show in the proposal both the unit price and the total amount on items when indicated. In the event of discrepancy between the unit price and the extension, THE UNIT PRICE SHALL PREVAIL. Prices shall be extended in decimals.

B. INVOICING AND PAYMENT: The vendor shall be paid upon submission of proper certified invoices to the ordering agency at the prices stipulated on the contract. Invoices shall contain the purchase order number. THE VENDOR SHALL ACCEPT NO ORDER WITHOUT A PURCHASE ORDER NUMBER FROM THE CONTRACTING ENTITY.

C. TAXES: The purchase of certain items by the City/DCMSA are exempt from the payment of excise, transportation and sales tax imposed by the Federal, State and/or City governments. Such taxes must not be included in proposal prices. Upon request, applicable Federal Excise Exemption certificates will be furnished.

7. CONDITION AND PRICING: It is understood and agreed that any item offered or shipped as a result of this bid shall be new (current model at the time of this bid). All containers shall be suitable for storage or shipment and all prices shall include standard commercial packaging.

8. SAFETY STANDARDS: Unless otherwise stipulated in the bid, all manufactured items or fabricated assemblies shall comply with applicable requirements of occupational Safety and Health Act and any standards thereunder.

9. MANUFACTURER'S NAMES AND APPROVED EQUIVALENTS: Unless qualified by the provision "NO SUBSTITUTE" any manufacturers' names, trade name, brand names, information and/or catalogue numbers listed in a specification are for information and not intended to limit competition. The Contractor may offer any brand for which (s)he is an authorized representative, which meets or exceeds the specification for any item(s). If proposals are based on equivalent products, indicate in the proposal form the manufacturers' name and number. Contractor shall submit with his/her proposal, sketches, and descriptive literature, and/or complete specifications. Reference to literature submitted with a previous proposal will not satisfy this provision. The Contractor shall also explain in detail the reason(s) why the proposed equivalent will meet the specifications and not be considered an exception thereto. Proposals, which do not

comply with these requirements, are subject to rejection. Proposals lacking any written indication of intent to quote an alternate brand will be received and considered in complete compliance with the specification as listed on the bid form.

10. AWARDS: The City reserves the right to make award(s) by individual item, group of items, all or none, or any combination thereof; on a geographical basis and/or on a statewide basis with one (1) or more suppliers; to reject any and all proposals or waive any minor irregularity or technicality in proposals received. Contractors are cautioned to make no assumptions unless their proposal has been evaluated as being responsive. The City reserves the right to delete any item from this contract when deemed to be in the best interest of the City.

11. SERVICE AND WARRANTY: Unless otherwise specified, the Contractor shall define any warranty service and replacements that will be provided during and subsequent to this contract. Contractors must explain on an attached sheet to what extent warranty and service facilities are provided.

12. SAMPLES: Samples of items, when called for, must be furnished free of expense. Each individual sample must be labeled with contractor's name, manufacturers' brand name and number, contract number and item reference, or as specified in the attached special conditions.

13. NONCONFORMANCE TO CONTRACT CONDITIONS: Items may be tested for compliance with specifications by appropriate testing laboratories. The data derived from any tests for compliance with specifications are public records and open to examination thereto in accordance with Oklahoma Statutes. Items delivered not conforming to specifications may be rejected. Any violation of these stipulations may result in supplier's name being removed from the City and or DCMSA vendor list.

A. TESTING: In cases when material fails to meet specifications the cost of testing shall be borne to the vendor, both on samples and delivered materials.

14. INSPECTION, ACCEPTANCE AND TITLE: Inspection and acceptance will be at destination unless otherwise provided. DESTINATION: Shall mean delivered to the receiving dock, agency stockroom, or other point specified in the purchase order. The City accepts no responsibility for goods until accepted at the receiving point in good condition. Title and risk of loss or damage to all items shall be the responsibility of the contract supplier until accepted by the ordering agency, unless loss or damage results from negligence by the ordering agency. The contract supplier shall be responsible for filing, processing and collecting all damage claims. However to assist in the expeditious handling of damage claims, the ordering agency will:

a) Record any evidence of visible damage on all copies of the delivering carrier's Bill of Lading.

b) Report damage (visible and concealed), in writing, to the carrier and contract supplier, within fifteen (15) days of delivery.

c) Retain the item and its shipping container including inner packaging material, until inspection is performed by the carrier, and disposition given by the contract supplier.

d) Provide the contract supplier with a copy of the carrier's Bill of Lading and damage inspection report.

15. PATENTS AND ROYALTIES: The contractor, without exception, shall indemnify and save harmless the City/DCMSA and its employees from liability of any nature or kind, including cost and expenses for or on account of any copyrighted, patented, or unpatented invention, process, or article manufactured or used in the performance of the contract including its use by the City/DCMSA. If the Contractor uses any design, device or materials covered by letters, patent copyright, it is mutually agreed and understood without exception that the bid prices shall include all royalties or cost arising from the use of such design, device, or materials in any way involved in the work.

16. PRICE ADJUSTMENTS: Manufacturers' price increases, or other increases in the cost of doing business may not be passed on to the City/DCMSA unless so specified in the Request for Proposal, nor may the vendor withdraw or cancel the contract, or any part of the contract for these reasons. Vendors may cancel contract only if a vendor cancellation clause is included as a part of the Request for Proposal and then only if the contractual obligation has been fulfilled by the vendor in accordance with the terms stated in the Request for Proposal. Any price decrease effectuated during the contract period by reason of market change shall be passed on to the City.

17. LIABILITY: The supplier shall hold and save the City/DCMSA, its officers, agents and employees harmless against the claims by third parties resulting from the supplier's breach of this contract or the supplier's negligence.

18. FACILITIES: The City/DCMSA reserves the right to inspect the contractor’s facilities at any time with prior notice.

19. THE SUCCESSFUL CONTRACOR(S) MUST PROVIDE: Only the pertinent information or items you are bidding. Complete catalogues are not necessary - but, if furnished, you are to identify exact location in catalogue and circle or identify clearly item(s) being bid.

20. IN-STATE PREFERENCE: An in-state preference not to exceed a five percent (5%) differential may be allowed for supplies, materials and provisions produced, manufactured or grown in this State, 74 O.S. 85.32. If you wish to claim this preferential, place an asterisk (*) by each item so claimed and identify whether it is produced, grown or manufactured in Oklahoma. Proof of qualification rests with the vendor.

21. WAVIER: The City/DCMSA reserves the right to waive any General provisions, Special Provision, or minor specification deviation when considered to be in the best interest of the City/DCMSA.

22. QUANTITIES: Quantities of the commodities to be purchased are set forth in the specifications as specified numbers or estimates. Items of estimated quantity will be awarded on a "NO GUARANTEE" basis.

23. TERMINATION FOR CONVENIENCE OF THE CITY/DCMSA: The performance of work and/or the delivery of ordered materials under this contract may be terminated by the City/DCMSA, in whole or in part, whenever it is determined to be in the best interest of the City/DCMSA. Any such termination shall be effected by delivery to the vendor of a notice of termination specifying the extent to which performance of work and/or delivery of ordered materials is terminated, and the date upon which such termination becomes effective. After receipt of a notice of termination, the contractor shall stop work and/or place no further orders under the contract on the date and to the extent specified in the notice of termination.

It is not the intent of the City of Del City and/or Del City Municipal Services Authority to deny anyone the opportunity to bid. Alternate specifications may be accepted if found by technical personnel to be in accordance and equal to or better than the specifications described and indicated in the proposal package.

INFORMATION:

For further information contact Brandon Pursell (405) 671-2895 dcfd103@sbcglobal.net

PROPOSAL IN REPLY TO SPECIFICATIONS:

No.	***Description***	***Price***
	Electronic Access Control and Intrusion Detection System	***$***

*** THIS SECTION FOR CORPORATION ONLY ***

AFFIX CORPORATE SEAL HERE

ATTEST:

_____
Name of Corporation (as on official seal)

_____ By_____
Corporate Secretary or Assistant Signature — Elected Corporate Official Signature and Title

_____ _____
Type or Print Name — Type or Print Name

*** THIS SECTION FOR ALL BUSINESSES OTHER THAN CORPORATIONS**

Dba _____ _____
Owner/Partner (Type or Print Name) — Name of Business

By_____ _____
Owner/Partner Signature — Type or Print Name

STATE OF _____
COUNTY OF _____

Before me, the undersigned, a notary public in and said State, on this _____ day of _____, 20___, a member of the firm of _____to me known to be the identical person who executed the within and foregoing instrument on behalf of said firm and to acknowledge to me that (s)he executed the same as his/her free and voluntary act and deed, and as the free and voluntary act and deed of said firm, for the purposes therein set forth,

_____ _____ _____
Notary Public — Commission Expiration — Commission Number

*** THIS SECTION FOR CITY/DCMSA ONLY ***

CITY OF DEL CITY — DEL CITY MUNICIPAL SERVICES AUTHORITY

_____ _____
By Mayor — By Chairman

AFFIX SEAL — AFFIX SEAL
Attest: — Attest

_____ _____
City Clerk — Secretary

SECTION 28 10 00 VELOCITY ELECTRONIC ACCESS CONTROL AND INTRUSION DETECTION SYSTEM (EACIDS) WITH INTEGRATED CCTV SYSTEM

GENERAL

RELATED DOCUMENTS

General: Drawings and General Provisions of the Contract, including General and Supplementary Conditions and Special Provisions, apply to this section. Also provide the work in accordance with the Section 28 05 00, Common Work Results for Electronic Safety and Security and Division 26 Electrical.

DESCRIPTION

General Description: This specification section covers the furnishing and installation of a complete Velocity EACIDS version 3.6 that is an expansion and upgrade to the existing Identiv Velocity EACIDS version 3.5.

Contractor shall furnish and install security hardware devices, mounting brackets, power supplies, switches, controls, consoles and other components of the system as shown and specified.

Contractor shall furnish and install all outlets, junction boxes, conduit, connectors, wiring, and other accessories necessary to complete the system installation.

Related Work

07 00 00 – Thermal and Moisture Protection (Division 7)

Section 07 84 00 – Firestopping

08 00 00 – Opening (Division 8)

Section 08 71 00 – Door Hardware

26 00 00 – Electrical (Division 26)

26 05 00 – Common Work Results for Electrical

26 05 06 – Grounding and Bonding

26 05 29 – Hangars and Supports

26 05 33 – Raceways and Boxes

27 00 00 – Communications (Division 27)

27 05 00 – Common Work Results for Communications

27 05 26 – Grounding and Bonding for Communication Systems

27 05 28 – Pathways for Communication Systems

27 05 29 – Hangars and Supports for Communication Systems

27 05 33 – Conduit and Backboxes for Communication Systems

27 05 39 – Surface Raceways for Communication Systems

28 00 00 – Electronic Safety and Security (Division 28)

28 05 00 – Common Work Results for Electronic Safety and Security

28 13 26 – Access Control Remote Devices

SHOP DRAWINGS & EQUIPMENT SUBMITTAL

Provide the work in accordance with Section 28 05 00, Common Work Results for Electronic Safety and Security.

OPERATIONS AND MAINTENANCE MANUALS

Provide the work in accordance with Section 28 05 00, Common Work Results for Electronic Safety and Security.

WARRANTY

Provide the work in accordance with Section 28 05 00, Common Work Results for Electronic Safety and Security.

TRAINING

Provide the work in accordance with Section 28 05 00, Common Work Results for Electronic Safety and Security.

