State of West Virginia
Department of Administration
Purchasing Division
2019 Washington Street East
Post Office Box 50130
Charleston, WV 25305-0130

Request for Quotation

RFQ NUMBER	PAGE
DEFK9007	1

ADDRESS CORRESPONDENCE TO ATTENTION OF:
JOHN ABBOTT
304-558-2544

VENDOR
RFQ COPY
TYPE NAME/ADDRESS HERE

SHIP TO
DIV ENGINEERING & FACILITIES
HUNTINGTON TRI-STATE AFRC

2194 BOOTH DRIVE
KENOVA, WV
25330 304-453-5780

DATE PRINTED	TERMS OF SALE	SHIP VIA	F.O.B.	FREIGHT TERMS
08/27/2008				

BID OPENING DATE: 09/18/2008 BID OPENING TIME 01:30PM

LINE	QUANTITY	UOP	CAT. NO.	ITEM NUMBER	UNIT PRICE	AMOUNT
0001	1	LS		680-02		

ACCESS CONTROL SYSTEM

CONTRACT TO PROVIDE ALL LABOR, MATERIALS, AND EQUIPMENT NECESSARY TO INSTALL AN ACCESS CONTROL SYSTEM AT THE WV ARMY NATIONAL GUARD READINESS CENTER, KENOVA, WV, PER THE SPECIFICATIONS.

MANDATORY ON-SITE PRE-BID: 9/10/2008; 1:30 PM
WVANG, READINESS CENTER
2194 BOOTH DRIVE
KENOVA, WV 25539

CONTACT: WILLIAM "BILL" SUVER AT 304-561-6454 TO CONFIRM ATTENDANCE AND/OR DIRECTIONS.

EXHIBIT 5

NOTICE TO PROCEED: THIS CONTRACT IS TO BE PERFORMED WITHIN XXXX CALENDAR DAYS AFTER THE NOTICE TO PROCEED IS RECEIVED. UNLESS OTHERWISE SPECIFIED, THE FULLY EXECUTED PURCHASE ORDER WILL BE CONSIDERED NOTICE TO PROCEED.

CANCELLATION: THE DIRECTOR OF PURCHASING RESERVES THE RIGHT TO CANCEL THIS CONTRACT IMMEDIATELY UPON WRITTEN NOTICE TO THE VENDOR IF THE MATERIALS OR WORKMANSHIP SUPPLIED ARE OF AN INFERIOR QUALITY OR DO NOT CONFORM WITH THE SPECIFICATIONS OF THE BID AND CONTRACT

SEE REVERSE SIDE FOR TERMS AND CONDITIONS

SIGNATURE	TELEPHONE	DATE

TITLE	FEIN	ADDRESS CHANGES TO BE NOTED ABOVE

WHEN RESPONDING TO RFQ, INSERT NAME AND ADDRESS IN SPACE ABOVE LABELED 'VENDOR'

GENERAL TERMS & CONDITIONS
REQUEST FOR QUOTATION (RFQ) AND REQUEST FOR PROPOSAL (RFP)

1. Awards will be made in the best interest of the State of West Virginia.

2. The State may accept or reject in part, or in whole, any bid.

3. All quotations are governed by the ***West Virginia Code*** and the ***Legislative Rules*** of the Purchasing Division.

4. Prior to any award, the apparent successful vendor must be properly registered with the Purchasing Division and have paid the required $125 fee.

5. All services performed or goods delivered under State Purchase Order/Contracts are to be continued for the term of the Purchase Order/Contracts, contingent upon funds being appropriated by the Legislature or otherwise being made available. In the event funds are not appropriated or otherwise available for these services or goods, this Purchase Order/Contract becomes void and of no effect after June 30.

6. Payment may only be made after the delivery and acceptance of goods or services.

7. Interest may be paid for late payment in accordance with the ***West Virginia Code***.

8. Vendor preference will be granted upon written request in accordance with the ***West Virginia Code***.

9. The State of West Virginia is exempt from federal and state taxes and will not pay or reimburse such taxes.

10. The Director of Purchasing may cancel any Purchase Order/Contract upon 30 days written notice to the seller.

11. The laws of the State of West Virginia and the ***Legislative Rules*** of the Purchasing Division shall govern all rights and duties under the Contract, including without limitation the validity of this Purchase Order/Contract.

12. Any reference to automatic renewal is hereby deleted. The Contract may be renewed only upon mutual written agreement of the parties.

13. BANKRUPTCY: In the event the vendor/contractor files for bankruptcy protection, this Contract may be deemed null and void, and terminated without further order.

14. HIPAA BUSINESS ASSOCIATE ADDENDUM: The West Virginia State Government HIPAA Business Associate Addendum (BAA), approved by the Attorney General, and available online at the Purchasing Division's web site (**http://www.state.wv.us/admin/purchase/vrc/hipaa.htm**) is hereby made part of the agreement. Provided that, the Agency meets the definition of a Cover Entity (45 CFR §160.103) and will be disclosing Protected Health Information (45 CFR §160.103) to the vendor.

15. WEST VIRGINIA ALCOHOL & DRUG-FREE WORKPLACE ACT: If this Contract constitutes a public improvement construction contract as set forth in Article 1D, Chapter 21 of the West Virginia Code ("The West Virginia Alcohol and Drug-Free Workplace Act"), then the following language shall hereby become part of this Contract: "The contractor and its subcontractors shall implement and maintain a written drug-free workplace policy in compliance with the West Virginia Alcohol and Drug-Free Workplace Act, as set forth in Article 1D, Chapter 21 of the West Virginia Code. The contractor and its subcontractors shall provide a sworn statement in writing, under the penalties of perjury, that they maintain a valid drug-free work place policy in compliance with the West Virginia and Drug-Free Workplace Act. It is understood and agreed that this Contract shall be cancelled by the awarding authority if the Contractor: 1) Fails to implement its drug-free workplace policy; 2) Fails to provide information regarding implementation of the contractor's drug-free workplace policy at the request of the public authority; or 3) Provides to the public authority false information regarding the contractor's drug-free workplace policy."

INSTRUCTIONS TO BIDDERS

1. Use the quotation forms provided by the Purchasing Division.

2. SPECIFICATIONS: Items offered must be in compliance with the specifications. Any deviation from the specifications must be clearly indicated by the bidder. Alternates offered by the bidder as **EQUAL** to the specifications must be clearly defined. A bidder offering an alternate should attach complete specifications and literature to the bid. The Purchasing Division may waive minor deviations to specifications.

3. Complete all sections of the quotation form.

4. Unit prices shall prevail in case of discrepancy.

5. All quotations are considered F.O.B. destination unless alternate shipping terms are clearly identified in the quotation.

6. BID SUBMISSION: All quotations must be delivered by the bidder to the office listed below prior to the date and time of the bid opening. Failure of the bidder to deliver the quotations on time will result in bid disqualifications: Department of Administration, Purchasing Division, 2019 Washington Street East, P.O. Box 50130, Charleston, WV 25305-0130

State of West Virginia
Department of Administration
Purchasing Division
2019 Washington Street East
Post Office Box 50130
Charleston, WV 25305-0130

Request for Quotation

RFQ NUMBER	PAGE
DEFK9007	2

ADDRESS CORRESPONDENCE TO ATTENTION OF:
JOHN ABBOTT
304-558-2544

VENDOR
RFQ COPY
TYPE NAME/ADDRESS HERE

SHIP TO
DIV ENGINEERING & FACILITIES
HUNTINGTON TRI-STATE AFRC

2194 BOOTH DRIVE
KENOVA, WV
25330 304-453-5780

DATE PRINTED	TERMS OF SALE	SHIP VIA	F.O.B	FREIGHT TERMS
08/27/2008				

BID OPENING DATE: 09/18/2008 BID OPENING TIME 01:30PM

LINE	QUANTITY	UOP	CAT NO	ITEM NUMBER	UNIT PRICE	AMOUNT

HERE IN.

WAGE RATES: THE CONTRACTOR OR SUBCONTRACTOR SHALL PAY THE HIGHER OF THE U.S. DEPARTMENT OF LABOR MINIMUM WAGE RATES AS ESTABLISHED FOR WAYNE COUNTY, PURSUANT TO WEST VIRGINIA CODE 21-5A, ET, SEQ. (PREVAILING WAGE RATES APPLY TO THIS PROJECT)

ARBITRATION: ANY REFERENCES MADE TO ARBITRATION OR INTEREST FOR PAYMENTS DUE (EXCEPT FOR ANY INTEREST REQUIRED BY STATE LAW) CONTAINED IN THIS CONTRACT OR IN ANY AMERICAN INSTITUTE OF ARCHITECTS DOCUMENTS PERTAINING TO THIS CONTRACT ARE HEREBY DELETED.

WORKERS' COMPENSATION: VENDOR IS REQUIRED TO PROVIDE A CERTIFICATE FROM WORKERS' COMPENSATION IF SUCCESSFUL.

ALL OF THE ITEMS CHECKED BELOW WILL BE A REQUIREMENT OF THIS CONTRACT:

(XX) INSURANCE: SUCCESSFUL VENDOR SHALL FURNISH PROOF OF COMMERCIAL GENERAL LIABILITY INSURANCE PRIOR TO ISSUANCE OF CONTRACT. UNLESS OTHERWISE SPECIFIED IN THE BID DOCUMENTS, THE MINIMUM AMOUNT OF INSURANCE COVERAGE REQUIRED IS $250,000.

( ) BUILDERS RISK INSURANCE: SUCCESSFUL VENDOR SHALL FURNISH PROOF OF BUILDERS RISK - ALL RISK INSURANCE IN AN AMOUNT EQUAL TO 100% OF THE AMOUNT OF THE CONTRACT.

(XX) BONDS: FIVE PERCENT (5%) OF THE TOTAL AMOUNT OF THE BID PAYABLE TO THE STATE OF WEST VIRGINIA, SHALL BE SUBMITTED WITH EACH BID AS A BID BOND. THE SUCCESSFUL BIDDER SHALL ALSO FURNISH A PERFORMANCE BOND AND LABOR/MATERIAL BOND FOR 100% OF THE AMOUNT OF THE CONTRACT. BONDS MAY BE PROVIDED IN THE FORM OF A CERTIFIED CHECK

SEE REVERSE SIDE FOR TERMS AND CONDITIONS

SIGNATURE	TELEPHONE	DATE

TITLE	FEIN	ADDRESS CHANGES TO BE NOTED ABOVE

WHEN RESPONDING TO RFQ, INSERT NAME AND ADDRESS IN SPACE ABOVE LABELED 'VENDOR'

State of West Virginia
Department of Administration
Purchasing Division
2019 Washington Street East
Post Office Box 50130
Charleston, WV 25305-0130

Request for Quotation

RFQ NUMBER	PAGE
DEFK9007	3

ADDRESS CORRESPONDENCE TO ATTENTION OF:
JOHN ABBOTT
304-558-2544

VENDOR
RFQ COPY
TYPE NAME/ADDRESS HERE

SHIP TO
DIV ENGINEERING & FACILITIES
HUNTINGTON TRI-STATE AFRC

2194 BOOTH DRIVE
KENOVA, WV
25330 304-453-5780

DATE PRINTED	TERMS OF SALE	SHIP VIA	F.O.B.	FREIGHT TERMS
08/27/2008				

BID OPENING DATE: 09/18/2008 BID OPENING TIME 01:30PM

LINE	QUANTITY	UOP	CAT. NO.	ITEM NUMBER	UNIT PRICE	AMOUNT

IRREVOCABLE LETTER OF CREDIT, OR BOND FURNISHED BY A SOLVENT SURETY COMPANY AUTHORIZED TO DO BUSINESS IN THE STATE OF WEST VIRGINIA. A LETTER OF CREDIT SUBMITTED IN LIEU OF A PERFORMANCE AND LABOR & MATERIAL BOND WILL ONLY BE ALLOWED FOR PROJECTS UNDER $100,000. PERSONAL OR BUSINESS CHECKS ARE NOT ACCECPTABLE IN LIEU OF THE 5% BID BOND, PERFORMANCE BOND, OR LABOR AND MATERIAL BOND.