EQUIPMENT COMPATIBILITY REQUIREMENTS

Provide the work in accordance with Section 28 05 00, Common Work Results for Electronic Safety and Security.

TECHNICAL REQUIREMENTS, VELOCITY EACIDS

General: The following information is provided to establish required system performance for the complete operating Velocity EACIDS. Contractor shall provide equipment, wiring, and software programming, as necessary, to provide a complete system as described herein and as shown on the drawings.

Contractor shall be responsible for providing equipment and software to achieve the specified system performance described herein and, by reference, realize absolute and seamless compatibility with the existing system.

Contractor shall ensure that modifications provided under this scope of work have no negative effect on the existing systems and operations, and no permanent effect beyond that specified or implied by the scope of work unless otherwise noted herein.

Attributes

The system shall comprise Electronic Access Control System field devices located as shown on the drawings and connected together to provide a complete and operational system.

The Velocity EACIDS shall be based on a distributed system of fully intelligent, stand-alone controllers, operating in a multi-tasking, multi-user environment.

The Velocity EACIDS shall utilize a single seamlessly integrated relational database for all functions utilizing a fully multi-tasking multi-threading Microsoft Windows Server environment and utilize SQL Server as the database engine.

The Velocity EACIDS shall function as an Electronic Access Control System and shall integrate alarm monitoring, ID badging and database management into a single platform. A modular and network-enabled architecture shall allow maximum versatility for tailoring secure and dependable access and alarm monitoring solutions.

The Velocity EACIDS shall be a modular and network-enabled access control system. The Velocity EACIDS shall be capable of controlling multiple remote sites, alarm monitoring, video imaging, ID badging, emailing of events and alarms, digital video and CCTV switching and control that allows for easy expansion or modification of inputs and remote control stations. The Velocity EACIDS 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. Velocity EACIDS reconfiguration shall be accomplished online through system programming. The Velocity EACIDS shall include the following:

Multi-User/Network Capabilities: The Velocity EACIDS 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 shall have the capability to log on to workstations and remotely configure devices from the workstation. Standard operator permission levels shall be enforced, with full operator audit.

Licensing: The system shall include a license that provides unlimited number of doors, readers and alarm points, and the following features: Photo ID badging, Graphics, Alarm Monitoring, unlimited number of clients, unlimited WEB client console for mobiles devices, and advanced feature set.

There shall be no additional licenses required to expand the number of readers, inputs, outputs, client workstations or web client console connections. Systems that shall require additional licensing for standard expansion shall not be accepted.

Relational Database Management System: The Velocity EACIDS shall support industry standard relational database management systems. This shall include relational database management system Microsoft SQL Server Express. Full versions of SQL are supported at additional cost.

System Partitioning: The Velocity EACIDS shall provide the option to restrict access to sensitive information by Roles. The Velocity EACIDS shall support dynamic partitioning. A Velocity EACIDS in which partitions are set up at installation and cannot be easily changed shall not be acceptable.

The Velocity EACIDS shall have an LDAP Integration that will run as a Windows Service and listen for log entries written by Active Directory to the domain controller's Event Logs for AD user adds, updates, and deletes to synchronize Velocity EACIDS users and credentials in real time. In addition, LDAP Integration will poll Active Directory on a scheduled basis for AD user changes as a secondary measure to ensure synchronization. LDAP Integration will include a configuration application to configure synchronization rules and physical access. Basic features of Active Velocity include (but are not limited to):

Automatic synchronization of AD and Velocity EACIDS users in real time.

Disable/Enable Velocity credentials for physical access based on status of AD users. For example, if an AD user is disabled, LDAP integration will disable all credentials associated with the AD user resulting in no physical access to any doors on the premise secured by Velocity EACIDS.

Map AD fields to Velocity EACIDS User Defined Fields (UDFs) through LDAP integration configuration. Changes made to AD user fields will be synchronized with associated Velocity EACIDS UDFs

Add/Update/Delete performed on AD users will be synchronized with associated Velocity EACIDS user.

Auto provision physical access to a user's credential based on AD user's job code or assigned AD user field. LDAP integration will make use of Velocity EACIDS Credential Templates to assign default access based on the AD user's position or group name (to be decided by customer).

Unicode: The Velocity EACIDS shall utilize Unicode worldwide character set standard. The Velocity EACIDS shall support double-byte character sets.

Encryption: The Velocity EACIDS shall provide multiple levels of data encryption

True 128-bit AES data encryption between the host and controllers. The encryption shall ensure data security 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 Velocity EACIDS based on a successful match.

Transparent database encryption, including log files and backups

SQL secure connections via SSL

Supervised Alarm Points: Both supervised and non-supervised alarm point monitoring shall be provided. Upon recognition of an alarm, the system shall be capable of switching CCTV cameras that are associated with the alarm point.

Alarm Monitoring Supervision: The system shall support input point supervision. The sensitivity of the line supervision shall be 2% AA Standard. End-of-Line modules shall be placed at the device end only. The system shall display the following alarm point monitoring functions:

Normal

Forced Entry

Alarm

Door Open too Long (Door Prop)

Noisy

Short

Out-of-Spec

Tamper

Windows Authentication Login: The Velocity EACIDS shall use an integrated authentication method which utilizes Windows user accounts and policies.

Roles

The Systems Administrator defines the Operator Role that allows permissions for each specific component of the system. The System Administrators can assign one or more Roles to an Operator. These roles authorize which workstation and what the Operator is allowed to see and do within the EAC.

Options:

Each system component will have a set of Options specific to that component. The System Administrator defines which Options are available for each User.

Standard Options for each component shall be Add, Delete, Save, and Edit

System Components Shall Include:

Application Permission: Identifies which modules are visible to an Operator and which tasks within the application are available.

Cameras can be assigned or restricted by role.

Command Sets: Control over any point or points through a single mouse click

Credential Templates: Pre-defines access and all attributes within Enrollment except the specific card or PIN

Controller Hardware: Each point is subject to a permission by Time Zone

Door Groups: Access through Reader + Time Zone in multiple combinations

Event Viewer Filters: Events may be routed and specified to a single workstation and down to a single event

FICAM Card Validation Profiles: Displays a list of all currently defined FICAM card validation profiles

Function Groups: Multiple functions both control and access, pre-defined utilizing keypad and may be assigned to multiple PINS that assume the same functionality

Graphics: Live state changes in graphical format

Person Groups: Segregation of the Enrollment Manager database and may limit to a single Person Group by Operator Role

Person Templates: Auto populate customer defined fields for Enrollment Manager

Reports: 112 basic reports with SQL statement capability for creating custom reports

Status Viewer Groups: Built in filters for monitoring one or multiple points in any combination. Allows access to all properties and functions

Video Explorer Groups shall enable pre-configured camera views on system launch.

Alarm and Event Routing can be defined by Operator Role. Specific alarms and events can be routed by Time Zone to Operators to allow for only those Operators needing to see certain alarms and events to see them

Operators: Operators entered into the system shall take on the properties of the Roles to which they are assigned. If the Operator is already defined in the Operating System, the “Find” feature can be used to select this Operator for use in Velocity

Switch Operator: There shall be the capability to change Operators without the need for the current Operator to Log Off the computer. The new Operator’s permissions are then used during the session to control access to Velocity EACIDS functionality

Information Access: The Velocity EACIDS shall be capable of limiting operator access to sensitive information. Operators must have proper authorization to edit the information.

Graphical User Interface: The Velocity EACIDS shall be fully compliant with Microsoft graphical user interface standards, with the look and feel of the software being that of a standard Windows application, including hardware tree-based system configuration.

Status Viewer: The software shall include a Status Viewer which will display real-time status of all or selected Doors, Readers, Inputs, Relays, Expansion Inputs, Expansion Relays, and Controllers. Devices may be grouped into "Status Groups", which are selectable from a drop down list. Authorized operators shall be capable of right clicking each point to control the point to change the complete properties including the ability to mask/unmask alarms, trigger relays, access and control the doors, view the state of the relay and line module voltage. Devices may have selected information displayed. Filtering of components shall be built into the Status viewer. The available information includes the following:

Name and Address

Status

Alarm and Acknowledged Status

Masking Status

Line Module Input Status and Type

Relay Status

Detailed Relay Status

Controller Threat Level Status

Revision Number

Enables Status

Controller Alarm Relay, Tamper, and Battery Status

Alarm Viewer

The Alarm Viewer shall have 4 panes: Alarm, Acknowledged Alarms, Instructions, and Comments. Counters will indicate Active Alarms, Acknowledged Alarms, and Off Normal Conditions. The Alarm Viewer may be manually launched or launched automatically in the event of a new alarm occurrence. Alarm Viewer properties that may be configured include:

Require Acknowledgement before Clearing Auto

Acknowledge on RTN (Return to Normal)

Require Entry of Note on Acknowledgement

Force New Note on Multiple Acknowledgements

Require Entry of Note on Clear

Force New Note on Multiple Clear

Restore Alarm Viewer on New Alarm

Specify the number of Cached Alarms to Load at Launch of Alarm Viewer

Foreground, Background, Alarm, and Secure colors may be changed. In addition, the Columns of data viewed in the Alarm and Acknowledged windows may be selected, and the sequence in which they will appear.

Right-Clicking an Alarm Event shall display a list of available options, including

Acknowledge Selected/All

Clear Selected/All

Add Operator Note

Go To Graphic

Display Credential (User Photo)

Replay WAV file

NVR Alarm Video: Show Viewer, and Get Recorded Alarm Video

Event Viewer

The Event Viewer can display all or Filtered Transactions. Custom filters may be defined and selected, or Standard selections can be made for main categories of Event types. Column width, order, selection, and scrolling direction are user definable, as well as text and background color.

The number of cached events to load when launched (up to 10,000) may be defined. The Operator shall be able to scroll back in time to view events no longer seen on the screen, without the need for running a report.

Keyboard Shortcuts: The Velocity EACIDS shall allow the user to use a shortcut key to enable designated system commands.

User Functions and ADA Ability: The Velocity EACIDS shall provide user functions and ADA (Americans with Disabilities Act) ability that provides the capability to trigger an event at the Velocity EACIDS intelligent controller when a defined card is presented.

Boolean Logic Functions: The system shall support Boolean algebra logic function programming. The system shall support 'AND', 'OR', and 'IF/THEN' programming function for any input/and/or output device in the system.

Report Manager

The Report Manager shall allow the Operator to select from a number of pre-defined Reports. Custom Reports can be created outside the software, and added to a Custom folder, making the Custom Reports available from within the Report Manager application.

When a Report is selected, the default Criteria and Sorting options may be used, or custom Criteria and Sorting options may be selected. The report criteria can be optionally displayed on the top of the report.

After the report is run, it may be viewed, printed, or saved in various standard file formats.