( ) MAINTENANCE BOND: A TWO (2) YEAR MAINTENANCE BOND COVERING THE ROOFING SYSTEM WILL BE A REQUIREMENT OF THE SUCCESSFUL VENDOR.

REV. 11/00

EXHIBIT 7

DOMESTIC ALUMINUM, GLASS & STEEL IN PUBLIC WORKS PROJECTS

IN ACCORDANCE WITH WEST VIRGINIA CODE 5-19-1 ET., SEQ., EVERY CONTRACT FOR CONSTRUCTION, RECONSTRUCTION, ALTERATION, REPAIR, IMPROVEMENT OR MAINTENANCE OF PUBLIC WORKS, WHERE THE COST IS MORE THAN $50,000 AND, IN THE CASE OF STEEL ONLY, WHERE THE COST OF STEEL IS MORE THAN $50,000 OR WHERE MORE THAN 10,000 POUNDS OF STEEL ARE REQUIRED, THE STATE WILL ACCEPT ONLY ALUMINUM GLASS, OR STEEL PRODUCTS PRODUCED IN THE UNITED STATES. IN ADDITION, ITEMS OF MACHINERY OR EQUIPMENT PURCHASED FOR USE AT THE SITE OF PUBLIC WORKS SHALL BE MADE OF DOMESTIC ALUMINUM, GLASS OR STEEL, UNLESS THE COST OF THE PRODUCT IS LESS THAN $50,000 OR LESS THAN 10,000 POUNDS OF STEEL ARE USED IN PUBLIC WORKS PROJECTS.

FOREIGN MADE ALUMINUM, GLASS OR STEEL PRODUCTS MAY BE

SEE REVERSE SIDE FOR TERMS AND CONDITIONS

SIGNATURE	TELEPHONE	DATE

TITLE	FEIN	ADDRESS CHANGES TO BE NOTED ABOVE

WHEN RESPONDING TO RFQ, INSERT NAME AND ADDRESS IN SPACE ABOVE LABELED 'VENDOR'

State of West Virginia
Department of Administration
Purchasing Division
2019 Washington Street East
Post Office Box 50130
Charleston, WV 25305-0130

Request for Quotation

RFQ NUMBER	PAGE
DEFK9007	4

ADDRESS CORRESPONDENCE TO ATTENTION OF:
JOHN ABBOTT
304-558-2544

VENDOR
RFQ COPY
TYPE NAME/ADDRESS HERE

SHIP TO
DIV ENGINEERING & FACILITIES
HUNTINGTON TRI-STATE AFRC

2194 BOOTH DRIVE
KENOVA, WV
25330 304-453-5780

DATE PRINTED	TERMS OF SALE	SHIP VIA	F.O.B.	FREIGHT TERMS
08/27/2008				

BID OPENING DATE: 09/18/2008 BID OPENING TIME 01:30PM

LINE	QUANTITY	UOP	CAT. NO	ITEM NUMBER	UNIT PRICE	AMOUNT

ACCEPTED ONLY IF THE COST OF DOMESTIC PRODUCTS IS FOUND TO BE UNREASONABLE. SUCH COST IS UNREASONABLE IF IT IS 20% OR MORE HIGHER THAN THE BID PRICE FOR FOREIGN MADE PRODUCTS. IF THE DOMESTIC ALUMINUM, GLASS OR STEEL PRODUCTS TO BE SUPPLIED OR PRODUCED IN A "SUBSTANTIAL LABOR SURPLUS AREA", AS DEFINED BY THE UNITED STATES DEPARTMENT OF LABOR, FOREIGN PRODUCTS MAY BE SUPPLIED ONLY IF DOMESTIC PRODUCTS ARE 30% OR MORE HIGHER IN PRICE THAN THE FOREIGN MADE PRODUCTS.

IF, PRIOR TO THE AWARD OF A CONTRACT UNDER THE ABOVE PROVISIONS, THE SPENDING OFFICER OF THE SPENDING UNIT DETERMINES THAT THERE EXISTS A BID FOR LIKE FOREIGN ALUMINUM, GLASS OR STEEL THAT IS REASONABLE AND LOWER THAN THE LOWEST BID DOMESTIC PRODUCTS, THE SPENDING OFFICE MAY REQUEST, IN WRITING, A REEVALUATION AND REDUCTION IN THE LOWEST BID FOR SUCH DOMESTIC PRODUCTS. ALL VENDORS MUST INDICATE IN THEIR BID IF THEY ARE SUPPLYING FOREIGN ALUMINUM, GLASS OR STEEL.

REV. 3/88

EXHIBIT 9

NOTICE FOR ISSUANCE & ACKNOWLEDGEMENT OF CONSTRUCTION PROJECT ADDENDA

THE ARCHITECT/ENGINEER AND/OR AGENCY SHALL BE REQUIRED TO ABIDE BY THE FOLLOWING SCHEDULE IN ISSUING CONSTRUCTION PROJECT ADDENDA FOR STATE AGENCIES:

(1) THE ARCHITECT/ENGINEER SHALL PREPARE THE ADDENDUM AND A LIST OF ALL PARTIES THAT HAVE PROCURED DRAWINGS AND SPECIFICATIONS FOR THE PROJECT. THE ADDENDUM AND LIST SHALL BE FORWARDED TO THE BUYER IN THE STATE

SEE REVERSE SIDE FOR TERMS AND CONDITIONS

SIGNATURE	TELEPHONE	DATE

TITLE	FEIN	ADDRESS CHANGES TO BE NOTED ABOVE

WHEN RESPONDING TO RFQ, INSERT NAME AND ADDRESS IN SPACE ABOVE LABELED 'VENDOR'

State of West Virginia
Department of Administration
Purchasing Division
2019 Washington Street East
Post Office Box 50130
Charleston, WV 25305-0130

Request for Quotation

RFQ NUMBER	PAGE
DEFK9007	5

ADDRESS CORRESPONDENCE TO ATTENTION OF:
JOHN ABBOTT
304-558-2544

VENDOR
RFQ COPY
TYPE NAME/ADDRESS HERE

SHIP TO
DIV ENGINEERING & FACILITIES
HUNTINGTON TRI-STATE AFRC

2194 BOOTH DRIVE
KENOVA, WV
25330 304-453-5780

DATE PRINTED	TERMS OF SALE	SHIP VIA	F.O.B.	FREIGHT TERMS
08/27/2008				

BID OPENING DATE: 09/18/2008 BID OPENING TIME 01:30PM

LINE	QUANTITY	UOP	CAT NO.	ITEM NUMBER	UNIT PRICE	AMOUNT

PURCHASING DIVISION. THE ARCHITECT/ENGINEER SHALL ALSO SEND A COPY OF THE ADDENDUM TO THE STATE AGENCY FOR WHICH THE CONTRACT IS ISSUED.

(2) THE BUYER SHALL SEND THE ADDENDUM TO ALL INTERESTED PARTIES AND, IF NECESSARY, EXTEND THE BID OPENING DATE. ANY ADDENDUM SHOULD BE RECEIVED BY THE BUYER WITHIN FOURTEEN (14) DAYS PRIOR TO THE BID OPENING DATE.

(3) ALL ADDENDA SHOULD BE FORMALLY ACKNOWLEDGED BY ALL BIDDERS AND SUBMITTED TO THE STATE PURCHASING DIVISION. THE SAME RULES AND REGULATIONS THAT APPLY TO THE ORIGINAL BIDDING DOCUMENT SHALL ALSO APPLY TO AN ADDENDUM DOCUMENT. THE ONLY EXCEPTION MAY BE FOR AN ADDENDUM THAT IS ISSUED FOR THE SOLE PURPOSE OF CHANGING A BID OPENING TIME AND/OR DATE.

REV. 11/96

EXHIBIT 10

ADDENDUM ACKNOWLEDGEMENT

I HEREBY ACKNOWLEDGE RECEIPT OF THE FOLLOWING CHECKED ADDENDUM(S) AND HAVE MADE THE NECESSARY REVISIONS TO MY PROPOSAL, PLANS AND/OR SPECIFICATION, ETC.

ADDENDUM NOS.:

NO. 1 .....

NO. 2 .....

SEE REVERSE SIDE FOR TERMS AND CONDITIONS

SIGNATURE	TELEPHONE	DATE

TITLE	FEIN	ADDRESS CHANGES TO BE NOTED ABOVE

WHEN RESPONDING TO RFQ, INSERT NAME AND ADDRESS IN SPACE ABOVE LABELED 'VENDOR'

State of West Virginia
Department of Administration
Purchasing Division
2019 Washington Street East
Post Office Box 50130
Charleston, WV 25305-0130

Request for Quotation

RFQ NUMBER	PAGE
DEFK9007	6

ADDRESS CORRESPONDENCE TO ATTENTION OF:
JOHN ABBOTT
304-558-2544

VENDOR
RFQ COPY
TYPE NAME/ADDRESS HERE

SHIP TO
DIV ENGINEERING & FACILITIES
HUNTINGTON TRI-STATE AFRC

2194 BOOTH DRIVE
KENOVA, WV
25330 304-453-5780

DATE PRINTED	TERMS OF SALE	SHIP VIA	F.O.B.	FREIGHT TERMS
08/27/2008				

BID OPENING DATE: 09/18/2008 BID OPENING TIME 01:30PM

LINE	QUANTITY	UOP	CAT NO.	ITEM NUMBER	UNIT PRICE	AMOUNT

NO. 3 .....

NO. 4 .....

NO. 5 .....

I UNDERSTAND THAT FAILURE TO CONFIRM THE RECEIPT OF THE ADDENDUM(S) MAY BE CAUSE FOR REJECTION OF THE BIDS.

VENDOR MUST CLEARLY UNDERSTAND THAT ANY VERBAL REPRESENTATION MADE OR ASSUMED TO BE MADE DURING ANY ORAL DISCUSSION HELD BETWEEN VENDOR'S REPRESENTATIVES AND ANY STATE PERSONNEL IS NOT BINDING. ONLY THE INFORMATION ISSUED IN WRITING AND ADDED TO THE SPECIFICATIONS BY AN OFFICIAL ADDENDUM IS BINDING.

.....SIGNATURE

.....COMPANY

.....DATE

REV. 11/96

CONTRACTORS LICENSE

WEST VIRGINIA STATE CODE 21-11-2 REQUIRES THAT ALL PERSONS DESIRING TO PERFORM CONTRACTING WORK IN THIS STATE MUST BE LICENSED. THE WEST VIRGINIA CONTRACTORS LICENSING BOARD IS EMPOWERED TO ISSUE THE CONTRACTORS LICENSE. APPLICATIONS FOR A CONTRACTORS LICENSE MAY BE MADE BY CONTACTING THE WEST VIRGINIA DIVISION OF LABOR CAPITOL COMPLEX, BUILDING 3, ROOM 319, CHARLESTON, WV 25305. TELEPHONE: (304) 558-7890.

SEE REVERSE SIDE FOR TERMS AND CONDITIONS

SIGNATURE	TELEPHONE	DATE

TITLE	FEIN	ADDRESS CHANGES TO BE NOTED ABOVE

WHEN RESPONDING TO RFQ, INSERT NAME AND ADDRESS IN SPACE ABOVE LABELED 'VENDOR'

State of West Virginia
Department of Administration
Purchasing Division
2019 Washington Street East
Post Office Box 50130
Charleston, WV 25305-0130

Request for Quotation

RFQ NUMBER	PAGE
DEFK9007	7

ADDRESS CORRESPONDENCE TO ATTENTION OF:
JOHN ABBOTT
304-558-2544

VENDOR
RFQ COPY
TYPE NAME/ADDRESS HERE

SHIP TO
DIV ENGINEERING & FACILITIES
HUNTINGTON TRI-STATE AFRC

2194 BOOTH DRIVE
KENOVA, WV
25330 304-453-5780

DATE PRINTED	TERMS OF SALE	SHIP VIA	F.O.B.	FREIGHT TERMS
08/27/2008				

BID OPENING DATE: 09/18/2008 BID OPENING TIME 01:30PM

LINE	QUANTITY	UOP	CAT NO.	ITEM NUMBER	UNIT PRICE	AMOUNT

WEST VIRGINIA STATE CODE 21-11-11 REQUIRES ANY PROSPECTIVE BIDDER TO INCLUDE THE CONTRACTORS LICENSE NUMBER ON THEIR BID.

BIDDER TO COMPLETE:

CONTRACTORS NAME: .....

CONTRACTORS LICENSE NO.: .....

THE SUCCESSFUL BIDDER WILL BE REQUIRED TO FURNISH A COPY OF THEIR CONTRACTORS LICENSE PRIOR TO ISSUANCE OF A PURCHASE ORDER/CONTRACT

APPLICABLE LAW

THE WEST VIRGINIA STATE CODE, PURCHASING DIVISION RULE AND REGULATIONS, AND THE INFORMATION PROVIDED IN THE "REQUEST FOR QUOTATION" ISSUED BY THE PURCHASING DIVISION IS THE SOLE AUTHORITY GOVERNING THIS PROCUREMENT.

ANY INFORMATION PROVIDED IN SPECIFICATION MANUALS, OR ANY OTHER SOURCE, VERBAL OR WRITTEN, WHICH CONTRADICTS OR ALTERS THE INFORMATION PROVIDED FROM THE SOURCES AS DESCRIBED IN THE ABOVE PARAGRAPH IS VOID AND OF NO EFFECT.

BANKRUPTCY: IN THE EVENT THE VENDOR/CONTRACTOR FILES FOR BANKRUPTCY PROTECTION, THIS CONTRACT IS AUTOMATICALLY NULL AND VOID, AND IS TERMINATED WITHOUT FURTHER ORDER.

REV. 1/2005

SEE REVERSE SIDE FOR TERMS AND CONDITIONS

SIGNATURE	TELEPHONE	DATE

TITLE	FEIN	ADDRESS CHANGES TO BE NOTED ABOVE

WHEN RESPONDING TO RFQ, INSERT NAME AND ADDRESS IN SPACE ABOVE LABELED 'VENDOR'

State of West Virginia
Department of Administration
Purchasing Division
2019 Washington Street East
Post Office Box 50130
Charleston, WV 25305-0130

Request for Quotation

RFQ NUMBER	PAGE
DEFK9007	8

ADDRESS CORRESPONDENCE TO ATTENTION OF:
JOHN ABBOTT
304-558-2544

VENDOR
RFQ COPY
TYPE NAME/ADDRESS HERE

SHIP TO
DIV ENGINEERING & FACILITIES
HUNTINGTON TRI-STATE AFRC

2194 BOOTH DRIVE
KENOVA, WV
25330 304-453-5780

DATE PRINTED	TERMS OF SALE	SHIP VIA	F.O.B.	FREIGHT TERMS
08/27/2008				

BID OPENING DATE: 09/18/2008 BID OPENING TIME 01:30PM

LINE	QUANTITY	UOP	CAT. NO.	ITEM NUMBER	UNIT PRICE	AMOUNT

NOTICE

A SIGNED BID MUST BE SUBMITTED TO:

DEPARTMENT OF ADMINISTRATION
PURCHASING DIVISION
BUILDING 15
2019 WASHINGTON STREET, EAST
CHARLESTON, WV 25305-0130

THE BID SHOULD CONTAIN THIS INFORMATION ON THE FACE OF THE ENVELOPE OR THE BID MAY NOT BE CONSIDERED:

SEALED BID

BUYER: JOHN ABBOTT----------

REQ. NO.: DEFK9007----------

BID OPENING DATE: 9/18/08----------

BID OPENING TIME: 1:30 PM----------

PLEASE PROVIDE A FAX NUMBER IN CASE IT IS NECESSARY TO CONTACT YOU REGARDING YOUR BID:

PLEASE PRINT OR TYPE NAME OF PERSON TO CONTACT CONCERNING THIS QUOTE:

SEE REVERSE SIDE FOR TERMS AND CONDITIONS

SIGNATURE	TELEPHONE	DATE

TITLE	FEIN	ADDRESS CHANGES TO BE NOTED ABOVE

WHEN RESPONDING TO RFQ, INSERT NAME AND ADDRESS IN SPACE ABOVE LABELED 'VENDOR'

State of West Virginia
Department of Administration
Purchasing Division
2019 Washington Street East
Post Office Box 50130
Charleston, WV 25305-0130

Request for Quotation

RFQ NUMBER	PAGE
DEFK9007	9

ADDRESS CORRESPONDENCE TO ATTENTION OF:
JOHN ABBOTT
304-558-2544

VENDOR
RFQ COPY
TYPE NAME/ADDRESS HERE

SHIP TO
DIV ENGINEERING & FACILITIES
HUNTINGTON TRI-STATE AFRC

2194 BOOTH DRIVE
KENOVA, WV
25330 304-453-5780

DATE PRINTED	TERMS OF SALE	SHIP VIA	F.O.B	FREIGHT TERMS
08/27/2008				

BID OPENING DATE: 09/18/2008 BID OPENING TIME 01:30PM

LINE	QUANTITY	UOP	CAT NO	ITEM NUMBER	UNIT PRICE	AMOUNT
	****** THIS IS THE END OF RFQ DEFK9007 ****** TOTAL:					

SEE REVERSE SIDE FOR TERMS AND CONDITIONS

SIGNATURE	TELEPHONE	DATE

TITLE	FEIN	ADDRESS CHANGES TO BE NOTED ABOVE

WHEN RESPONDING TO RFQ, INSERT NAME AND ADDRESS IN SPACE ABOVE LABELED 'VENDOR'

ACCESS CONTROL SYSTEM INSTALLATION
WV Army National Guard
Kenova Readiness Center
Kenova, WV 25539

PART 1 - GENERAL

1.1 PROJECT

A. BASE BID – Provide design, materials, equipment, hardware and software and labor to install a facility access control system. Each bidder will quote a fully operational / installed access control system that complies with National Guards Bureau's (NGB) Electronic Security System (ESS) equipment Criteria and Standards or approved equal. This system has already been installed at more than ten WV-ARNG locations around the state, and must possess the capability to communicate with existing equipment to include software and hardware. Each bidder must provide a verification letter from National Guard Bureau as a general contractor to supply, install and maintain Galaxy Access Control Systems or approved equal. System alterations or substitutions must be compatible with existing NGB and State approved equal. Drawings shall be provided during mandatory pre-bid.

1.1 SUMMARY

A. This Section includes a security access system consisting of Central Station, operating system and application software, and field-installed Controllers connected by a high-speed electronic data transmission network. The security access system shall have the following:

1. Access Control:

a. Regulating access through doors, gates, or any other area that shall require control of access.
b. Anti-passback.
c. Visitor assignment.
d. Surge and tamper protection.
e. Credential cards and readers.
f. Push-button switches.
g. Monitoring of field-installed devices.
h. Reporting.

B. See Division 13 Section "Intrusion Detection" for interface devices and communications protocol to integrate security functions of that Section into security access system.

C. See Division 13 Section "Digital Surveillance" for interface devices and communications protocol to integrate motion detection and video camera selection and positioning into security access system.

1.2 SYSTEM DESCRIPTION

A. PC-based Central Station and Fujitsu Life Book U810 Mini-Notebook (Note Book minimum Specification: - A110 / 800 MHz - Ultra Mobile 2007 - RAM 1 GB - HDD 40 GB - WLAN : 802.11 Super AG, 802.11a/b/g, Bluetooth 2.0 - TPM - fingerprint reader - Vista Home Premium - 5.6" Widescreen TFT 1024 x 600 (WSVGA) - camera) shall be provided by the vendor, field-installed Controllers shall be installed by this contractor. The system shall also be connected to the owner's high-speed electronic data transmission network.

B. System shall consist of a PC-based Central Server, Workstation, and field-installed Controllers, connected by a high-speed electronic data transmission network.

1. System Software: Based on 32-bit, Microsoft Windows central-station operating system, server operating system, and application software. Software shall have the following capabilities:

a. Graphical user interface to show pull-down menus and a menu tree format that complies with interface guidelines of Microsoft Windows operating system.
b. System license shall be for the entire system and shall include capability for future additions that are within the indicated system size limits specified in this Section.
c. System shall have open architecture that allows importing and exporting of data and interfacing with other systems that are compatible with Microsoft Windows operating system.
d. Password-protected operator login and access.
e. System software shall be either Microsoft Windows XP Professional or Microsoft Windows 2000 Professional.

C. Network(s) connecting PCs and Controllers shall consist of one or more of the following:

1. Local area, IEEE 802.3 Fast Ethernet 100 BASE-TX, star topology network based on TCP/IP.

1.3 PERFORMANCE REQUIREMENTS

A. Security access system shall use a single database for access-control and credential-creation functions.

B. Distributed Processing: System shall be a fully distributed processing system so that information, including time, date, valid codes, access levels, and similar data, is downloaded to Controllers so that each Controller makes access-control decisions for that Location. Do not use intermediate Controllers for access control. If communications to Central Station are lost, all Controllers shall automatically buffer event transactions until communications are restored, at which time buffered events shall be uploaded to the Central Station.