Standard Reports: Provide a minimum of the following standard reports, completely configured, formatted and linked to the system database:

- Customization Reports
  - Component Resources
  - Customizations Reports
- Hardware Configuration
  - Controllers
  - Doors
  - Expansion Inputs
  - Expansion Relays
  - Inputs
  - Network Layout
  - Printers
  - Readers
  - Relays
- History Logs
  - Active Alarms by Date
  - Alarm Log by Date
  - Alarm Log by Date with Comments
  - All Events Log
  - External Events Log
  - Internal Events Log
  - Operator Log
  - User Activity Log
- User Information
  - Credential Status
  - Door Access by Person
  - Dossier Style by Person
  - Expired and To-Be-Expired Person Access
  - Expired Credentials
  - Last Access by Person
  - Person Access and Function Group Summary
  - Person Access and Function Group Summary with Codes and Cards
  - Person Access by Door
  - Person Access Summary
  - Person Access Summary with Codes and Cards

Person FG Summary with Codes and Cards

Person Function Group Summary

Who Is Inside Where

Software Configuration

Command Sets

Door Groups

Function Group Extensions

Functions Groups with Users

Functions with Users

Holiday Schedules

Holidays

Master Door Groups

Master Door Groups with Persons

Operator Groups

Operators

Time Zones – Grand Master Time Zone

Time Zones – Master Time Zone

Time Zones – Standard Time Zone

Time Zones – Standard Time Zones in Use

Reports – Boolean Logic: Provide software that supports easy access reporting using Boolean Logic for the creation, storage and retrieval of user-defined reports comprising information extracted from the system database. All database information including, but not limited to, event, activity, audit trail, cardholder and configuration information shall be accessible for database searches, on-screen viewing, and inclusion onto printed reports. Database links shall be user-definable.

Database Operator Audit Log: The Velocity EACIDS shall be capable of creating a detailed audit log in the history file following any change made to the Velocity EACIDS database by an operator. The audit log shall record specific changes or manual operations made by an operator.

Hardware XML Configuration: The Velocity EACIDS shall support the ability to define hardware to simplify the process of creating an access control system including time zones, door set-ups, and alarm action triggers.

Analog CCTV Interface

System Software shall allow the ability to define, view, monitor, and control the CCTV Matrix Control System. Simulated Alarms can be sent to the switcher, as well as Tours, Presets, Camera Selection, obtain and store a CCTV image, and pan/tilt/zoom/iris controls for the selected

camera. In addition, one or more Triggers and Actions can be defined for each camera.

Analog CCTV Interface shall accommodate American Dynamics, Pelco, and Vicon

Digital Video Interface (DVR/NVR)

The DVR/NVR interface configuration enables a qualified Operator to add a supported DVR or NVR to the Velocity EACIDS software. The following DVR/NVR interfaces shall be supported.

DVR/NVR Integration	SDK Supported
American Dynamics - INTELLEX 3.2	INTELLEX 4.3
American Dynamics - INTELLEX 4.3	INTELLEX 4.3
MATE Behavior Watch - INTELLEX 4.0(+) Support	INTELLEX 4.0(+)
American Dynamics - VideoEdge 3.0	VideoEdge 4.5
American Dynamics – Hybrid	Unified 1.0
PELCO DX8100	X-Portal 3.2 or 3.3
BOSCH	
Aventura 4.5	
ExacqVision 8.2	
GENETEC Security Center 4.5	
Milestone XProtect 2014	
OnSSI – NetDVMS	
OnSSI - Ocularis 5.2	
Verint Nextiva 6.2	
VICON	

Properties defined when adding a DVR include

DVR Name

DVR Description

DVR Vendor

DVR I.P. Address

I.P. Port (Control)

I.P. Port (Live Video)

DVR Server Name

Port (Listen)

Time Zone

DVR Enabled

From the DVR Interface Configuration, the Operator shall be able to Search and Retrieve video from one or more cameras for a specified period of time. In addition, the Event Viewer History enables a qualified Operator to track and report events that are specific to the DVR subsystem history logs. These logs include:

Active Alarms by Date

Active Alarms by Date with Comments

Alarm Log by Date

Alarm Log by Date with Comments

All Events Log by Category

All Events Log by Date

The DVR interface shall allow a qualified Operator to

View Cameras

Generate a Host Alarm

Stop a Host Alarm

Get Alarm List from DVR

Search and Retrieve Recorded Video

Play Local Video

Time Synchronization

Diagnostics

View DVR Properties

When Viewing cameras, the Operator may select Small, Medium, or Large display size, and select for viewing 1, 4, 9, or 16 cameras to display in the View Window. Cameras may be selected, then dragged to the window the Operator wishes to view the camera in. If the camera has Pan/Tilt/Zoom/Focus/Iris control, the Operator can open the control functions and operate the on-screen controls for the selected camera.

An Operator shall be able to define Triggers and Actions that allows Alarms and Events in Velocity to cause Alarm recording in the DVR through an API interface. A camera preset can be defined, as well as a View Group to automatically display on alarm.

In Graphics, DVR Cameras and DVR recorder icons can be placed on floor plans and used to view the associated video from the selected camera.

Video can be exported from a DVR and stored on the Velocity PC, then transferred to other media such as CD-R, CD-RW, or DVD-R.

There shall be a Video Explorer application that lets a qualified Operator view multiple cameras from multiple DVRs in a single window. Cameras can be displayed in 1, 4, 9, or 16 display views, and these views can be saved as View Groups for fast and easy selection by the Operator.

Alarms can be sent from the DVR to the Velocity EACIDS software. Alarms include: Motion and Video Loss. When used with MATE Behavior Watch advanced analytics, these alarms can be displayed in the Velocity EACIDS viewer.

Software Developers Kit (SDK): The Velocity EACIDS Manufacture shall provide a published Software Development Kit (SDK) that includes a programming interface (API) and deployable Web Services for executing device commands (opening and locking doors, triggering relays and control zones, etc.). The SDK shall include sample code and documentation to enable development of secure interfaces for two-way data transmission with the Velocity EACIDS.

The Vendor shall have available a Professional Services Group to assist and/or provide solutions using the SDK.

The SDK shall enable third-party applications to perform the following from outside the Velocity EACIDS:

Add, modify and delete people and credentials from the Velocity EACIDS

Create, update, delete door groups and master door groups

Receive alarms, events and transactions from the Velocity EACIDS

Execute commands (e.g., lockdown, mask, change, add from the Velocity EACIDS).

Generate Velocity EACIDS events and alarms from any event based on 3rd party system including: (BACnet, Video Management Systems, Logical and Network Access Systems, etc.)

Velocity EACIDS Software Functionality

General: This information is provided to explain the Velocity EACIDS functional capabilities. Some, but not all, of these functions will be utilized to accomplish the functionality required for this project

The Velocity EACIDS Software shall inherently support an unlimited number of card readers, input points, intrusion detection points, and relay outputs. The Velocity EACIDS database server shall support an unlimited number of cardholders, visitors, and assets limited only by the available memory on the Controller. The database server shall also support an unlimited number of system events and System Operator transactions in the history file limited only by available hard disk space. Client Workstations shall be limited only by the limitations of the operating system server software.

Time Zones

Time Zones define periods during which readers, cards, codes, alarm inputs, doors, or other system features are active or inactive. Basic configuration parameters shall “ask” the Operator to define “when” the user is enabling (or disabling) a specific feature. In addition to Monday-Sunday, there shall be one day of the week called Holiday.

When selected, there will be 4 Holiday Schedules that determine if the Holiday is to be followed for this Time Zone. There shall be 64 Standard Time Zones, 64 Master Time Zones, and 20 Grand Master Time Zones

Each time zone shall be assignable to an alphanumeric name of up to 50 characters. Time zones shall be applied to access levels, card reader modes, alarm inputs, alarm outputs, and alarm masking and logging functions. Time zones shall be allowed to belong to any or all access levels so that the time zone only has to be defined once.

Holidays

The Velocity EACIDS software shall support Holidays to make an exception to a time zone on a specific date. Each time zone has up to 4 holiday schedules. There are 366 user definable holidays per year. It shall be possible for the operator to “make the rest of today a holiday”. Holidays shall be selected from a calendar, including the ability to select multiple days.

Access Levels

The Velocity EACIDS shall be capable of defining access levels with unlimited number of credentials per cardholder. Access Levels shall consist of a combination of card readers and time zones.

Each Access Level shall be assignable to an alphanumeric name using up to 50 characters.

Card readers shall have the ability to be assigned to any or all access levels defined in the Velocity EACIDS. Individual card readers shall be capable of having a distinct time zone assigned to it.

The Velocity EACIDS shall allow an ‘Allow User Commands’ option to be assigned on a per access level basis where keypad readers are in use.

Temporary Access Levels

The Velocity EACIDS shall support Guest Credentials. Using the Enrollment feature a Guest credential may be configured the same as any other credential without being assigned to a specific person. Credential Templates may be pre-configured with an access allotment to allow issuing credentials before they are used. The Guest credential may be a PIN or card and can be set to expire, disable, or re-assigned.

Function Groups

Credentials can be assigned to perform a single User Function, such as Momentary Access, or multiple functions such as Momentary Access in one controller and Control Trigger Function in a relay controller for Elevator Access. When multiple User Functions are required by a Person, a Function Group may be defined and associated with one or more credentials. The Function Group requires a ScramblePad keypad to be used, where the Person’s base Credential PIN number is entered, followed by an * (Asterisk), followed by a one or two digit

Extension digit, which defines which User Function will be issued for which Control. This allows for a single person to perform multiple User Functions such as: Unlock Door, Relock Door, Change Threat Level, Mask Alarm Inputs, Lock Down Doors.

Credential Templates: Credential Templates allow the System Administrator to establish all parameters for a credential except the unique card or code. Pre-defined credentials that include the following parameters:

Linking – allows for linked credentials to auto update when changes are made to the template.

Badge Template Assignment – pre-determines which Badge Template will be printed when the Credential is assigned using the template.

The system shall be capable of issuing users various types of credentials. Credentials can be utilized a variety of ways dependent on requirements at specific areas. These would include: Badge Only, Keypad, Card, Dual, Card+Dual, Keypad+Dual, Keypad+Card

Card Type – defines bit format

Activation/Expiration Date

Code Length - pre-established code length from 3 to 15 digits

Duress Digit – may be selected for each credential using the template

Access or Control Credential Assigned

Door Group

Control Function

Limits

Threat Authority

Day/Use Limits

2-Person Rule

Apply Globally

Options

Executive Override Passback

Special Needs Additional Timers

Print Control

Biometrics

Smartcard Reader

Panel ID and Site ID

Expiration Date

Command Sets

A Command Set defines an action or actions to be sent to one or more controllers. Command Sets can include: Unlock and Relock a Door; Lock Down and Release a Lock Down on one or more doors; make the rest of today a Holiday; Mask all Interior Alarm Points; change the facility Threat Level; Forgive All Passback. After being defined, a Command Set can be executed from the Command Set window, or from a Graphic Floor Plan icon, if defined. There shall be an unlimited number of Command Sets available to be defined. Command sets shall be defined with pick lists, and shall be capable of being restricted by Operator Group and Workstation.

First Person Unlock: The Velocity EACIDS shall provide a First Card Unlock feature than when configured retards a pre-determined time zone activated unlock command until a valid credential has been presented and granted access to the portal.

The following functions shall not require a host computer and shall function for all devices configured in a RS-485 topology.

Two-Man Rule: Two access credentials required to enter an area. A user can be defined as Normal, A/B Rule A, A/B Rule B, or Executive Override. Function can be enabled/disabled by Time Zone.

Door Interlocking (Mantrap): Requires authorized user to pass through a portal and for the portal to close and be in secure mode before the user can pass through the next portal. Function shall be implemented without third party hardware or software.

Anti-passback Control: An authorized access credential shall not be able to re-enter an area until it has exited the area by presenting the credential to an exit reader.

Timed Anti-passback: An authorized credential shall not be able to re-enter an area for a programmable time period.