C. Number of Locations: Support at Unlimited separate Locations using a single PC with combinations of direct-connect, dial-up, or TCP/IP LAN connections to each Location.

1. Each Location shall have its own database and history in the Central Station. Locations may be combined to share a common database.

D. Data Capacity:

1. Shall support all card technologies within the Controller.
2. 1500 access groups per site to allow or deny an operator to perform functions as determined by the owner.
3. Shall support biometric readers.
4. Shall support 10,000 event buffers per Controller.
5. System shall support up to 16 doors per Controller.

E. System Network Requirements:

1. Interconnect system components and provide automatic communication of status changes, commands, field-initiated interrupts, and other communications required for proper system operation.
2. Communication shall not require operator initiation or response, and shall return to normal after partial or total network interruption such as power loss or transient upset.
3. System shall automatically annunciate communication failures to the operator and identify the communication link that has experienced a partial or total failure.
4. Communications Controller may be used as an interface between the Central Station display systems and the field device network. Communications Controller shall provide functions required to attain the specified network communications performance.

F. Central Station shall provide operator interface, interaction, display, control, and dynamic and real-time monitoring. Central Station shall control system networks to interconnect all system components, including field-installed Controllers.

G. Field equipment shall include Controllers, sensors, and controls. Controllers shall serve as an interface between the Central Station and sensors and controls. Data exchange between the Central Station and the Controllers shall include down-line transmission of commands, software, and databases to Controllers. The up-line data exchange from the Controller to the Central Station shall include status data such as intrusion alarms, status reports, and entry-control records. Controllers are classified as alarm-annunciation or entry-control type.

H. System Response to Alarms: Field device network shall provide a system end-to-end response time of 5 second(s) or less for every device connected to the system.

I. False Alarm Reduction: The design of Central Station and Controllers shall contain features to reduce false alarms. Equipment and software shall comply with SIA CP-01.

J. Data Line Supervision: System shall initiate an alarm in response to opening, closing, shorting, or grounding of data transmission lines.

K. Door Hardware Interface: Coordinate with Division 8 Sections that specify door hardware required to be monitored or controlled by the security access system. The Controllers in this Section shall have electrical characteristics that match the signal and power requirements of door hardware. Integrate door hardware specified in Division 8 Sections to function with the controls and PC-based software and hardware in this Section.

1.4 SUBMITTALS

A. Product Data: For each type of product indicated. Include operating characteristics, furnished specialties, and accessories. Reference each product to a location on Drawings. Test and evaluation data presented in Product Data shall comply with SIA BIO 01-1993.02 (R2000.06) (SECURITY INDUSTRY ASSOCIATION - BIOMETRICS).

B. Shop Drawings:

1. Diagrams for cable management system.
2. System labeling schedules, including electronic copy of labeling schedules that are part of the cable and asset identification system of the software specified in Parts 2 and 3.
3. Wiring Diagrams. Show typical wiring schematics including the following:

   a. Outlets, jacks, and jack assemblies.
   b. Patch cords.
   c. Patch panels.

4. Cable Administration Drawings: As specified in Part 3 "Identification" Article.
5. Battery and charger calculations for Central Station and Controllers.

C. Project planning documents as specified in Part 3.

D. Field quality-control test reports.

1. Operation and maintenance data.

1.5 QUALITY ASSURANCE

A. Electrical Components, Devices, and Accessories: Listed and labeled as defined in NFPA 70, Article 100, by a testing agency acceptable to authorities having jurisdiction, and marked for intended use.

B. Comply with NFPA 70, "National Electrical Code."

PART 2 - PRODUCTS

2.1 MANUFACTURERS

A. In other Part 2 articles where titles below introduce lists, the following requirements apply to product selection:
1. Manufacturers: Subject to compliance with requirements, provide products by one of the manufacturers specified.

2.2 SECURITY ACCESS SYSTEM

A. Manufacturers:
1. Galaxy Control Systems.

2.3 Vendors:

A. In order to qualify for bidding, vendors must meet the following qualifications:
   1. Shall have a minimum of five (5) complete Galaxy Access Control (or approved equal) installations in the WVARNG within the past two (2) years.
   2. Shall have been in business for a minimum of 10 years.
   3. Shall have been manufacturer approved for NGB product installation and have a minimum of three (3) employees trained in NGB approved 600 Series systems (or approved equal) with required redundancy and specifications.
   4. Due to the sensitive nature of Access Controls, only the vendor that sells the products may bid as the prime or general contractor on this project.

2.4 APPLICATION SOFTWARE

A. System Software: Based on 32-bit, Microsoft Windows central-station operating system and application software. Software shall have the following features:
   1. Graphical user interface to show pull-down menus and a menu tree format.
   2. Capability for future additions within the indicated system size limits.
   3. Open architecture that allows importing and exporting of data and interfacing with other systems that are compatible with operating system.
   4. Password-protected operator login and access.

B. Application Software: Interface between the entry-control Controllers, to monitor sensors, operate displays, report alarms, generate reports, and help train system operators. Software shall have the following functions:
   1. Resides at the Central Station and Controllers as required to perform specified functions.
   2. Operate and manage peripheral devices.
   3. Manage files for disk I/O, including creating, deleting, and copying files; and automatically maintain a directory of all files, including size and location of each sequential and random-ordered record.
   4. Import custom icons into graphics views to represent alarms and I/O devices.
   5. Globally link I/O so that any I/O can link to any other I/O within the same Location, without requiring interaction with the host PC. This operation shall be at the Controller.
   6. Globally code I/O links so that any access-granted event can link to any I/O with the same Location without requiring interaction with the host PC. This operation shall be at the Controller.
   7. Messages from PC to Controllers and Controllers to Controllers shall be on a polled network that utilizes check summing and acknowledgment of each message. Communication shall be automatically verified, buffered, and retransmitted if message is not acknowledged.
   8. Selectable poll frequency and message time-out settings shall handle bandwidth and latency issues for TCP/IP, RF, and other PC-to-Controller communications methods by changing the polling frequency and the amount of time the system waits for a response.
   9. Automatic and encrypted backups for database and history backups shall be automatically stored at the central control PC and encrypted with a nine-character alphanumeric password, which must be used to restore or read data contained in backup.

10. Operator audit trail for recording and reporting all changes made to database and system software.

C. Controller Software:

1. Controllers shall operate as an autonomous intelligent processing unit. Controllers shall make decisions about access control, alarm monitoring, linking functions, and door locking schedules for its operation, independent of other system components. Controllers shall be part of a fully distributed processing control network. The portion of the database associated with a Controller and consisting of parameters, constraints, and the latest value or status of points connected to that Controller, shall be maintained in the Controller.
2. Functions: The following functions shall be fully implemented and operational within each Controller:

    a. Monitoring inputs.
    b. Controlling outputs.
    c. Automatically reporting alarms to the Central Station.
    d. Reporting of sensor and output status to Central Station on request.
    e. Maintaining real time, automatically updated by the Central Station every 24 hours.
    f. Automatically load new access card data as the cards are loaded.
    g. Communicating with the Central Station.
    h. Executing Controller resident programs.
    i. Diagnosing.
    j. Downloading and uploading data to and from the Central Station.

3. Controller Operations at a Location:

    a. Location: System shall control and unlimited amount of Controllers connected across a TCP/IP communications system. Globally operating I/O linking and anti-passback functions between Controllers within the same Location without central-station intervention. Linking and anti-passback shall remain fully functional within the same Location even when the Central Station is off line.
    b. In the event of communications failure between the Central Station and a Location, there shall be no degradation in operations at the Controllers at that Location. The Controllers at each Location shall be connected to a memory buffer with a capacity to store up to 20,000 events; there shall be no loss of transactions in system history files until the buffer overflows.
    c. Buffered events shall be handled in a first-in-first-out mode of operation.

4. Individual Controller Operation:

    a. Controllers shall transmit alarms, status changes, and other data to the Central Station when communications circuits are operable. If communications are not available, Controllers shall function in a stand-alone mode and operational data, including the status and alarm data normally transmitted to the Central Station, shall be stored for later transmission to the Central Station. Storage capacity for the latest 1024 events shall be provided at each Controller.

b. Card-reader ports of a Controller shall be custom configurable for at least 15 different card-reader or keypad formats. Multiple reader or keypad formats may be used simultaneously at different Controllers or within the same Controller.
c. Controllers shall provide a response to card-readers or keypad entries in less than 0.25 seconds, regardless of system size.
d. Initial Startup: When Controllers are brought on-line, database parameters shall be automatically downloaded to them. After initial download is completed, only database changes shall be downloaded to each Controller.
e. Failure Mode: On failure for any reason, Controllers shall perform an orderly shutdown and force Controller outputs to a predetermined failure mode state, consistent with the failure modes shown and the associated control device.
f. Startup After Power Failure: After power is restored, startup software shall initiate self-test diagnostic routines, after which Controllers shall resume normal operation.
g. Startup After Controller Failure: On failure, if the database and application software are no longer resident, Controllers shall not restart, but shall remain in the failure mode until repaired. If database and application programs are resident, Controllers shall immediately resume operation. If not, software shall be restored automatically from the Central Station.

5. Communications Monitoring:

a. System shall monitor and report status of RS-485 communications loop of each Location.
b. Communication status window shall display which Controllers are currently communicating, a total count of missed polls since midnight, and which Controller last missed a poll.
c. Communication status window shall show the type of CPU, the type of I/O board, and the amount of RAM memory for each Controller.

6. Operating systems shall include a real-time clock function that maintains seconds, minutes, hours, day, date, and month. The real-time clock shall be automatically synchronized with the Central Station at least once a day to plus or minus 10 seconds. The time synchronization shall be automatic, without operator action and without requiring system shutdown.

D. PC-to-Controller Communications:

1. Central-station communications shall use the following:

a. Direct connection using serial ports of the PC.
b. TCP/IP LAN network interface cards.

2. Serial Port Configuration: Each serial port used for communications shall be individually configurable for "direct communications," "modem communications incoming and outgoing," or "modem communications incoming only"; or as an ASCII output port.
3. Multiport Communications Board: Use if more than two serial ports are needed.

a. Expandable and modular design. Use a 4, 8, or 16 serial port configuration that is expandable to 32 or 64 serial ports.
b. Connect the first board to an internal PCI bus adapter card.

4. Direct serial, TCP/IP, and dial-up communications shall be alike in the monitoring or control of system, except for the connection that must first be made to a dial-up Location.
5. TCP/IP network interface card shall have an option to set the poll frequency and message response time-out settings.
6. PC-to-Controller and Controller-to-Controller communications (direct, dial-up, or TCP/IP) shall use a polled-communication protocol that checks sum and acknowledges each message. All communications shall be verified and buffered and retransmitted if not acknowledged.

E. Direct Serial or TCP/IP PC-to-Controller Communications:

1. Communication software on the PC shall supervise the PC-to-Controller communications link.
2. Loss of communications to any Controller shall result in an alarm at all PCs running the communications software.
3. When communications are restored, all buffered events shall automatically upload to the PC, and any database changes shall be automatically sent to the Controller.

F. Controller-to-Controller Communications:

1. Controller-to-Controller Communications: RS-485, 4-wire, point-to-point, regenerative (repeater) communications network methodology.
2. RS-485 communications signal shall be regenerated at each Controller.

G. Database Downloads:

1. All data transmissions from PCs to a Location, and between Controllers at a Location, shall include a complete database checksum to check the integrity of the transmission. If the data checksum does not match, a full data download shall be automatically retransmitted.
2. If a Controller is reset for any reason, it shall automatically request and receive a database download from the PC. The download shall restore data stored at the Controller to their normal working state and shall take place with no operator intervention.

H. Operator Interface:

1. Inputs in system shall have two icon representations, one for the normal state and one for the abnormal state.
2. When viewing and controlling inputs, displayed icons shall automatically change to the proper icon to display the current system state in real time. Icons shall also display the input's state, whether armed or bypassed, and if the input is in the armed or bypassed state due to a time zone or a manual command.
3. Outputs in system shall have two icon representations, one for the secure (locked) state and one for the open (unlocked) state.
4. Icons displaying status of the I/O points shall be constantly updated to show their current real-time condition without prompting by the operator.
5. The operator shall be able to scroll the list of I/Os and press the appropriate toolbar button, or right click, to command the system to perform the desired function.
6. Graphic maps or drawings containing inputs, outputs, and override groups shall include the following:

a. Database to import and store full-color maps or drawings and allow for input, output, and override group icons to be placed on maps.
b. Maps to provide real-time display animation and allow for control of points assigned to them.
c. System to allow inputs, outputs, and override groups to be placed on different maps.
d. Software to allow changing the order or priority in which maps will be displayed.

7. Override Groups Containing I/Os:

a. System shall incorporate override groups that provide the operator with the status and control over user-defined "sets" of I/Os with a single icon.
b. Icon shall change automatically to show the live summary status of points in that group.
c. Override group icon shall provide a method to manually control or set to time zone points in the group.
d. Override group icon shall allow the expanding of the group to show icons representing the live status for each point in the group, individual control over each point, and the ability to compress the individual icons back into one summary icon.

8. Schedule Overrides of I/Os and Override Groups:

a. To accommodate temporary schedule changes that do not fall within the holiday parameters, the operator shall have the ability to override schedules individually for each input, output, or override group.
b. Each schedule shall be composed of a minimum of two dates with separate times for each date.
c. The first time and date shall be assigned the override state that the point shall advance to, when the time and date become current.
d. The second time and date shall be assigned the state that the point shall return to, when the time and date become current.

9. Copy command in database shall allow for like data to be copied and then edited for specific requirements, to reduce redundant data entry.

I. Operator Access Control:

1. Control operator access to system controls through three to five password-protected operator levels. System operators and managers with appropriate password clearances shall be able to change operator levels for operators.
2. Three successive attempts by an operator to execute functions beyond their defined level during a 24-hour period shall initiate a software tamper alarm.
3. A minimum of 32-bit passwords shall be available with the system software. System shall display the operator's name or initials in the console's first field. System shall print the operator's name or initials, action, date, and time on the system printer at login and logoff.
4. The password shall not be displayed or printed.
5. Each password shall be definable and assignable for the following:

a. Commands usable.
b. Access to system software.

c. Access to application software.
d. Individual zones that are to be accessed.
e. Access to database.

J. Operator Commands:

1. Command Input: Plain-language words and acronyms shall allow operators to use the system without extensive training or data-processing backgrounds. System prompts shall be a word, a phrase, or an acronym.
2. Command inputs shall be acknowledged and processing shall start in not less than 4 second(s).
3. Tasks that are executed by operator's commands shall include the following:

a. Acknowledge Alarms: Used to acknowledge that the operator has observed the alarm message.
b. Place Zone in Access: Used to remotely disable intrusion alarm circuits emanating from a specific zone. System shall be structured so that console operator cannot disable tamper circuits.
c. Place Zone in Secure: Used to remotely activate intrusion alarm circuits emanating from a specific zone.
d. System Test: Allows the operator to initiate a system-wide operational test.
e. Zone Test: Allows the operator to initiate an operational test for a specific zone.
f. Print reports.
g. Change Operator: Used for changing operators.
h. Run system tests.
i. Generate and format reports.
j. Request help with the system operation.

1) Include in main menus.
2) Provide unique, descriptive, context-sensitive help for selections and functions with the press of one function key.
3) Provide navigation to specific topic from within the first help window.
4) Help shall be accessible outside the applications program.

k. Entry-Control Commands:

1) Lock (secure) or unlock (open) each controlled entry and exit up to four times a day through time-zone programming.
2) Arm or disarm each monitored input up to four times a day through time-zone programming.
3) Enable or disable readers or keypads up to twice a day through time-zone programming.
4) Enable or disable cards or codes up to four times per day per entry point through access-level programming.

4. Command Input Errors: Show operator input assistance when a command cannot be executed because of operator input errors. Assistance screen shall use plain-language words and phrases to explain why the command cannot be executed. Error responses that require an operator to look up a code in a manual or other document are not acceptable. Conditions causing operator assistance messages include the following:

a. Command entered is incorrect or incomplete.
b. Operator is restricted from using that command.
c. Command addresses a point that is disabled or out of service.
d. Command addresses a point that does not exist.
e. Command is outside the system's capacity.

K. Alarms:

1. System Setup:

a. Assign manual and automatic responses to incoming point status change or alarms.
b. Automatically respond to input with a link to other inputs, outputs, operator-response plans, unique sound with use of WAV files, and maps or images that graphically represent the point location.
c. 60-character message field for each alarm.
d. Operator-response-action messages shall allow message length of at least 65,000 characters, with database storage capacity of up to 32,000 messages.
e. Secondary messages shall be assignable by the operator for printing to provide further information and shall be editable by the operator.
f. Allow 25 secondary messages with a field of 4 lines of 60 characters each.
g. Store the most recent 1000 alarms for recall by the operator using the report generator.

2. Software Tamper:

a. Annunciate a tamper alarm when unauthorized changes to system database files are attempted. Three consecutive unsuccessful attempts to log onto system shall generate a software tamper alarm.
b. Annunciate a software tamper alarm when an operator or other individual makes three consecutive unsuccessful attempts to invoke functions beyond their authorization level.
c. Maintain a transcript file of the last 5000 commands entered at the each Central Station to serve as an audit trail. System shall not allow write access to system transcript files by any person, regardless of their authorization level.
d. Allow only acknowledgment of software tamper alarms.

3. Read access to system transcript files shall be reserved for operators with the highest password authorization level available in system.
4. Animated Response Graphics: Highlight alarms with flashing icons on graphic maps; display and constantly update the current status of alarm inputs and outputs in real time through animated icons.
5. Alarm Handling: Each input may be configured so that an alarm cannot be cleared unless it has returned to normal, with options of requiring the operator to enter a comment about disposition of alarm. Allow operator to silence alarm sound when alarm is acknowledged.

L. Alarm Monitoring: Monitor sensors, Controllers, and DTS circuits and notify operators of an alarm condition. Display higher-priority alarms first and, within alarm priorities, display the oldest unacknowledged alarm first. Operator acknowledgment of one alarm shall not be considered acknowledgment of other alarms nor shall it inhibit reporting of subsequent alarms.

1. Displayed alarm data shall include type of alarm, location of alarm, and secondary alarm messages.
2. Printed alarm data shall include type of alarm, location of alarm, date and time (to nearest second) of occurrence, and operator responses.
3. Maps shall automatically display the alarm condition for each input assigned to that map, if that option is selected for that input location.
4. Alarms initiate a status of "pending" and require the following two handling steps by operators:

    a. First Operator Step: "Acknowledged." This action shall silence sounds associated with the alarm. The alarm remains in the system "Acknowledged" but "Un-Resolved."
    b. Second Operator Step: Operators enter the resolution or operator comment, giving the disposition of the alarm event. The alarm shall then clear.

5. Each alarm point shall be programmable to disallow the resolution of alarms until the alarm point has returned to its normal state.
6. Alarms shall transmit to Central Station in real time, except for allowing connection time for dial-up locations.
7. Alarms shall be displayed and managed from a minimum of four different windows.

    a. Input Status Window: Overlay status icon with a large red blinking icon. Selecting the icon will acknowledge the alarm.
    b. History Log Transaction Window: Display name, time, and date in red text. Selecting red text will acknowledge the alarm.
    c. Alarm Log Transaction Window: Display name, time, and date in red. Selecting red text will acknowledge the alarm.
    d. Graphic Map Display: Display a steady colored icon representing each alarm input location. Change icon to flashing red when the alarm occurs. Change icon from flashing red to steady red when the alarm is acknowledged.

8. Once an alarm is acknowledged, the operator shall be prompted to enter comments about the nature of the alarm and actions taken. Operator's comments may be manually entered or selected from a programmed predefined list, or a combination of both.
9. For locations where there are regular alarm occurrences, provide programmed comments. Selecting that comment shall clear the alarm.
10. The time and name of the operator who acknowledged and resolved the alarm shall be recorded in the database.
11. Identical alarms from same alarm point shall be acknowledged at same time the operator acknowledges the first alarm. Identical alarms shall be resolved when the first alarm is resolved.
12. Alarm functions shall have priority over downloading, retrieving, and updating database from Controllers.
13. When a reader-controlled output (relay) is opened, the corresponding alarm point shall be automatically bypassed.

M. System test software enables operators to initiate a test of the entire system or of a particular portion of the system.

1. Test Report: The results of each test shall be stored for future display or printout. The report shall document the operational status of system components.

N. Report Generator Software: Include commands to generate reports for displaying, printing, and storing on disk and tape. Reports shall be stored by type, date, and time. Report printing shall be the lowest priority activity. Report generation mode shall be operator selectable but set up initially as periodic, automatic, or on request. Include time and date printed and the name of operator generating the report. Report formats may be configured by operators.

1. Automatic Printing: Setup shall specify, modify, or inhibit the report to be generated; the time the initial report is to be generated; the time interval between reports; the end of period; and the default printer.
2. Printing on Requests: An operator may request a printout of any report.
3. Alarm Reports: Reporting shall be automatic as initially set up. Include alarms recorded by system over the selected time and information about the type of alarm, the type of sensor, the location, the time, and the action taken.
4. Access and Secure Reports: Document zones placed in access, the time placed in access, and the time placed in secure mode.
5. Custom Reports: Reports tailored to exact requirements of who, what, when, and where. As an option, custom report formats may be stored for future printing.
6. Automatic History Reports: Named, saved, and scheduled for automatic generation.
7. Cardholder Reports: Include data, or selected parts of the data, as well as the ability to be sorted by name, card number, imprinted number, or by any of the user-defined fields.
8. Cardholder by Reader Reports: Based on who has access to a specific reader or group of readers by selecting the readers from a list.
9. Cardholder by Access-Level Reports: Display everyone that has been assigned to the specified access level.
10. Panel Labels Reports: Printout of control-panel field documentation including the actual location of equipment, programming parameters, and wiring identification. Maintain system installation data within system database so that they are available on-site at all times.
11. History Reports: Custom reports that allows the operator to select any date, time, event type, device, output, input, operator, Location, name, or cardholder to be included or excluded from the report.

    a. Initially store history on the hard disk of the host PC.
    b. Print history to any system printer.
    c. The report shall be definable by a range of dates and times with the ability to have a daily start and stop time over a given date range.
    d. Each report shall depict the date, time, event type, event description, device, or I/O name, cardholder group assignment, and cardholder name or code number.
    e. Each line of a printed report shall be numbered to ensure that the integrity of the report has not been compromised.
    f. Total number of lines of the report shall be given at the end of the report. If the report is run for a single event such as "Alarms," the total shall reflect how many alarms occurred during that period.