Verified Anti-passback: A person shall not be considered as having moved to the next location following any incomplete transaction (such as access being granted at a reader but the associated door not being opened and closed within a normal amount of time)

Occupancy Counting: The system shall be able to identify the number of credentials that have entered an area. The system shall be able to set minimum and maximum limits for any area and shall be capable of triggering one or more event based on the minimum and maximum levels for the area. The system shall be capable of displaying the count in any secured area without the need to run a report.

Virtual Relays: The system shall support the ability to program alarm and event triggers for multiple points without requiring a physical relay. This function shall be capable of triggering control functions (inputs/outputs) through Time Zones allowing IF/THEN statements.

Threat Levels: Threat levels shall allow an operator to change the function of the system based on the Threat Level chosen. Each system device

can be programmed to operate in a different mode based on the current Threat Level for the system.

No additional software license shall be required to enable the threat level feature.

The system shall support a minimum of 99 threat levels.

Use Count Limit: Limits the number of times a credential can be used before it is disabled. The system shall be able to set the limit from 1 to 255.

Temporary-Day Limit: Shall specify the number of number of days a credential shall function before it is disabled.

Absentee Rule: Shall disable a credential after a specified number of absences.

After Hours Rule: Sets the time and date after which a credential will no longer be valid. Use of the credential after the expiration time and date shall prevent the credential from allowing access at a portal and shall notify the operator.

Duress Code at Keypad (ScramblePad only): Allows a user to enter a specific PIN when being forced to open a portal. The portal shall still open and a duress alarm shall be sent to the operator.

Function Commands: This function allows a user to enter a command at a keypad to activate a pre-programmed set of functions. A function command can include inputs and outputs in the event. An example would be to lock all doors in an area or arm all alarm points in a zone. The system shall support up to 99 Function Commands per credential.

Tag User: Sends an alert to the Alarm Viewer each time the credential/PIN is used at a reader/keypad location regardless of access authorized or denied. This alarm can also be issued when the card/code triggers a tagged control zone. A lost or stolen credential may also be tagged, so an alarm would occur if it was used.

Extended Individual Strike Times: The Velocity EACIDS shall support Extended Individual Strike Times that allows a card reader's strike to be active for an extended period of time beyond the pre-determined standard strike time on a per cardholder basis. The extended strike time shall be user definable up to 8100 seconds. Extended strike times shall be set on a card reader by card reader basis.

Extended Individual Door Held Open Times: The Velocity EACIDS shall support Extended Individual Door Held Open Times that allows a card reader's door to be held open for an extended period of time beyond the pre-determined standard held open time on a per cardholder basis. The extended held open time shall be user definable up to 1440 minutes. Extended held open times shall be set on a card reader by card reader basis.

Only those cardholders having Command Authority at a given card reader configured for 'Allow User Commands' shall have the ability to execute the Extended Held Open command at that card reader. The Extended Held Open command shall be available

after a valid cardholder has received an Access Grant at the card reader. The cardholder shall have a period of fifteen seconds after the Access Grant to enter the extended held open command sequence.

Field Hardware Communications

The Velocity EACIDS shall support communication with the Controllers by the following protocols:

RS-232

RS-485

TCP/IP

Communication baud rate shall be system selectable with a range between 1,200 to 115,200 bits per second.

Download communication between the Velocity EACIDS and the Controller shall be fully multi-tasking and shall not interfere with operational functions.

Upon loss of communications between the Velocity EACIDS Server and the Controller an alarm shall be created with a time stamp. Upon re-established communication the Velocity EACIDS and the Controller shall automatically re-synchronize from the point of communication loss without operator intervention.

Firmware Upgrades: Controller firmware shall be upgradeable via download from the server.

Multi-Drop Panel Support

The Velocity EACIDS shall support a multi-drop Controller architecture whereby up to 16 Controllers shall be multi-dropped over RS485 from a single IP Port and whereby all 16 panels communicate back to that or IP port.

The multi-drop panel support shall be used in conjunction with other Controller wiring support such as the star wiring configuration, home-run wire architecture, and advanced distributed network architecture.

Global Boolean Event Linkage

The Velocity EACIDS shall support a global linkage feature whereby any input/output/event shall be linked to any other input/output/event in the Velocity EACIDS. Input / Output Linkages shall be able to span across Controllers multidropped off the same IP port.

System Administrators shall be able to create global I/O function lists, each consisting of a sequence of actions to be performed, such as changing card reader modes, activating outputs, and opening or closing anti-passback areas. Each function list may include up to six actions.

Elevator Control: The Velocity EACIDS application software should be capable of supporting this feature as an integral part of the Velocity EACIDS application

environment for future use, but Elevator Control software is not a requirement this phase of work.

The Velocity EACIDS shall provide elevator control using standard access control field hardware that will permit the restriction of cardholder access to certain floors while also allowing general access to other floors. The elevator control feature shall allow, at the elevator, the use of any card reader and all card reader modes used on any other card reader in the Velocity EACIDS. Each elevator card reader shall control access for all floors of the building.

The Velocity EACIDS shall be able to track which floor was selected by an individual cardholder for auditing and reporting purposes.

Alarms

Pre-Alarm: The Velocity EACIDS shall support a pre-alarm feature at the ScrambleSmart card reader. The pre-alarm will sound a tone at the card reader prior to the door held open alarm.

Alarm/Event Logging

Alarms and events in the Velocity EACIDS shall by default always be recorded in the database. The Velocity EACIDS shall give System Administrators the ability to select on a time zone basis, the times that they require the Velocity EACIDS to log specific events to the database.

System Administrators shall have the option for Alarm/Events to be set to log or not to log particular alarms/events on any individual reader and or input.

Alarm/Event Routing

The Velocity EACIDS shall be capable of allowing System Administrators to route alarms and events to various Alarm Monitoring client workstations on the network. The Velocity EACIDS shall allow any alarm or event to be routed to one or multiple client workstations on the network regardless of where the alarm is generated in the field. Alarms shall be routed to client workstations on a device by device level.

The Velocity EACIDS shall implement network synchronization that in the event alarm/event is routed to multiple client workstations, once the first client workstation ‘grabs’ the alarm, the alarm/event shall be cleared from all other client workstations. As such, alarms that are routed to an Alarm Monitoring client workstation which does not have a System Operator logged in shall be queued so that all unacknowledged alarms will report to that client workstation once a System Operator has logged into the Velocity EACIDS. Alarms/Events shall be routed based on default settings or time zone control.

The Velocity EACIDS shall provide alarm escalations to system administrators by priority level.

Text Instructions: The Velocity EACIDS shall allow for a set of text instructions to be associated with each alarm that arrives into the Velocity EACIDS. Each alarm or event in the Velocity EACIDS shall have its own unique set of text instructions should the System Administrator desire.

Customizable Voice Instructions: The Velocity EACIDS shall allow for a customizable voice instruction to be associated with Velocity EACIDS alarms. The customizable voice instruction feature shall allow the System Administrator to record a voice instruction of unlimited length.

Customizable Voice Annunciation: The Velocity EACIDS shall allow for a customizable voice annunciation to be associated Velocity EACIDS alarms. The customizable voice annunciation shall allow the System Administrator to record a voice annunciation of unlimited length.

Alarm Function Configuration

The System Administrator shall have the ability to configure how the Velocity EACIDS handles the annunciation of alarms on an individual basis. Each alarm and/or event shall have the option(s) to:

Display at one or more Alarm Monitoring client workstation.

Allow higher priority alarms to be displayed on the Alarm Monitoring client workstation ahead of lower priority alarms.

Require the field device, which generated the alarm to be restored to its normal state before the alarm is cleared.

Print the alarm to the local event printer.

Have a customized voice message annunciate at the client workstation.

Have the alarm breakthrough to the Alarm Monitoring window should the System Operator be working in another application

Ensure that the alarm will not be able to be deleted from the Alarm Monitoring window upon acknowledgment.

Display text and audio instructions outlining the procedures to follow when responding to the alarm.

Automatically call-up associated maps.

Automatically call up the associated cardholder record.

Automatically call up the associated cardholder photo using the video verification function.

Require acknowledgment to clear.

Allow mandatory operator note upon acknowledgment.

Use pre-defined operator note entries for alarms.

Select the option for operator instructions based upon the specific alarm.

Send DVR/NVR interface commands to the DVR/NVR

Automatically send an e-mail message.

Automatically send an alphanumeric page.

Have the alarm appear on the Alarm Monitoring window with a flashing colored icon across the alarm for high priority alarms.

Have the alarm, when acknowledged, display an alternative flashing color coded icon in the alarm window column

Require User Logon for Acknowledgment

Require Local Acknowledgement from a related Reader/Keypad.

Alarm-Event Mappings: The Velocity EACIDS attributes in Customization Manager shall be assignable on a 'global' basis to all devices that share an alarm description. Thus, the 'door forced open' alarm attributes shall apply to any door with a card reader that is forced opened. The Velocity EACIDS shall have the capability to assign a unique group of alarm attributes to specific device/alarm combinations to override the global settings for specific case settings. For example, System Administrators may assign a different set of attributes to be applied to a 'door forced open' at a vehicle gate or door onto the AOA than they would if the front door to a building was forced open. The Velocity EACIDS must include this type of flexibility. Each device/alarm combination shall have the ability to have its own unique attribute set if the System Administrator desires.

Alarm Masking: The Velocity EACIDS shall support the masking of alarms to be controlled on a time zone basis or by manual control.

Alarm Masking shall be able to be implemented in groups or as individual points (a "group" of one).

The Velocity EACIDS shall support a group alarm masking feature where System Administrators shall be able to create groups of alarm inputs that enable them to mask or unmask multiple Input Control Module inputs and card reader inputs simultaneously.

The following events shall have the ability to be part of an alarm masking group:

Alarm Input Active

Card Reader Events

Auxiliary Input Active

Door Contact Tamper

Door Forced Open

Door Held Open

Card Reader Input Tamper

When a point is “masked” the system shall continue to track the status of the point for display on the active GUI, and monitor the supervisory status of the point and its wiring.

The Velocity EACIDS shall support an Alarm Masking Group status change (Masked to Unmasked or Unmasked to Masked) action to be linked to a function list that is capable of performing many system actions, such as activating a relay output.

Input/Output Point Options: The Velocity EACIDS shall provide the following options for the Input Points:

Alarm Masking – The ability to mask the alarm input on a time zone basis.

Local Linkage – The ability to locally link outputs with inputs that are attached to the same Controller segment

Activate Output - The ability to activate an output on a time zone basis.

Activate Output Always- The ability to activate an output always.

Guard Tour Log – The ability to configure an input as a designated stop on one or more guard tours.

Entry/Exit Delay – The ability to set up entry/exit delays for inputs. This shall include

Non-Latched Entry: When an input activates, the alarm will not be reported until the Entry delay expires. If the input is still active when the entry delay expires, the alarm will be reported. If the input is not active when the entry delay expires, then the alarm will not report.

Latched Entry: When an input activates, the alarm will not be reported until the Entry delay expires. If the input is still active when the entry delay expires AND the alarm has NOT BEEN MASKED, the alarm will be reported. If the input has been masked when the entry delay expires, then the alarm will not report

Exit Delay: When an input activates, the alarm will not be reported (operates as if masked) until the Exit delay expires. If the input is still active when the exit delay expires, the alarm will be reported. If the input is not active when the exit delay expires, the alarm will not be reported.

Current Status Indication: The Alarm Monitoring window shall provide a status indicator that displays the current status of alarms, card readers, and Controllers.