12. Reports shall have the following four options:

    a. View on screen.
    b. Print to system printer. Include automatic print spooling and "Print To" options if more than one printer is connected to system.
    c. "Save to File" with full path statement.

d. System shall have the ability to produce a report indicating status of system inputs and outputs or of inputs and outputs that are abnormal, out of time zone, manually overridden, not reporting, or in alarm.

13. Custom Code List Subroutine: Allow the access codes of system to be sorted and printed according to the following criteria:

    a. Active, inactive, or future activate or deactivate.
    b. Code number, name, or imprinted card number.
    c. Group, Location, access levels.
    d. Start and stop code range.
    e. Codes that have not been used since a selectable number of days.
    f. In, out, or either status.
    g. Codes with trace designation.
    h. Vendor shall provide 300 each proximity cards and 20 each system compatible proximity key ring tags or fobs.

14. The reports of system database shall allow options so that every data field may be printed.
15. The reports of system database shall be constructed so that the actual position of the printed data shall closely match the position of the data on the data-entry windows.

O. Anti-Passback:

1. System shall have global and local anti-passback features, selectable by Location. System shall support hard and soft anti-passback.
2. Hard Anti-Passback: Once a credential holder is granted access through a reader with one type of designation (IN or OUT), the credential holder may not pass through that type of reader designation until the credential holder passes though a reader of opposite designation.
3. Soft Anti-Passback: Should a violation of the proper IN or OUT sequence occur, access shall be granted, but a unique alarm shall be transmitted to the control station, reporting the credential holder and the door involved in the violation. A separate report may be run on this event.
4. Timed Anti-Passback: A Controller capability that prevents an access code from being used twice at the same device (door) within a user-defined amount of time.
5. Provide four separate zones per Location that can operate without requiring interaction with the host PC (done at Controller). Each reader shall be assignable to one or all four anti-passback zones. In addition, each anti-passback reader can be further designated as "Hard," "Soft," or "Timed" in each of the four anti-passback zones. The four anti-passback zones shall operate independently.
6. The anti-passback schemes shall be definable for each individual door.
7. The Master Access Level shall override anti-passback.
8. System shall have the ability to forgive (or reset) an individual credential holder or the entire credential holder population anti-passback status to a neutral status.

P. Visitor Assignment:

1. Provide for and allow an operator to be restricted to only working with visitors. The visitor badging subsystem shall assign credentials and enroll visitors. Allow only access levels that have been designated as approved for visitors.
2. Provide an automated log of visitor name, time and doors accessed, and whom visitor contacted.
3. Allow a visitor designation to be assigned to a credential holder.
4. Security access system shall be able to restrict the access levels that may be assigned to credentials that are issued to visitors.
5. Allow operator to recall visitors' credential holder file, once a visitor is enrolled in the system.
6. The operator may designate any reader as one that deactivates the credential after use at that reader. The history log shall show the return of the credential.
7. System shall have the ability to use the visitor designation in searches and reports. Reports shall be able to print all or any visitor activity.

Q. Entry-Control Enrollment Software: Database management functions that allow operators to add, delete, and modify access data as needed.

1. The enrollment station shall not have alarm response or acknowledgment functions.
2. Provide multiple, password-protected access levels. Database management and modification functions shall require a higher operator access level than personnel enrollment functions.
3. The program shall provide means to disable the enrollment station when it is unattended to prevent unauthorized use.
4. The program shall provide a method to enter personnel identifying information into the entry-control database files through enrollment stations. Allow entry of personnel identifying information into the system database using menu selections and data fields. The data field names shall be customized during setup to suit user and site needs.
5. Cardholder Data: Provide 99 user-defined fields. System shall have the ability to run searches and reports using any combination of these fields. Each user-defined field shall be configurable, using any combination of the following features:

    a. MASK: Determines a specific format that data must comply with.
    b. REQUIRED: Operator is required to enter data into field before saving.
    c. UNIQUE: Data entered must be unique.
    d. DEACTIVATE DATE: Data entered will be evaluated as an additional deactivate date for all cards assigned to this cardholder.
    e. NAME ID: Data entered will be considered a unique ID for the cardholder.

6. Personnel Search Engine: A report generator with capabilities such as search by last name, first name, group, or any predetermined user-defined data field; by codes not used in definable number of days; by skills; or by seven other methods.
7. Multiple Deactivate Dates for Cards: User-defined fields to be configured as additional stop dates to deactivate any cards assigned to the cardholder.
8. Batch card printing.
9. Default card data can be programmed to speed data entry for sites where most card data are similar.
10. Enhanced ACSII File Import Utility: Allows the importing of cardholder data and images.
11. Card Expire Function: Allows readers to be configured to deactivate cards when a card is used at selected devices.

2.5 SYSTEM DATABASE

A. Database and database management software shall define and modify each point in database using operator commands. Definition shall include parameters and constraints associated with each system device.

B. Database Operations:

1. System data management shall be in a hierarchical menu tree format, with navigation through expandable menu branches and manipulated with use of menus and icons in a main menu and system toolbar.
2. Navigational Aids:

    a. Toolbar icons for add, delete, copy, print, capture image, activate, deactivate, and muster report.
    b. Point and click feature to facilitate data manipulation.
    c. Next and previous command buttons visible when editing database fields to facilitate navigation from one record to the next.
    d. Copy command and copy tool in the toolbar to copy data from one record to create a new similar record.

3. All data entry shall be automatically checked for duplicate and illegal data and shall verify that data are in a valid format.
4. Provide a memo or note field for each item that is stored in database, allowing the storing of information about any defining characteristics of the item. Memo field is used for noting the purpose the item was entered for, reasons for changes that were made, and the like.

C. File Management:

1. Provide database backup and restoration system, allowing selection of storage media, including 3.5-inch floppy disk, Zip and Jaz drives, and designated network resources.
2. Provide manual and automatic mode of backup operations. The number of automatic sequential backups before the oldest backup becomes overwritten; FIFO mode shall be operator selectable.
3. Backup program shall provide manual operation from any PC on the LAN and shall operate while system remains operational.

D. Operator Passwords:

1. Software shall support up to 32,000 individual system operators, each with a unique password.
2. Operator Password: One to Eight characters.
3. Allow passwords to be case sensitive.
4. Passwords shall not be displayed when entered.
5. Provide each password with a unique and customizable password profile, and allow several operators to share a password profile. Include the following features in the password profile:
    a. Predetermine the highest-level password profile for access to all functions and areas of program.

b. Allow or disallow operator access to any program operation, including the functions of View, Add, Edit, and Delete.
c. Restrict which doors an operator can assign access to.

6. Operators shall use a user name and password to log on to system.

   a. This user name and password is used to access database areas and programs as determined by the associated profile.

7. Make provision to allow the operator to log off without fully exiting program. User may be logged off but program will remain running while displaying the login window for the next operator.

E. Access Card/Code Operation and Management: Access authorization shall be by card, by a manually entered code (PIN), or by a combination of both (card plus PIN).

1. Access authorization shall verify the facility code first, the card or card-and-PIN validation second, and the access level (time of day, day of week, date), anti-passback status, and number of uses last.
2. Use data-entry windows to view, edit, and issue access levels. Access authorization entry management system shall maintain and coordinate all access levels to prevent duplication or the incorrect creation of levels.
3. Allow assignment of multiple cards/codes to a cardholder.
4. Allow assignment of up to four access levels for each Location to a cardholder. Each access level may contain any combination of doors.
5. Each door may be assigned four time zones.
6. Access codes may be up to 11 digits in length.
7. Software shall allow the grouping of locations so cardholder data can be shared by all locations in the group.
8. Visitor Access: Issue a visitor badge, without assigning that person a card or code, for data tracking or photo ID purposes.
9. Cardholder Tracing: Allow for selection of cardholder for tracing. Make a special audible and visual annunciation at control station when a selected card or code is used at a designated code reader. Annunciation shall include an automatic display of the cardholder image.
10. Allow each cardholder to be given either an unlimited number of uses or a number from 1 to 9998 that regulates the number of times the card can be used before it is automatically deactivated.
11. Provide for cards and codes to be activated and deactivated manually or automatically by date. Provide for multiple deactivate dates to be preprogrammed.

F. Security Access Integration:

1. Photo ID badging and photo verification shall use same database as the security access and may query data from cardholder, group, and other personal information to build a custom ID badge.
2. Automatic or manual image recall and manual access based on photo verification shall also be a means of access verification and entry.
3. System shall allow sorting of cardholders together by group or other characteristic for a fast and efficient method of reporting on, and enabling or disabling, cards or codes.

G. Operator Comments:

1. With the press of one appropriate button on toolbar, the user shall be permitted to make operator comments into history at anytime.
2. Automatic prompting of operator comment shall occur before the resolution of each alarm.
3. Operator comments shall be recorded by time, date, and operator number.
4. Comments shall be sorted and viewed through reports and history.
5. The operator may enter comments in two ways; either or both may be used:

    a. Manually entered through keyboard data entry (typed), up to 65,000 characters per each alarm.
    b. Predefined and stored in database for retrieval on request.

6. System shall have a minimum of 999 predefined operator comments with up to 30 characters per comment.

H. Group:

1. Group names may be used to sort cardholders into groups that allow the operator to determine the tenant, vendor, contractor, department, division, or any other designation of a group to which the person belongs.
2. System software shall have the capacity to assign 1 of 32,000 group names to an access authorization.
3. Make provision in software to deactivate and reactivate all access authorizations assigned to a particular group.
4. Allow sorting of history reports and code list printouts by group name.

I. Time Zones:

1. Each zone consists of a start and stop time for 7 days of the week and three holiday schedules. A time zone is assigned to inputs, outputs, or access levels to determine when an input shall automatically arm or disarm, when an output automatically opens or secures, or when access authorization assigned to an access level will be denied or granted.
2. Up to four time zones may be assigned to inputs and outputs to allow up to four arm or disarm periods per day or four lock or unlock periods per day; up to three holiday override schedules may be assigned to a time zone.
3. Data-entry window shall display a dynamically linked bar graph showing active and inactive times for each day and holiday, as start and stop times are entered or edited.

J. Holidays:

1. Three different holiday schedules may be assigned to a time zone. Holiday schedule consists of date in format MM/DD/YYYY and a description. When the holiday date matches the current date of the time zone, the holiday schedule replaces the time zone schedule for that 24-hour period.
2. System shall have the capacity for Unlimited holidays.
3. Three separate holiday schedules may be applied to a time zone.
4. Holidays have an option to be designated as occurring on the designated date each year. These holidays remain in system and will not be purged.