Pre-Defined “Canned” Alarm Acknowledgment Responses: The Velocity EACIDS shall have the capability for pre-defined alarm acknowledgment responses for alarms in the Velocity EACIDS. An

unlimited number of pre-defined responses shall be able to be configured for each alarm in the Velocity EACIDS.

Alarm Monitoring – Column Display & Configuration: The Velocity EACIDS shall allow System Administrators and System Operators to define which columns are displayed in the Main Alarm Monitoring Window and in which order. System Administrators and System Operators shall also be able to determine the column order.

On-Line Context Sensitive Help: The Velocity EACIDS shall provide on-line context sensitive help. The help menus shall be available from any window in the Velocity EACIDS by pressing the F1 function key or clicking on the help icon in the toolbar.

Sorting Capabilities: The Velocity EACIDS shall allow System Operators to arrange the way that alarms and/or events in the Alarm Monitoring window are listed by sorting the alarms and events. Sort criteria shall be based on priority, time/date, Controller, Card Reader, Input Device, or Cardholder. Additionally alarms and events can be sorted based on asset scan ID, asset name, intercom station, intrusion panel, transmitter, or transmitter input.

Device Control through Command Sets: The Velocity EACIDS shall support Operator Roles for device grouping for uniform command and control of groups of devices within the system. There shall be no limit on the Groupings. Any point connected to the Velocity EACIDS shall be capable of being grouped together for Operator Control including:

Card Reader Groups

Input Groups

Relay Output Groups

Video Camera Groups

Control Panels

Trigger Groups (groups of inputs and outputs) with associated functions

Threat Levels up to 99

Scheduling Agent Utility

The Velocity EACIDS shall provide an integral Scheduling Utility. The Scheduling Utility shall allow System Administrators to schedule actions to occur on a one-time or a recurring basis. Recurring schedules shall be configured to begin immediately, last indefinitely, or have optional start and end dates.

The Scheduling Utility shall be available from both the System Administration and Alarm Monitoring modules.

The types of actions that shall be schedulable include but are not limited to:

Action Group

Event Archiving / Purging

Arm / Disarm Area

Start of Guard Tour

Execution of Data Exchange Scripts

Activate, Deactivate, Pulse Device Output and Device Output Groups

Global Anti-Passback Reset

Download Firmware to Controllers and IP Cameras

Download Database to Controllers

Execute Function List

Mask / Unmask Inputs, Input Groups, Alarm Mask Groups, Door Forced Open or Held Open

Open Door, Open Door Group

Change Reader Mode

Automatic Reports

Reset Use Limit

The Scheduling Utility shall maintain a history log in the database for actions that it executes.

Access Control

Multiple Card Formats: The Velocity EACIDS shall support an unlimited number of card formats. Magnetic stripe, RFID, contactless smart card, and contact smart card formats shall be supported. Each Controller shall support multiple card formats and combinations of card formats from various bit length structures simultaneously. In addition, the Velocity EACIDS shall support the following:

Any industry standard Wiegand card format.

Any industry standard 125Khz and 13.56 MHz card technology.

Amy biometric device that provides wiegand output data

ID Formats: The Velocity EACIDS shall support multiple ID formats for a variety of credentials enrolled in the system: These would include Badge Only, Keypad, Card, Dual, Card+Dual, Keypad+Dual, Keypad+Card..

Denied Access Attempts Counter: The Velocity EACIDS shall support a denied access attempts count per controller. The “Denied Attempts Count” value shall be configurable from 1 to 99 seconds. The following access denial types shall cause the current reader to be disables for 1 to 60 minutes:

Unknown PIN entry at a card reader configured as ‘PIN or Card’ mode

Invalid PIN entered for a given card at a card reader configured as ‘Card and PIN’ mode

Non-matching biometric presented for a given card at a card reader in biometric verify mode.

Each card reader shall have the ability to have multiple time zone setting overrides assigned to them as required by the System Administrator.

Card Reader Options:

The Velocity EACIDS shall include the following options for each reader on the system:

Allow User Commands

Rename Auxiliary Inputs

Rename Auxiliary Outputs

Independently Supervise RQE (request-to-exit) and DPS

Configure RQE and DPS as Normally Open or Normally Closed

Deny if Duress

Alarm Masking

Activate Outputs

Two Person Rule

Do Not Activate Strike on RQE

ScrambleSmart Reader shall include standard Card Reader options plus the following options:

LED Control

Silent Operation

Code Tamper Disable User

Scramble Normal

Viewing Restriction

Physical Tamper Switch

Moisture, Dust, Dirt and ESD Resistant

125kHz proximity and 13.56MHz (ISO14443A&B/ISO15693) contactless

MATCH2 functionality

UL Listed

On Board MATCH options shall include standard reader options plus the following:

Weigand pass through

Allow for Greater Distance (Up to 1,800 feet using

18 gauge wires)

Configurable Multiple Outputs and Custom Formats

Entry and Exit Readers on a Single Reader Controller Port

Tamper

Addressable

The Velocity EACIDS shall allow for user definable door strike functionality for each card reader in the Velocity EACIDS.

The Velocity EACIDS shall allow for each card reader to be selected as either an 'in' reader, 'out' reader, or 'none' to allow for ease of reporting time and attendance basic 'time in' and 'time out' data.

Enforce Use Limit – This option shall enable Card Use Limits at the card reader limiting the number of times that cardholders may use their credential to gain access at the card reader

Supervise Door – Sets the Velocity EACIDS so that the card reader door contact is wired as a supervised input.

Automatic Credential Deactivation based upon an Event: The Velocity EACIDS shall have a programmable ability to deactivate an active badge based upon a pre-determined event. Any User Definable Field may be configured with an Expiration Date to effect deactivation based on specific criteria.

On-Line Context Sensitive Help: The Velocity EACIDS shall provide on-line context sensitive help files to guide System Administrators and System Operators in the configuration and operation of the Velocity EACIDS. The help menu shall be available from any window in the Velocity EACIDS by pressing the F1 function key or clicking on the Help icon in the toolbar. Help windows shall be context sensitive so System Administrators can move from form to form without leaving the help window. The Velocity EACIDS shall also come with complete on-line documentation with the Velocity EACIDS software.

System Downloads

The Velocity EACIDS shall provide for the downloading of data to the Controllers. Downloads shall load Velocity EACIDS information (time zones, access levels, alarm configurations, etc.) into the Controllers first, followed by cardholder information and card reader configurations.

All Controllers on the Velocity EACIDS shall be downloaded simultaneously (in parallel with one another) and bi-directionally so that alarms will still report to their respective Alarm Monitoring client workstations as cardholder information is being downloaded.

Information on cardholder status, badge status, time zones or access levels shall download in real time as they are added, modified, or deleted from the Velocity EACIDS.

Auto Exit to Windows: The Velocity EACIDS shall be configurable to automatically exit the Alarm Monitoring application and log the System Operator out of the Windows when a System Operator logs off an Alarm Monitoring client workstation. The Velocity EACIDS shall then bring the System Operator to the Windows Login Window for the next System Operator to log on.

Manual Control: The Velocity EACIDS shall provide the System Operator the option to manually control all output points or input points connected to the Velocity EACIDS. Control points are defined as any door strike, auxiliary card reader output, or any other relay output point of a Controller.

Third Party Interface: The Velocity EACIDS shall be capable of passing alarm information to any third party system using a published SDK. When the Velocity EACIDS receives an alarm from any monitoring point on the Velocity EACIDS, a minimum of three (3) control commands relating to that alarm point may be sent to a third party system per alarm input or card access alarm. The 3 commands are sent based upon the following conditions:

Upon arrival of the alarm at the Velocity EACIDS

Upon “selecting” or reviewing of the alarm

Upon alarm acknowledgment or clearing the alarm

Real-Time, Dynamic Graphical Maps

The Velocity EACIDS shall support graphical maps that display device / group status, function lists and video cameras dynamically in real-time. The maps may be configured to appear on command or when specified alarms are selected for acknowledgment. Map device icons shall have the ability to dynamically change shape and / or color to reflect the current state of the device.

The Velocity EACIDS shall support all map formats listed below:

AutoCAD DXF (.dxf)

BMP (.bmp)

JPEG (.jpg)

TIFF (.tif)

Windows Metafile (.wmf, .emf)

VBD (.vbd)

The Velocity EACIDS shall support map hierarchies or maps within maps. There shall be no limit to the number of maps that shall be nested hierarchically with each other. Multiple maps may be displayed simultaneously.

The Velocity EACIDS shall support user defined icons for field hardware devices. The Velocity EACIDS shall also give System Operators the ability to affect the mode of card readers, open doors, mask/unmask alarm inputs, and activate/deactivate/pulse an output from the map icons.

The graphical maps shall have the ability to be printed to a local printer.

Credentialing

Credential Management

The Velocity EACIDS shall include as a standard a Credential Management and Enrollment module that is integral to the Velocity EACIDS source code with the ability to create and maintain the Cardholder database. Features shall include the ability to:

Add, Modify and Delete records based upon permissions.

Capture photo images and signatures.

Print Credentials.

Boolean Search on any single or multiple fields.

Customization of screen layout and field names.

Advanced customization of fields, field names and screen tabs (pages) with optional Forms Designing and Editing Module.

Determine single or multiple active badges.

Assign Access Levels and Access Groups.

Bulk Assignment/Modification/Deletion of Access Levels.

Bulk Deletion of Cardholder Records.

Native support for U.S. Government Standards (FIPS-201)

Credentials: The Velocity EACIDS shall support the following credential types and allow for direct Thermal Dye Sublimation printing onto the credential surface.

Composite Credentials - 3.375” x 2.125”, UPVC Composite credentials with an ISO standard 30 mil thickness

Proximity credentials

Smart Cards – Contact and Contact-less

Credential Management Enrollment Features:

The Velocity EACIDS shall allow for automation of enrollment procedures with the following attributes based upon badge type:

Default Deactivation Date

Default Access Levels

Badge Design Layout

Badge Printer Selection

Encoding Format (if required)

Badge ID if set to automatic generation

Cardholder Image Capture

The Velocity EACIDS must be compatible with flash lighting, RGB video cameras, composite input cameras, S-Video input sources, USB sources and digital cameras and allow the capturing of the cardholder image at a minimum resolution of 1024 x 968.

Velocity EACIDS image capture, storage, and hardware compression techniques must be in compliance with the ANSI standard or JPEG (Joint Photographic Experts Group). Cardholder images must be stored as Binary Large Objects (BLOB) within the cardholder record.

The Velocity EACIDS shall provide the ability to capture a cardholder's image through the use of any industry standard scanner or digital camera that utilizes a TWAIN interface. Images shall be able to be scanned in at up to 16.7 million colors for a true color scanned image.

Image Import: The Velocity EACIDS shall allow for System Operators to have the ability to import a cardholder's image at the time of enrollment. The Velocity EACIDS must support the following image formats:

Bitmaps (.bmp, .dib)

JPEG (.jpg)

Portable Network Graphics (.png)

TIFF (.tif)

Windows Metafile (.wmf, .emf)

Biometric Verification: The Velocity EACIDS application software should be capable of integrating with biometric readers.

Network Account Allocation via Active Directory

The Velocity EACIDS shall be able to link a Velocity EACIDS cardholder account to the cardholder's Active Directory network account.

The Velocity EACIDS shall enforce the allowable number of Network accounts per Cardholder

The Velocity EACIDS shall be able to link/unlink an existing Windows Active Directory Account to a cardholder account.