5. Holidays not designated to occur each year shall be automatically purged from database after the date expires.

K. Access Levels:
1. One level shall be predefined as the Master Access Level. The Master Access Level shall work at all doors at all times and override any anti-passback.
2. System shall allow for access to be restricted to any area by reader and by time. Access levels shall determine when and where an Identifier is authorized.
3. System shall be able to create multiple door and time zone combinations under same access level so that an Identifier may be valid during different time periods at different readers even if the readers are on the same Controller.

L. User-Defined Fields:

1. System shall provide a minimum of 99 user-defined fields, each with up to 50 characters, for specific information about each credential holder.
2. System shall accommodate a title for each field; field length shall be 20 characters.
3. A "Required" option may be applied to each user-defined field that, when selected, forces the operator to enter data in the user-defined field before the credential can be saved.
4. A "Unique" option may be applied to each user-defined field that, when selected, will not allow duplicate data from different credential holders to be entered.
5. Data format option may be assigned to each user-defined field that will require the data to be entered with certain character types in specific spots in the field entry window.
6. A user-defined field, if selected, will define the field as a deactivate date. The selection shall automatically cause the data to be formatted with the windows MM/DD/YYYY date format. The credential of the holder will be deactivated on that date.
7. A search function shall allow any one user-defined field or combination of user-defined fields to be searched to find the appropriate cardholder. The search function shall include search for a character string.
8. System shall have the ability to print cardholders based on and organized by the user-defined fields.

2.6 SURGE AND TAMPER PROTECTION

A. Surge Protection: Protect components from voltage surges originating external to equipment housing and entering through power, communication, signal, control, or sensing leads. Include surge protection for external wiring of each conductor-entry connection to components.

1. Minimum Protection for Power Connections 120 V and More: Auxiliary panel suppressors complying with requirements in Division 16 Section "Transient Voltage Suppression."
2. Minimum Protection for Communication, Signal, Control, and Low-Voltage Power Connections: Comply with requirements in Division 16 Section "Transient Voltage Suppression" as recommended by manufacturer for type of line being protected.

B. Tamper Protection: Tamper switches on enclosures, control units, pull boxes, junction boxes, cabinets, and other system components shall initiate a tamper-alarm signal when unit is opened or partially disassembled. Control-station control-unit alarm display shall identify tamper alarms and indicate locations.

2.7 CENTRAL-STATION HARDWARE

A. PC-based Central Station and Fujitsu Life Book U810 Mini-Notebook shall be provided by vendor.

B. Central-Station Computer: Standard unmodified PC of modular design. The CPU operating speed shall be at least 2.8 GHz.

1. Memory: 256 MB of usable installed memory, expandable to a minimum of 1024 MB without additional chassis or power supplies.
2. Power Supply: Minimum capacity of 350W.
3. Real-Time Clock shall be accurate to plus or minus 1 minute per month.
4. Parallel Port: An enhanced parallel port.
5. LAN Adapter Card: 10/100 Mbps PCI bus, internal network interface card.
6. Sound Card: For playback and recording of digital WAV sound files that are associated with audible warning and alarm functions.
7. Color Monitor: Not less than 17", with a minimum resolution of 1024x768 pixels, and a maximum dot pitch of 0.28 mm. The video card shall support at least 32 million colors at a resolution of 1280x1024 at a minimum refresh rate of 60 Hz.
8. Keyboard: With a minimum of 64 characters, standard ASCII character set based on ANSI X3.154.
9. Mouse: Standard, compatible with the installed software.
10. Special function keyboard attachments or special function keys to facilitate data input of the following operator tasks:

    a. Help.
    b. Alarm Acknowledge.
    c. Place Zone in Access.
    d. Place Zone in Secure.
    e. System Test.
    f. Print Reports.
    g. Change Operator.

11. Disk storage shall include the following, each with appropriate controller:

    a. Minimum 60 GB hard disk.
    b. Floppy Disk Drive: High density, 3-1/2-inch (90-mm) size.

12. CD-ROM Drive:

13. Interface: Bidirectional parallel and universal serial bus.
14. LAN Adapter Card: 10/100 Mbps internal network interface card.

C. UPS: Self-contained; complying with requirements in Division 16 Section "Static Uninterruptible Power Supply."

1. Size: Provide a minimum of 8 hours of operation of the central-station equipment, including 2 hours of alarm printer operation.
2. Batteries: Sealed, valve regulated, recombinant, lead calcium.
3. Accessories:

a. Transient voltage suppression.
b. Input-harmonics reduction.
c. Rectifier/charger.
d. Battery disconnect device.
e. Static bypass transfer switch.
f. Internal maintenance bypass/isolation switch.
g. External maintenance bypass/isolation switch.
h. Output isolation transformer.
i. Remote UPS monitoring.
j. Battery monitoring.
k. Remote battery monitoring.
l. <Insert accessories.>

D. Fujitsu Life Book U810 Mini-Notebook
a. A110 / 800 MHz
b. Ultra Mobile 2007
c. RAM 1 GB
d. HDD 40 GB
e. WLAN : 802.11 Super AG, 802.11a/b/g, Bluetooth 2.0
f. TPM - fingerprint reader
g. 5.6" Widescreen TFT 1024 x 600 (WSVGA) - camera)
h. Windows XP / Microsoft Office 2007 Professional

2.8 CONTROLLERS

A. Controllers: Intelligent peripheral control unit, complying with UL 294, that stores time, date, valid codes, access levels, and similar data downloaded from the Central Station for controlling its operation.

B. Subject to compliance with requirements in this Article, manufacturers may use multipurpose Controllers.

C. Battery Backup: Sealed lead acid; sized to provide run time during a power outage of 90 minutes complying with UL924.

D. Alarm Annunciation Controller:

1. The Controller shall automatically restore communication within 10 seconds after an interruption with the field device network..

a. Inputs: Monitor dry contacts for changes of state that reflect alarm conditions. Provides at least eight alarm inputs, which are suitable for wiring as normally open or normally closed contacts for alarm conditions.

b. Outputs: Managed by Central Station software.

2. Auxiliary Equipment Power: A GFI service outlet inside the Controller enclosure.

E. Entry-Control Controller:

1. Function: Provide local entry-control functions including one- and two-way communications with access-control devices such as card readers, keypads, biometric personal identity verification devices, door strikes, magnetic latches, gate and door operators, and exit push-buttons.

    a. Operate as a stand-alone portal Controller using the downloaded database during periods of communication loss between the Controller and the field-device network.
    b. Accept information generated by the entry-control devices; automatically process this information to determine valid identification of the individual present at the portal:

        1) On authentication of the credentials or information presented, check privileges of the identified individual, allowing only those actions granted as privileges.
        2) Privileges shall include, but not be limited to, time of day control, day of week control, group control, and visitor escort control.

    c. Maintain a date-, time-, and Location-stamped record of each transaction. A transaction is defined as any successful or unsuccessful attempt to gain access through a controlled portal by the presentation of credentials or other identifying information.

2. Inputs:

    a. Data from entry-control devices; use this input to change modes between access and secure.
    b. Database downloads and updates from the Central Station that include enrollment and privilege information.

3. Outputs:

    a. Indicate success or failure of attempts to use entry-control devices and make comparisons of presented information with stored identification information.
    b. Maintain a date, time, and location stamped record of each transaction and transmit transaction records to the Central Station.
    c. Door Prop Alarm: If a portal is held open for longer than 20 seconds, alarm sounds.

4. With power supplies sufficient to power at voltage and frequency required for field devices and portal-control devices.
5. Data Line Problems: For periods of loss of communications with Central Station, or when data transmission is degraded and generating continuous checksum errors, the Controller shall continue to control entry by accepting identifying information, making authentication decisions, checking privileges, and controlling portal-control devices.

    a. Store up to 10,000 transactions during periods of communication loss between the Controller and access-control devices for subsequent upload to the Central Station on restoration of communication.

6. Controller Power: NFPA 70, Class II power supply transformer, with 12- or 24-V ac secondary, backup battery and charger.
   a. Backup Battery: Valve-regulated, recombinant-sealed, lead-acid battery; spill proof. With single-stage, constant-voltage-current, limited battery charger, comply with battery manufacturer's written instructions for battery terminal voltage and charging current recommendations for maximum battery life.
   b. Backup Power Supply Capacity: 90 minutes of battery supply. Submit battery and charger calculations.
   c. Power Monitoring: Provide manual dynamic battery load test, initiated and monitored at the control center; with automatic disconnection of the Controller when battery voltage drops below Controller limits. Report by using local Controller-mounted LEDs and by communicating status to Central Station. Indicate normal power on and battery charger on trickle charge. Indicate and report the following:

      1) Trouble Alarm: Normal power off load assumed by battery.
      2) Trouble Alarm: Low battery.
      3) Alarm: Power off.

2.9 KEYPADS

A. Designed for use with unique combinations of alphanumeric and other symbols as an Identifier. Keys of keypads shall contain an integral alphanumeric/special symbol keyboard with symbols arranged in ascending ASCII-code ordinal sequences.

B. Communications protocol shall be compatible with Controller.

1. Keypad display or enclosure shall limit viewing angles of the keypad as follows:

   a. Maximum Horizontal Viewing Angle: 5 degrees or less off in either direction of a vertical plane perpendicular to the plane of the face of the keypad display.
   b. Maximum Vertical Viewing Angle: 15 degrees or less off in either direction of a horizontal plane perpendicular to the plane of the face of the keypad display.

2. Duress Codes: Provide duress situation indication by entering a special code.

2.10 CARD READERS

A. Power: Card reader shall be powered from its associated Controller, including its standby power source.

B. Response Time: Card reader shall respond to passage requests by generating a signal that is sent to the Controller. Response time shall be 800 ms or less, from the time the card reader finishes reading the credential card until a response signal is generated.

C. Enclosure: Suitable for semi flush. Mounting types shall additionally be suitable for installation in the following locations:

1. Indoors, controlled environment.

2. Indoors, uncontrolled environment.
3. Outdoors, with built-in heaters or other cold-weather equipment to extend the operating temperature range as needed for operation at the site.

D. Display: LED or other type of visual indicator display shall provide visual status indications and user prompts. Indicate power on/off, whether user passage requests have been accepted or rejected, and whether the door is locked or unlocked.

E. Touch Plate and Proximity Readers:

1. Active detection proximity card readers shall provide power to compatible credential cards through magnetic induction, and shall receive and decode a unique identification code number transmitted from the credential card.
2. Passive detection proximity card readers shall use a swept-frequency, RF field generator to read the resonant frequencies of tuned circuits laminated into compatible credential cards. The resonant frequencies read shall constitute a unique identification code number.
3. The card reader shall read proximity cards in a range from contact with to at least 4 inches from the reader.

F. Keypad and Wiegand Swipe

2.11 DOOR AND GATE HARDWARE INTERFACE

A. Exit Device with Alarm: Operation of the exit device shall generate an alarm Exit device and alarm contacts are specified in Division 8 Section "Door Hardware."

B. Exit Alarm: Operation of a monitored door shall generate an alarm. Exit devices and alarm contacts are specified in Division 8 Section "Door Hardware."