Badge Design: The Velocity EACIDS shall incorporate a Badge Design module that is integral to the Velocity EACIDS source code with the ability to create and maintain badge designs. Features shall include the ability to support:

Complete Badge design and Layout tools

Image Import

Ghosting

Signature Capture

Barcode

Smart chip Support

ID Printers: The Velocity EACIDS shall support any printer with industry standard and Microsoft Certified Windows 7 drivers. The Velocity EACIDS shall support

Double-sided full color printing

Edge to edge printing

High-speed printing

Holographic overlays

In-line Magnetic Stripe Encoding

Image Export: The Velocity EACIDS shall have the ability to export a captured and cropped cardholder image to an industry standard JPEG (.jpg) file format.

Special Functions Requiring Manufacturer Professional Services Group Support

Anti-passback features shall be supported natively within the Velocity EACIDS. When configured in an RS485 fashion, all hardware shall support Global IO capability natively without the use of a Host server.

Global IO amongst IP networked controllers shall be supported through Professional Services.

Area Control (Global Functions): The Velocity EACIDS shall provide five (5) area control features: Global Hard Anti-passback, Global Soft Anti-passback, Timed Anti-passback, Two Person Control, and Occupancy Limit. Area control shall be a security method of preventing a person from passing their badge to another person for dual entry into a single location utilizing one credential.

Global Hard Anti-passback: The Global Hard Anti-passback feature shall require that a badge always be used to enter and exit an area. The controlled areas shall have both entry and exit card readers at all portals. Entry and Exit Readers shall be able to span across multiple Controllers. Areas shall be logically defined under the Velocity EACIDS, and area control shall not be required at all areas of the facility to be utilized. Global Hard Anti-passback shall work in the following manner. A cardholder must present his/her badge at the entry card reader of the area that the person wishes to enter. Once access has been granted into the area, the cardholder cannot present the badge to another entry card reader within the same area without first presenting his/her badge to the respective exit card reader of that area. Should a cardholder attempt to use any other card reader in the same area besides the occupied area's exit card reader once access has been granted to that area, the cardholder shall be denied access and an alarm shall be reported to the Alarm Monitoring client workstation. It shall be possible to have an area within an area and/or

multiple areas that are independent of each other in which Global Hard Anti-passback rules shall apply.

Global Soft Anti-passback: The Global Soft Anti-passback feature shall require that a badge be used to enter and exit an area. The controlled areas shall have both entry and exit card readers at all portals. Entry and Exit Readers shall be able to span across multiple Controllers. Areas shall be logically defined under the Velocity EACIDS, and area control shall not be required at all areas of the facility to be utilized. Global Soft Anti-passback shall work in the following manner. A cardholder must present his/her badge at the entry card reader of the area that the person wishes to enter. Once access has been granted into the area, the cardholder cannot present the badge to another entry card reader within the same area without first presenting his/her badge to the respective exit card reader of that area. Should a cardholder attempt to use any other card reader in the same area besides the occupied area's exit card reader once access has been granted to that area, the cardholder shall be allowed access (if that cardholder has the appropriate access level to access the new area), and an alarm shall be reported to the Alarm Monitoring client workstation. It shall be possible to have an area within an area and/or multiple areas that are independent of each other.

The following summary criteria shall apply under Global Hard or Soft Anti-passback:

Re-set of Passback Violations or Credential Forgiveness shall be capable so that all cardholders are re-set to Zone 0.

Any cardholder shall enter a controlled area any time after Credential Forgiveness by presenting a badge to an Velocity EACIDS entry card reader.

A cardholder shall not exit the controlled area unless he has entered the area presenting a badge to the Velocity EACIDS entry card reader

A cardholder shall not enter the controlled area a second time unless the cardholder has exited that area previously.

A cardholder shall be able to enter through any entry card reader and exit through any exit card reader of a single controlled area.

These options shall include a "forgiveness" feature that will allow the System Administrator to reset the anti-passback of all cardholders to Time 0 Area 0, either through a manual override or a time zone command.

The Velocity EACIDS shall provide an anti-passback exempt option for privileged or VIP cardholders. Cardholders with this option will not have anti-passback rules applied to them.

The Velocity EACIDS shall also have a "forgiveness" feature that will allow the System Administrator to assign "one free pass" to an individual cardholder. This shall allow the System Administrator

to reset the anti-passback of an individual cardholder to Time 0 Area 0.

Timed Anti-passback: Timed Anti-Passback shall allow the System Administrator to decide how long after a cardholder has swiped their badge that they will have to wait before the same badge will be accepted again at the same card reader. This helps prevent multiple swipes by an individual to allow access to others through turnstile doors.

Verified Anti-passback: A token shall not be considered as having moved to the next location following any incomplete transaction (such as access being granted at a reader but the associated door not being opened and closed within a normal amount of time)

Who's Inside Graphical Display

The Velocity EACIDS software shall natively include a real-time Who's Inside display. When an emergency occurs in an area or building, the user may know immediately who is inside a designated area and manage the swift movement of those people to a safe area. Individual access can be tracked using the Who's Inside option. Users are grouped into zones and may be manipulated into other zones. Who's Inside will also be able to produce an HTML report from the Who's Inside window without going inside the Report Manager.

Two Person Rule

Two-Person Rule shall be provided to restrict access to certain areas unless there are two (2) cardholders present. This restricts individuals from being alone in restricted or highly secure areas. When an area is configured for Two Person Rule, the following criteria shall prevail:

Two-person Rule shall support the ability to define A/B Rule allowing the administrator to specify that it must be a specific combination of credentials. For example: Credential A+A equals no access. Credential A+B equals access. (Supervisor and Employee)

The card reader shall grant access only if two valid cardholders (with authorized access levels) swipe their badges one after the other. In the event that a second authorized card is not presented within 10 seconds of the first authorized badge, the card reader shall reset and the first card will have to be swiped again.

Once 2 people occupy an area, individual access shall be granted.

Individual exit shall be permitted until an area is occupied by only 2 cardholders at which point the Two Person Rule applies for exit.

Controllers

The Controller (Controller) shall link the Velocity EACIDS Software to all "down-stream" field hardware components. The Controller shall provide full distributed processing of access control / Alarm Monitoring rules and

operations. A fully loaded and configured Controller with shall respond in less than one-half (0.5) second to grant or deny access to cardholder.

The Controller shall continue to function normally (stand-alone) in the event that it loses communication with the Velocity EACIDS server. While in this off-line state, the Controller shall make access granted/denied decisions and maintain a log of the events that have occurred. Events shall be stored in local memory, and then uploaded automatically to the Velocity EACIDS database after communication has been restored.

In addition, the Controller shall incorporate the following features:

UL 294, ULC, and CE Certified

Support for Host Communications Speed of 115,200 bps

Support for Direct Connect, Remote Dial Up, or Local Area Network (LAN) Connection

Support for up to 128 MB of On-Board Memory

LAN Support shall utilize RJ45 (10/100baseT) Ethernet Interface connectivity

Flash Memory for real time program updates and overall host communications

Memory storage of up to 132,000 cardholders

Support for up to 32 devices consisting of relay, input, and output modules, in any combination desired, with a maximum of 16 I/OCM devices per Controller

Support up to 9 door groups per controller

Support of multiple card technologies

Supervised Communications between Controller and Velocity EACIDS Software

AES 128 bit Symmetrical Block Encryption conforming to the FIPS-197 standard and conforming to the ICD 705 standard between Controller and Velocity EACIDS Software communications driver.

Multi – drop support for up to eight Controllers per Velocity EACIDS communications port

Support multiple card formats simultaneously

Support for FIPS 201-compliant card formats

RS-485 Full Duplex, UL 1076 Grade AA communication channel to the Velocity EACIDS head-end

Integration to other manufacturer’s card readers

Uninterruptible Power Supply (UPS) with battery backup (** Specify the amount of Backup Time Required)

32-bit Microprocessor

A Controller downstream serial port shall multi-drop 16 access control field hardware devices using an RS-485 UL 1076 Grade A communication format allowing a distance of 4,000 feet using Belden 9842 cable or equivalent

28 VDC input power

Issue Code Support for both Magnetic and Wiegand Card Formats

Individual Shunt Times (ADA Requirement)

Up to 15 Digit PIN Codes, including duress PIN Codes

Downstream serial RS-232 device support

Status LEDs for normal component and communication status

PRODUCTS

PRODUCT ACCEPTABILITY

The Products section contains lists of acceptable products. If product substitutions are proposed, they must be made based upon a comparison of equivalence to the product specified. Considerations may include but shall not be limited to functional, physical, aesthetic and/or interface aspects. CLIENT shall be the sole judge of whether or not a submitted substitution is deemed to be "equivalent" to that specified.

ELECTRONIC ACCESS CONTROL EQUIPMENT

System: Identiv Velocity Security Management System.

Software:

Software: Identiv Velocity Version 3.6, or latest supported version

Contractor shall provide a minimum of two (2) reprogramming sessions within twelve (12) months of the final acceptance of the system to modify the user programming.

The server software shall support Cold Redundant, Warm Redundant, Hot Redundant, and clustered server environments.

System shall be compatible with Virtual Machine environment such as VMWare or HyperV

During installation support for split SQL Server Database server and Application/Communication server shall be available.

Servers and Workstations: Provide Servers and Client Workstations as noted herein and as shown on the plans. The following describes the minimum guideline configuration for servers and workstations. The Contractor shall be responsible for insuring the acceptable performance of the system based on the Velocity EACIDS manufacturers' hardware requirements, the performance criteria specified herein for the access control system, and Client’s server standards.

Velocity EACIDS Server: The Primary Velocity EACIDS server shall be located in the {Identify Location} data center [and the redundant Velocity EACIDS server shall be located in {Identify Location}]. The primary and redundant server shall have the same hardware configuration.

The Server computer shall be a Dell Power Edge R710 or equal by IBM, or Hewlett Packard, 100% compatible Xeon E3-1220, 3.10 GHz Turbo Quad Core/4T or faster processor, configured as required by the manufacturer, with the following minimum attributes:

Rack-Mount Configuration (2 RU)

8 GB 1333MHz UDIMMS, Advanced ECC DDR3 RAM.

8 MB Cache

Raid Controller (Supports RAID 0, 1, 5, and 10): Embedded 6GB/s SAS, w/512MB cache

300.0 GB 15K RPM SAS Disk Drive (Provide number required for selected RAID configurat

DVD +/-RW, SATA Optical Drive

Computer Monitor/Keyboard/Mouse, 17" Flat Panel w/keyboard and mouse: Provide Dell Keyboard/Mouse/Monitor unit in 2 RU pull out rack drawer.

Video controller with 1GB of memory.

Sound Card and Speakers

1 eSATA Port

System compatible Bus Mouse and Hardware.

2 Parallel Ports LPT1 and LPT2.

2 Serial Ports, COM1 and COM2.

Software and hardware as recommended by Honeywell to provide hot redundant back-up services.

Microsoft Windows Server 2008 R2 64-bit Standard or Enterprise edition multi-tasking operating system platform with graphical user interface as required by system software. Also available and supported: Windows 8.1, Windows Server 2012, and Windows Server 2012 R2.

Security Network: The Server shall be capable of providing Network communications between Client Workstations subservient to the Server and to other Server or Administrative Workstations. Data, alarms, and information shall be shared between Server and Client Workstations at the discretion of the network administrator.