C. Electric Door Strikes: Use end-of-line resistors to provide power line supervision. Signal switches shall transmit data to Controller to indicate when the bolt is not engaged and the strike mechanism is unlocked, and shall report a forced entry. Power and signal shall be from the Controller. Electric strikes are specified in Division 8 "Door Hardware."

D. Electromagnetic Locks: End-of-line resistors shall provide power line supervision. Lock status sensing signal shall positively indicate door is secure. Power and signal shall be from the Controller. Electromagnetic locks are specified in Division 8 Section "Door Hardware."

E. Vehicle Gate Operator: Interface electrical operation of gate with controls of this Section. Vehicle gate operators shall be connected, monitored, and controlled, by the security access Controllers. Vehicle gate and accessories are specified in Division 2 Section "Chain-Link Fences and Gates."

2.12 TRANSFORMERS

A. NFPA 70, Class II control transformers, NRTL listed. Transformers for security access-control system shall not be shared with any other system.

2.13 CABLE AND ASSET MANAGEMENT

A. Manufacturers:

1. IMAP Textron; Division of Greenlee Textron.
2. Total Wire Software Company, Inc.
3. West Penn Wire, Inc.

B. Computer-based cable and asset management system, with fully integrated database and graphic capabilities, complying with requirements in TIA/EIA-606.

1. Document physical characteristics by recording the network, asset, user, TIA/EAI details, device configurations, and exact connections between equipment and cabling.

a. Manage the physical layer of security system.
b. List device configurations.
c. List and display circuit connections.
d. Record firestopping data.
e. Record grounding and bonding connections and test data.

2. Information shall be presented in database view, schematic plans, or technical drawings.

a. AutoCad Technical Drawing shall be used as drawing and schematic plans software. Drawing symbols, system layout, and design shall comply with SIA AG-01.

3. System shall interface with the following testing and recording devices:

a. Direct upload tests from circuit testing instrument into the PC.
b. Direct download circuit labeling into labeling printer.

C. Software shall be designed for Microsoft Windows of same version as security access system's Central Station shall be installed on the designated PC, using a hard drive dedicated only to this management function. Hard-drive capacity shall be not less than 60 GB.

PART 3 - EXECUTION

3.1 PREPARATION

A. Comply with recommendations in SIA CP-01.

B. Comply with EIA/TIA-606, "Administration Standard for the Telecommunications Infrastructure of Commercial Buildings."

C. Obtain detailed Project planning forms from manufacturer of access-control system; develop custom forms to suit Project. Fill in all data available from Project plans and specifications and publish as Project planning documents for review and approval.

1. Record setup data for control station.
2. For each Location, record setup of Controller features and access requirements.

3. Propose start and stop times for time zones and holidays, and match up access levels for doors.
4. Set up groups, facility codes, linking, and list inputs and outputs for each Controller.
5. Assign action message names and compose messages.
6. Set up alarms. Establish interlocks between alarms, intruder detection, and video surveillance features.
7. Prepare and install alarm graphic maps.
8. Develop user-defined fields.
9. Develop screen layout formats.
10. Propose setups for guard tours and key control.
11. Discuss badge layout options; design badges.
12. Complete system diagnostics and operation verification.
13. Prepare a specific plan for system testing, startup, and demonstration.
14. Develop acceptance test concept and, on approval, develop specifics of the test.
15. Develop cable and asset management system details; input data from construction documents. Include system schematics and AutoCad drawings.

D. In meetings with Architect and Owner, present Project planning documents and review, adjust, and prepare final setup documents. Use final documents to set up system software.

3.2 CABLING

A. Comply with NECA 1, "Good Workmanship in Electrical Contracting."

B. Install cables and wiring according to requirements in Division 16 Section "Voice and Data Communication Cabling."

C. Wiring Method: Install wiring in raceway and cable tray except within consoles, cabinets, desks, and counters. Conceal raceway and wiring except in unfinished spaces.

D. Wiring Method: Install wiring in raceway and cable tray except within consoles, cabinets, desks, and counters and except in accessible ceiling spaces and in gypsum board partitions where unenclosed wiring method may be used. Use NRTL-listed plenum cable in environmental air spaces, including plenum ceilings. Conceal raceway and cables except in unfinished spaces.

E. Install LAN cables using techniques, practices, and methods that are consistent with Category 5E rating of components and that ensure Category 5E performance of completed and linked signal paths, end to end.

F. Install cables without damaging conductors, shield, or jacket.

G. Boxes and enclosures containing security system components or cabling, and which are easily accessible to employees or to the public, shall be provided with a lock. Boxes above ceiling level in occupied areas of the building shall not be considered to be accessible. Junction boxes and small device enclosures below ceiling level and easily accessible to employees or the public shall be covered with a suitable cover plate and secured with tamperproof screws.

H. Install end-of-line resistors at the field device location and not at the Controller or panel location.

3.3 CABLE APPLICATION

A. Comply with EIA/TIA-569, "Commercial Building Standard for Telecommunications Pathways and Spaces."

B. Cable application requirements are minimum requirements and shall be exceeded if recommended or required by manufacturer of system hardware.

C. RS-485 Cabling: Install at a maximum distance of 4000 feet.

D. Card Readers and Keypads:

1. Install number of conductor pairs recommended by manufacturer for the functions specified.
2. Unless manufacturer recommends larger conductors, install No. 22 AWG.
3. Install minimum No. 18 AWG shielded cable to readers and keypads that draw 50mA or more.

E. Install minimum No. 16 AWG cable from Controller to electrically powered locks. Do not exceed 250ft.

F. Install minimum No. 18 AWG ac power wire from transformer to Controller, with a maximum distance of 20ft.

3.4 GROUNDING

A. Comply with Division 16 Section "Grounding and Bonding."

B. Comply with IEEE 1100, "Power and Grounding Sensitive Electronic Equipment."

C. Ground cable shields, drain conductors, and equipment to eliminate shock hazard and to minimize ground loops, common-mode returns, noise pickup, cross talk, and other impairments.

D. Bond shields and drain conductors to ground at only one point in each circuit.

E. Signal Ground:

1. Terminal: Locate in each equipment room and wiring closet; isolate from power system and equipment grounding.
2. Bus: Mount on wall of main equipment room with standoff insulators.
3. Backbone Cable: Extend from signal ground bus to signal ground terminal in each equipment room and wiring closet.

3.5 INSTALLATION

A. Push Buttons: Where multiple push buttons are housed within a single switch enclosure, they shall be stacked vertically with each push-button switch labeled with text and symbols as required. Push-button switches shall be connected to the Controller associated with the portal to which they are applied, and shall operate the appropriate electric strike, electric bolt, or other facility release device.

B. Install card, fob, and biometric readers.

3.6 SYSTEM SOFTWARE

A. Develop, install, and test software and databases for the complete and proper operation of systems involved. Assign software license to Owner.

3.7 FIELD QUALITY CONTROL

A. Manufacturer's Field Service: Engage a factory-authorized service representative to inspect, test, and adjust field-assembled components and equipment installation, including connections, and to assist in field testing. Report results in writing.

B. Perform the following field tests and inspections and prepare test reports:

1. LAN Cable Procedures: Inspect for physical damage and test each conductor signal path for continuity and shorts. Use Class 2, bidirectional, Category 5 tester. Test for faulty connectors, splices, and terminations. Test according to TIA/EIA-568-1, "Commercial Building Telecommunications Cabling Standards - Part 1 General Requirements." Link performance for UTP cables must comply with minimum criteria in TIA/EIA-568-B.
2. Test each circuit and component of each system. Tests shall include, but are not limited to, measurements of power supply output under maximum load, signal loop resistance, and leakage to ground where applicable. System components with battery backup shall be operated on battery power for a period of not less than 10 percent of the calculated battery operating time. Provide special equipment and software if testing requires special or dedicated equipment.
3. Operational Test: After installation of cables and connectors, demonstrate product capability and compliance with requirements. Test each signal path for end-to-end performance from each end of all pairs installed. Remove temporary connections when tests have been satisfactorily completed.

STATE OF WEST VIRGINIA
Purchasing Division

PURCHASING AFFIDAVIT

VENDOR OWING A DEBT TO THE STATE:
West Virginia Code §5A-3-10a provides that: No contract or renewal of any contract may be awarded by the state or any of its political subdivisions to any vendor or prospective vendor when the vendor or prospective vendor or a related party to the vendor or prospective vendor is a debtor and the debt owed is an amount greater than one thousand dollars in the aggregate.

PUBLIC IMPROVEMENT CONTRACTS & DRUG-FREE WORKPLACE ACT:
West Virginia Code §21-1D-5 provides that: Any solicitation for a public improvement construction contract shall require each vendor that submits a bid for the work to submit at the same time an affidavit that the vendor has a written plan for a drug-free workplace policy in compliance with Article 1D, Chapter 21 of the West Virginia Code. A public improvement construction contract may not be awarded to a vendor who does not have a written plan for a drug-free workplace policy in compliance with Article 1D, Chapter 21 of the West Virginia Code and who has not submitted that plan to the appropriate contracting authority in timely fashion. For a vendor who is a subcontractor, compliance with Section 5, Article 1D, Chapter 21 of the West Virginia Code may take place before their work on the public improvement is begun.

ANTITRUST:
In submitting a bid to any agency for the state of West Virginia, the bidder offers and agrees that if the bid is accepted the bidder will convey, sell, assign or transfer to the state of West Virginia all rights, title and interest in and to all causes of action it may now or hereafter acquire under the antitrust laws of the United States and the state of West Virginia for price fixing and/or unreasonable restraints of trade relating to the particular commodities or services purchased or acquired by the state of West Virginia. Such assignment shall be made and become effective at the time the purchasing agency tenders the initial payment to the bidder.

I certify that this bid is made without prior understanding, agreement, or connection with any corporation, firm, limited liability company, partnership or person or entity submitting a bid for the same materials, supplies, equipment or services and is in all respects fair and without collusion or fraud. I further certify that I am authorized to sign the certification on behalf of the bidder or this bid.

LICENSING:
Vendors must be licensed and in good standing in accordance with any and all state and local laws and requirements by any state or local agency of West Virginia, including, but not limited to, the West Virginia Secretary of State's Office, the West Virginia Tax Department, West Virginia Insurance Commission, or any other state agencies or political subdivision. Furthermore, the vendor must provide all necessary releases to obtain information to enable the Director or spending unit to verify that the vendor is licensed and in good standing with the above entities.

CONFIDENTIALITY:
The vendor agrees that he or she will not disclose to anyone, directly or indirectly, any such personally identifiable information or other confidential information gained from the agency, unless the individual who is the subject of the information consents to the disclosure in writing or the disclosure is made pursuant to the agency's policies, procedures and rules. Vendors should visit **www.state.wv.us/admin/purchase/privacy** for the Notice of Agency Confidentiality Policies.

Under penalty of law for false swearing (West Virginia Code §61-5-3), it is hereby certified that the vendor acknowledges the information in this said affidavit and is in compliance with the requirements as stated.

Vendor's Name: _____

Authorized Signature: _____ Date: _____