Network Interface Board: 1000BaseT Ethernet Communications Board, compatible with existing customer LAN network

Database Platform

Server: SQL Server 2012 R2 64-bit Standard, Workgroup, or Enterprise edition with SP1

Workstation: SQL Server 2012 R2 Express (Included with Velocity EACIDS software)

Client: Database connection to Server

Client Workstations: Provide Client Workstation as shown on the plans. The following describes the minimum guideline configuration for the Velocity EACIDS workstation. The Security Contractor shall be responsible for insuring the acceptable performance of the system based on the Velocity EACIDS manufacturers' hardware requirements and the performance criteria specified herein for the Velocity EACIDS.

The Workstation shall be a Dell T5500, HP Z400, or equal by IBM 100% compatible i7 Quad Core, 3.4 GHz or faster computer, configured as required by the manufacturer, with the following minimum attributes:

Rack-Mount, tower or desk top Configuration as required by location

8GB, DDR3 RDIMM,1333 MHz, ECC

12 MB L3 Cache

SATA Drive Adapter

250 GB SATA 3.0 GB/s Hard Disk Drive w/integrated controller

Recordable Optical DVD+R/+RW Drive with backup software, 24X write: The recordable DVD drive shall be used for system backups and to record stored video clips for archival and off site use.

Standard Monitor (24”): Provide Computer Monitor, 24" Flat Panel Color LCD Display Monitor. Monitor shall utilize TFT Active Matrix LCD technology, minimum 1000:1 contrast ratio and 250 cd/m2 brightness, resolution of 1920 x 1080, and a minimum viewing angle of 160 vertical x 170 horizontal. Provide Dell Professional P2210 22” HAS wide monitor or equal.

DVI Color Graphics Display Board: nVidia QuadroFX 4800, 1.5GB, dual monitor DVI board, or equal with cable compatible with selected monitor.

Sound Card: High Definition Integrated Realtek ALC262 Audio or Soundblaster Audigy II with on board 1394

System compatible Bus Mouse and Hardware

4 USB 2.0 ports

2 Serial Ports, COM1 and COM2

Microsoft Windows 10 SP1 32-bit or 64-bit Professional, Ultimate, or Enterprise edition multi-tasking operating system platform with graphical user interface and any additional software programs required to meet specifications

Network Card: 1 GB Ethernet Communications Board, compatible with WBMWD’s existing LAN network

[Fault-Tolerant Server: Provide redundant fault-tolerant Windows server 2012 R2 operating system, SQL Server 2012 database, with flat panel monitor.]

System Controller Panels: Provide sufficient controllers and input/output boards to meet all requirements of specifications.

Velocity EACIDS Controller: Where new controllers are required, provide the following;

Identiv Mx Controller, compatible with the Velocity EACIDS application software, with a flash ROM module, power supply, battery standby, and Communications Module, as described herein.

Contractor shall review drawings and specifications with the Project Representative, and may propose changes to the topology of the system based on device layout, where such changes improve performance or functionality of the system. Client has final authority as to the final approach for system topology.

Reader Support: Controller shall be configurable for 2, 4, or 8 readers. Enclosure, controller board, and accessories shall be the same for 2, 4, or 8 reader configuration for consistency in system hardware layout. Controllers shall be field upgradeable from 2 to 4 to 8 doors through firmware upgrade.

Provides Boolean logic functions for input/output points for primary and downstream controllers without need for host server

Dedicated encryption processor to enable PKI based certificate level encryption between controllers and host server. Encryption shall also include encrypted communication to readers with imbedded encryption processor.

The controller shall have integrated network communications with onboard Ethernet port.

High security supervised alarm points.

Configurable output relays.

Expansion capability within standard controller enclosure footprint:

Memory up to 132,000 users

8-input Alarm Expansion Boards – up to 4

8-output Relay expansion boards – up to 5

Controllers shall be capable of upgrading the firmware through the Velocity EACIDS head-end without requiring the need to access each controller to upgrade the firmware.

The controller shall support a MATCH reader interface board for entry/exit readers for a single door utilizing a single reader port on the controller.

The MATCH reader interface board shall enable enhanced cable distance from reader to controller up to 1,800 feet using 18 gauge wires.

CODE/Buffer: The controller shall be capable of expanding the CODE database up to a maximum of 132,000 Users with the addition of a memory expansion board. The board shall be mounted in the controller cabinet and connect to the controller board via an expansion bus cable. The CODE/Buffer expansion board shall be Identiv Model MEB\CB64 (64,000 Users) or the MEB\CB128 (128,000 Users). Both Expansion Boards shall expand the Buffer capacity as well as the Code record capacity. The Model M1N shall not accept any CODE/Buffer Expansion board.

Event Transaction Buffer: The controller shall be capable of expanding the event transaction buffer up to a maximum of 20,000 events and 2,000 alarms with the addition of a memory expansion board. The board shall be mounted in the controller cabinet and connect to the controller board via an expansion bus cable. The event transaction buffer expansion board shall be Identiv Model MEB\BE. The Model M1N shall not accept a Buffer Expansion board.

Controllers shall utilize Version 7.5.37 or later flash downloadable CCM (Command and Control Module) firmware.

Controller General Features: The software for the controller shall reside in Flash ROM (firmware) and be located on a plug removable module on the controller board to facilitate easy field upgradeability of the features. All of the necessary software for a fully functional System is located in the controller. The controller firmware shall be fully supported by the Velocity EACIDS head-end, and include the following general features at a minimum:

3 - 15 digit keypad Codes.

Duress digit for keypad codes.

150 Time Zones for access restriction and automatic event control.

128 Access Zones for access management.

256 Control Zones for alarm and relay management.

366 programmable holidays this year, 366 days next year. Each Holiday may be assigned to 1 - 4 Holiday Schedules.

Automatic daylight savings time clock adjustment.

27 different functions for Codes and cards, such as access, unlock, re-lock, alarm mask, and relay control.

Add user records.

Tag users for annunciation at host computer.

4,000 Users.

1500 event, 1500 alarm transaction buffer

Access Control Features: The controller shall include the following access control features at a minimum

Restrict access by: time of day; day of week; door; holiday.

Momentary Access of door up to 8100 seconds.

Extended Access for User Definable Momentary Access duration (requires ScramblePad). ScramblePad will display time remaining on the minute, and annunciate at the defined "Warning Time".

Special Needs Time Extension to provide additional time for Momentary Access and Door Open Too Long for selected people.

Unlock/Re-lock of door by CODE, card, or Time Zone.

Door status monitoring shall allow for: door forced monitoring; door-open-too-long monitoring; door-open-too-long while door is unlocked; and auto-re-lock of door when opened or closed.

Request-to-exit masks alarm and/or unlocks door.

2 person requirement by door. A user can be defined as Normal, A/B Rule A, A/B Rule B, or Executive Override. Can be disabled by Time Zone.

63 Passback Zones. Can be disabled by Time Zone. A User can be designated with Passback Executive Override.

Use Count limits on users.

Absentee Rule limits on users.

Temporary Day limits on users.

Occupancy Counting / Minimum & Maximum limits per Passback Zone.

Deadman CODE / Timer.

Threat Levels – 99 Levels may be defined. Based on the Level in effect for the facility, selected readers may be disabled, dual readers in Card/Code Only During Time Zone can require dual, and selected User's Credentials can be disabled.

Timed Anti-Passback

Alarm Management Features: The controller shall include the following alarm management features at a minimum:

Momentarily mask alarm by CODE and/or card.

Mask/unmask alarm by CODE and/or card or by Time Zone.

Alarm device supervised while masked.

Tamper switch on alarm device monitored while masked.

Tamper Input may be configured to operate as a "Latch Monitor" with the appropriate door lock hardware.

Entry/Exit delay per alarm input.

Alarm input triggers relays

Relay Control Features: The controller shall include the following relay control features at a minimum:

CODE and/or card, input, or other relay triggers relays.

Trigger relays by time zone.

Relay may be normally de-energized or energized.

Disable relays during time zone.

Clear relay at end of time zone

Controller Connectivity

Controllers shall support connection to the security LAN/WAN using TCP/IP protocol, and shall also support connection to the manufacturer's standard data communications protocol (RS-232, RS-485, or RS-422).

TCP/IP-connected controllers may act as a network "gateway", to re-transmit controller data via the manufacturers standard data communications protocol (RS-232, RS-485, or RS-422), to other Velocity EACIDS controllers located within the same site. Provide controllers which support the manufacturer's standard data communications protocol, RS-232/RS-485, as required.

LAN/WAN Interface Board: Model SNIB2 10/100 Mbps interface with 128-bit AES encryption.

LAN/WAN Interface Board: Model SNIB3 10/100/1000 Mbps interface, both IPv4 and IPv6 addressing is available with 256-bit AES encryption.

Intelligent Reader Interface: The control panels shall utilize an intelligent reader interface (Model: MRIA or MRIB) to communicate with card readers of various types. The interface shall be microprocessor based and allow data formats including ABA magnetic stripe, Wiegand (26- to 55-bit), Proximity, Bar Code, Touch Memory, RF, and Biometric. The interface shall utilize a digitizing algorithm, which will convert the card data to a unique number, thus eliminating the need for facility codes. A single interface shall support both entrance and exit readers with keypads associated with each door. The interface shall be U.L. Listed to U.L.294. The reader interface shall be included as standard in all Scramble Pads.

Alarm Inputs: The controller shall be capable of accepting up to 32 additional supervised alarm inputs, in increments of eight (8). The sensitivity of the line supervision shall be 2% AA Standard. The alarm expansion boards shall be mounted in the controller cabinet and connect to the controller board via an expansion bus cable. This option shall be limited to 16 additional supervised alarm inputs for the 16-zone alarm input controller (Model M16N), and none for the Model M1N. The alarm expansion board shall be Identiv Model AEB8.

Relay Output: The access control (Model M2N, Model M8N, and Mx) and alarm monitoring (Model M16N) controllers shall be capable of accepting up to 32 additional Form C, 2 Amp rated relay outputs in increments of 8. The 1 - 32 relay controller (Model MSPN-8R) shall accept up to a maximum of 24 additional Form C, 2 Amp rated relay outputs in increments of 8. The 1 - 64 relay controller (Model M64N) and the Model M1N shall not accept any additional relay outputs. These outputs shall be used for control applications other than standard door access, such as elevator floor control, local door

annunciators, HVAC interface, etc. The relay expansion boards shall be mounted in the controller cabinet and connect to the controller board via an expansion bus cable. The relay expansion board shall be Identiv Model REB8.

Controller Power Supply: Provide Identiv Model PSH5A power supply based on panel configuration.

Battery Back-up: Provide Identiv Model SB7AH batteries to provide battery back-up on 120 VAC power failure.

Multi-Frequency, Multi-Technology, contactless card reader: The multi-frequency contactless card reader(s) shall be designed to securely read, decipher, and authenticate user card data from 13.56 MHz and 125 kHz proximity cards

Shall be able to securely authenticate with cards that support a PLAID applet, extract and process the employee format data for building access

Support all three modulations of 125 KHz proximity card technologies (ASK, PSK, FSK) within the same standard reader and output card data from all three modulations in succession.

Supports programming and re-flashing through RS-485 data protocol

Through the use of a device certificate the reader shall support Strong Identity Verification when authenticated with identity cards that carry an employee certificate.

Reader connectivity shall include Wiegand and RS-485 protocols

The reader shall support enhanced security technology features including:

Optical sensor that detects physical tampering of the reader by the removal of the reader from its mounting plate

The multi-frequency contactless card reader shall utilize Secure Access Module to protect keys and cryptographic functions to the international standard Evaluation Assurance Level (EAL) 5+.

The multi-frequency contactless card reader shall provide enhanced usability features including

The reader shall support a Near Field Communication for reading NFC tokens

The multi-frequency contactless card reader shall provide enhanced user feedback options through the use of tri-colored LEDs configurable to support any three color combinations (RGB - Red, Green, and Blue).

Multi-frequency contactless card reader shall allow for secure installation mounting by utilizing tamper resistant screws

Multi-frequency contactless card reader shall provide the following configurable audio/visual feedback:

An audible device shall provide various tone sequences to signify: access granted, access denied, power up, and diagnostics.

A high-intensity red/green/blue (RGB) light ring shall provide clear visual status. The light ring shall provide uniform distribution of light eliminating individual bright spots

The multi-frequency contactless card reader shall provide the ability to upgrade its application code through the use of a cloud based application library.

Multi-frequency contactless card reader shall provide the ability for mounting to standard electrical boxes through the use of universal international mounting holes.

Multi-frequency contactless card readers shall provide the following compatibility features including:

The multi-frequency contactless card reader shall provide simultaneous support for 125 kHz proximity FSK (HID, AWID), PSK (Indala), and ASK (Casi Rusco) 125 kHz.

13.56MHz including MIFARE, DESFire EV1 and SmartMX applets including PIV and PLAID

ISO14443A/B & ISO15693 UID support

Sony FeliCa CSN

PIV and CIV compatibility

CAK validation

TWIC compatibility

FICAM smartcard validation compatibility

Multi-frequency contactless card reader shall provide enhanced environmental and sustainability features including:

Multi-frequency contactless card reader shall be fully compliant with Restriction of Hazardous Substances directive (RoHS) restricting the use of specific hazardous materials found in electrical and electronic products. The substances banned under RoHS are lead (Pb), mercury (Hg), cadmium (Cd), hexavalent chromium (CrVI), polybrominated biphenyls (PBB) and polybrominated diphenyl ethers (PBDE).

Multi-frequency contactless card reader shall comply with the following standards to ensure product compatibility and predictability of performance

Technical Standards

ISO 15693

ISO 14443A

ISO 14443B

Global Platform 2.1.1

Open Platform Java card 2.2.2

Certifications

FCC: reader shall comply with Part 15 of the FCC Rules

IC: reader shall comply with Industry Canada license-exempt RSS standard(s).

CE: reader shall be in compliance with essential requirements and other relevant portions of Directive R&TEE 1999/5/EC

The reader shall be compliant with RoHS requirements

IP65

UL294

Multi-frequency contactless card reader shall be provided with a full potted assembly.

Multi-frequency contactless card reader shall provide the following typical contactless read ranges:

SmartMX: Up to 3 cm

MIFARE/DESFire : Up to 5 cm

Proximity: Up to 6 cm

Multi-frequency contactless card reader shall be designed for low current operation. Power requirements shall be:

Operating voltage: 5 – 16 VDC, reverse voltage protected. Linear power supply recommended

Peak power consumption: 100mA or less (nominal)

Multi-frequency contactless card reader shall meet the following physical specifications:

Dimensions: 11.8cm x 4.3cm x 2.8cm

Weight: 235g Terminal Strip

Material: UL94 Polycarbonate

Plastics: Consist of two-piece design with mounting plate and separate front bezel / reader body with built in circular LED diffuser.

Color: Black

Multi-frequency contactless card reader shall meet the following environmental specifications:

Operating temperature: -35 to 65 degrees C

Operating humidity: 5% to 95% relative humidity non-condensing

Multi-frequency contactless card reader cabling requirements shall be:

Cable distance: (Wiegand): 150m

Cable type: 8-conductor #22 AWG (Shielded cable not required)

Reader termination: Terminal strip or pigtail

The multi-frequency contactless card reader shall provide a lifetime warranty against defects in materials and workmanship.

Multi-frequency contactless card reader [Select from options below for each specific project]

Identiv Model 8000: Mullion Mount, 13.56 MHz only, Pigtail or Terminal Connection

Identiv Model 8010: Mullion Mount, 125 kHz / 13.56 MHz, Pigtail or Terminal Connection

Identiv Model 8030: Mullion Mount, 125 kHz / 13.56 MHz, 6-pin Connector, RJ-45 PoE option

Identiv Model 8100: Wall Mount, 13.56 MHz only, Pigtail or Terminal Connection

Identiv Model 8110: Wall Mount, 125 kHz / 13.56 MHz, Pigtail or Terminal Connection

Identiv Model 8210: Wall Mount, 125 kHz/ 13.56 MHz, With Keypad, Terminal Connection

Identiv Model 8130: Wall Mount, 125 kHz / 13.56 MHz, 6-pin connector, RJ-45 PoE option.

ScramblePad Digital Keypad: The controller shall be capable of using scrambling keypad readers. The keypad shall incorporate the following features:

Scrambling display of numbers 0 - 9 (numbers appear in different location every time it is used); +/- 4 degrees horizontal and +/- 26 degrees vertical viewing restriction; accept 3 - 15 digit CODEs simultaneously; be disabled for 1 minute and report CODE Tamper violation (guessing CODEs); be disabled and report Physical Tamper violation (attempt to remove keypad from mounting box); silent CODE duress; status LEDs for reporting granted, denied, and overridden transactions, AC Fail, Programming Mode active, responses to Status Request of Alarm Inputs and Relay Outputs; weather-resistant; supervised by controller; and built-in diagnostics. The ScramblePad shall include the MATCH Reader Interface functionality for connection of up to two (2) card readers. The scrambling keypad shall be the Identiv ScramblePad Model DS47L.

A version of the scrambling keypad shall be available for use in high ambient lighting conditions, or where the front is subject to direct sunlight. This version shall have a +/- 12 degrees horizontal and +/- 26 degrees vertical viewing restriction. The high intensity display scrambling keypad shall be the Identiv ScramblePad Model DS47L-HI.

A version of the scrambling keypad shall be available with an integrated HID compatible proximity card reader. Presentation of the card shall automatically auto-start the scrambling display. The scrambling keypad with integrated proximity card reader shall be the Identiv ScrambleProx Model DS47L-SPX. High Intensity (DS47L-SPX-HI)

A version of the scrambling keypad with high intensity display shall be available with an integrated Indala compatible proximity card reader. Presentation of the card shall automatically auto-start the scrambling display. The scrambling keypad with integrated proximity card reader shall be the Identiv ScrambleProx Model DS47L-SPX-I. High Intensity (DS47L-SPX-I-HI)

A version of the scrambling keypad shall be available with an integrated smart card reader and HID proximity reader. Presentation of the card shall automatically auto-start the scrambling display. The scrambling keypad with integrated smart card reader and HID Proximity Reader shall be the Identiv ScrambleSmartProx Model DS47L-SSP-HID.

A version of the scrambling keypad with high intensity display shall be available with an integrated smart card reader and HID proximity reader. Presentation of the card shall automatically auto-start the scrambling display. The scrambling keypad with integrated smart card reader and HID proximity reader shall be the Identiv ScrambleSmartProx Model DS47L-SSP-HID-HI.

A version of the scrambling keypad with high intensity display shall be available with an integrated smart card reader and HID proximity reader. Presentation of the card shall automatically auto-start the scrambling display. The scrambling keypad with integrated smart card reader and HID proximity reader shall be the Identiv ScrambleSmartProx Model DS47L-SS-HID-HI.

Credentials (Access Cards):

Access cards shall be used with access readers to gain entry to access controlled portals. The card shall be made of durable material and shall be in a form suitable for direct one-sided dye-sublimation printing on the specified badge printer. Presentation to the access control reader at any angle within a minimum of two (2) inches shall result in an accurate reading of the card.

Provide [quantity] access cards compatible with the specified card readers.

The card shall not carry any identification showing the location of the property unless otherwise specified herein.

Provide [quantity] badge protectors, with clips, of a type acceptable to the Engineer.

Provide {Manufacturer} Model {Model Name} card or equal. Card shall be configured for compatibility with selected reader and controller

FICAM Credential Security (Smart Cards)

Smart cards shall be checked for certificates at specified intervals

Degraded mode shall be either enabled or disabled

OSDP addresses shall be assignable to any FICAM-compatible reader in the range from 0-126

RS-485 interface shall be available for FICAM-compatible readers

FICAM card validation profiles shall be available for badging roles

Controller Tamper Switch: Provide a tamper switch on the Controller enclosure. Connect to the system as an individual alarm point.

Terminations: Provide all connections to labeled screw barrier terminal blocks.

Secure all devices within the Controller enclosure. Dress all wiring in a neat and competent manner. Label all conductors to match documentation.

EXECUTION

GENERAL

The Contractor shall be a Certified Velocity Distributor and have 10 years experience installing Velocity systems, and have performed similar installations for the City of Del City. No subcontractors allowed. Contractor shall install system components and appurtenances in accordance with the manufacturer's instructions, and as shown. The Contractor shall furnish necessary interconnections, services, and adjustments required for a complete and operable system as specified and shown.

Follow the General Requirements of Section 28 05 00, Common Work Results for Electronic Safety and Security for equipment and services provided under this section.

Installation: The Contractor shall install the system in accordance with the standards for safety, NFPA 70, UL 681, UL 1037 and UL 1076, and the appropriate installation manual for each equipment type. Flexible cords or cord connections shall not be used to supply power to any components of the system, except where specifically noted. All other electrical work shall be as specified in Division 26, and as shown.

EQUIPMENT, RACK AND CONSOLE INSTALLATION

Mount equipment in rooms, consoles, equipment racks, and desktops in accordance with Section 28 05 00, Common Work Results for Electronic Safety and Security.

GROUNDING PROCEDURES

Provide grounding of all systems and equipment in accordance with Section 28 05 00, Common Work Results for Electronic Safety and Security.

WIRE AND CABLE INSTALLATION PRACTICES

Provide wire and cable installation in accordance with Section 28 05 00, Common Work Results for Electronic Safety and Security.

DATABASE PREPARATION, CHECKING AND ACTIVATION

Provide database preparation, checking, and activation in accordance with Section 28 05 00, Common Work Results for Electronic Safety and

Security. START-UP RESPONSIBILITY

Provide start-up services for all systems and equipment in accordance with Security General Requirements, Section 28 00 00.

SYSTEM PERFORMANCE TESTING AND ADJUSTING PROCEDURES

Provide Preliminary Testing, Inspection, Performance Verification Testing, Commissioning and Endurance Testing services for Velocity EACIDS systems and equipment in accordance with Section 28 05 00, Common Work Results for Electronic Safety and Security.

Electronic Access Control and Intrusion Detection System Testing

Test and verify the normal operation of every alarm point in all states at each alarm panel – normal, alarm (forced entry), door propped, noisy, short, out- of-spec, tamper. Test each alarm point for the alarm function by normal operation of the alarm point, i.e.: for a door position switch, open the door and so forth.

Test and verify the operation of the Electronic Access Control and Intrusion Detection System.

Test each door during its programmed secure time period to assure that it commands the lock to activate and permits access by valid credential within one second from presentation of the key.

Verify all egress systems on access controlled doors work correctly.

Verify system integration schemes function automatically and

correctly. Verify all activity at Monitoring Stations functions correctly.

FINAL PROCEDURES

Perform final procedures in accordance with Section 28 05 00, Common Work Results for Electronic Safety and Security.

END OF
SECTION