SULLIVAN COUNTY PURCHASING

INVITATION TO BID (ITB)

#ACMS2020(KD)

ACCESS CONTROL MANAGEMENT SYSTEM

FOR: KETRON ELEMENTARY, EMMETT ELEMENTARY & SULLIVAN CENTRAL HIGH SCHOOL

Proposals to be received by 2:00 p.m., Eastern Time

SEPTEMBER 17, 2020

Pre-bid on September 8, 2020 @ 10:00 a.m.

Submit Proposals to:
Sullivan County
Purchasing Department
Suite 201
3411 Hwy 126
Blountville, TN 37617

SULLIVAN COUNTY PURCHASING DEPARTMENT
INVITATION TO BID (ITB)
#ACMS2020(KD)

Proposals Due By: September 17, 2020 @ 2:00 p.m.

Pre-bid: September 8, 2020 at 10:00 a.m. starting at Emmett Elementary

---

VENDOR INFORMATION

Company Name____

Address____

City______________________________________State___________________Zip___________

Contact Person & Title____
(Please Print)

Telephone Number_____________________________________Fax Number_______________

Email of Contact Person____

Authorized Signature____

Date of Signature____

1. **Purpose and Objective**

A. The Office of the Sullivan County Purchasing Agent will receive sealed bids for the Sullivan County Department of Education until **Thursday, September 17, 2020 @ 2:00 p.m**. for a Turnkey Solution to Provide all Materials, Equipment, Labor, etc., for the complete installation of an **Access Control Management System including card readers and door strikes. System to be (Lenel or equal) and must be compatible to Aiphone)** for the following schools, Ketron Elementary, Emmett Elementary & Sullivan Central High School.

B. A Pre-Bid Meeting is scheduled on **Tuesday, September 8, 2020 @ 10:00 a.m.** starting at Emmett Elementary, proceeding after to Central High School then to Ketron Elementary.

School Addresses:

Emmett Elementary, 753 Emmett Road, Bristol, TN 37620
Central High School, 131 Shipley Ferry Road, Blountville, TN 37617
Ketron Elementary, 3301 Bloomingdale Pike, Kingsport, TN 37660

2. **ITB Time Line**

Pre-bid Date…………………………………………………………………………..September 8, 2020

Deadline for questions to be submitted in writing to the
Purchasing Department………………………………………………September 11, 2020

Proposal Due Date……………………………………………………………………September 17, 2020

This timetable is for the information of submitting entities. These dates are subject to change. However, in no event shall the deadline for submission of the proposals be changed except by written modification from the Sullivan County Purchasing Department.

3. **General Information**

A. This ITB will be made available to all interested Bidders upon request. The Bidder is advised to read this ITB in its entirety. Failure to read and/or understand any portion of this ITB shall not be cause for waiver of any portion of this ITB.

B. The Bidder must offer a turnkey project, assuming full responsibility for providing a fully-functional system.

4. **Proposal Submittal**

A. All proposals must be submitted on forms supplied in the bid package and shall be subject to all requirements of the ITB and these instructions to Bidders.

B. ITB documents, including the Bid Guaranty, shall be submitted in a sealed envelope and bearing on the outside**, the name of the Bidder, his address and the name of the project for which the bid is submitted.**

If Bid price is over $25,000 the bidder's name, licensed number, classification of license, and date of expiration must be placed on the outside of the envelope containing the contractor's bid per T.C.A. §62-6-119. The bid envelope shall also bear a list of any major sub-contractors as follows, if any, and their respective Tennessee license numbers and expiration dates. (Mechanical, Plumbing, Electrical, Sprinkler, Masonry).

Contractor installation personnel shall be trained and certified by the Access Control manufacturer and have a valid, current certification and Registered VAR at the time of installation.

Contractor installation provider shall retain a business within One Hundred Fifty (150) miles within Project Address.

If the Bidder chooses to submit his bid by mail, the Bid envelope should be placed inside another envelope which bears the mailing address below. The outside of the mailing envelope should be clearly labeled "**ITB #ACMS2020(KD) Access Control Management System for Ketron Elementary, Emmett Elementary & Sullivan Central High School"**. In order to receive consideration, the sealed proposal must be delivered to the Office of the Sullivan County Purchasing Agent on or before the day/time indicated.

C. Proposals shall be addressed and delivered to:

Sullivan County Purchasing Agent
Attn: Kristinia Davis
3411 Highway 126
Blountville, TN 37617

D. Any proposal received after the time and date on the cover sheet will not be considered. It shall be the sole responsibility of the submitting entity to have the proposal delivered to the Sullivan County Purchasing Department on or before that date. Proposals that arrive late due to the fault of the United States Postal Service, United Parcel Service, DHL, FEDEX, any delivery/courier service, or any other carrier of any sort are still considered late and shall not be accepted by Sullivan County. Such proposals shall remain unopened and will be returned to the submitting entity upon request.

E. Sullivan County and/or the Department of Education will not be responsible for any costs incurred by the Bidder in preparing and submitting its response to this ITB.

F. By submission of a signed bid, the bidder certifies total compliance with Title VI and Title VII of the Civil Rights Act of 1964, as amended, and all regulations promulgated thereunder.

5. <u>**Interpretations or Addenda**</u>

A. Any inquiries or requests concerning interpretations, clarification or additional information pertaining to this proposal must be e-mailed to Kristinia Davis @ kris.davis@sullivancountytn.gov by 5:00 p.m. Eastern time on Friday, September 11,

2020. In no case will verbal communication override written communication or documentation. Every interpretation made to a bidder will be in form of an Addendum to the Documents. In addition, all Addenda will be e-mailed, faxed or mailed to each person holding bid documents, but it shall be the bidder's responsibility to make inquiry as to the Addenda issued. All such Addenda shall become part of the Contract and all bidders shall be bound by such Addenda, whether or not received by the bidder.

6. **Instructions to Bidder**

A. The Bidder is advised to read this ITB in its entirety. Failure to read and/or understand any portion of this ITB shall not be cause for waiver of any portion of this ITB.

B. Responders taking exception to any requirements set forth herein shall be specific in each regard documenting the Exception in a document titled "Exceptions". The Exceptions document will be considered as part of the overall proposal evaluation.

All proposals shall be submitted as follows:

- ITB (this document)
- Price Proposal
- Exceptions (includes alternate systems proposed)
- Brochures, pamphlets, etc.
- Warranty/Service
- Bid Bond
- Compliance Affidavits

7. **Withdrawal of Proposals**

A. Any submission of proposals may be withdrawn and/or resubmitted up until the date and time for opening of the bids. Any submission not so withdrawn shall, upon opening, constitute an irrevocable offer for a period of ninety (90) calendar days following the bid date.

8. **No Contact Policy**

A. From the period beginning on the date of the issuance of the ITB and ending on the date of the award of the contract, no candidates submitting in response to this ITB, nor any individuals, consultants, or affiliates of such candidates shall contact through any means or engage in any discussion regarding this ITB, the selection process, or contract award with any member of the School Board, County Commission, County Mayor, School Department, apart from the designated point of contact referenced above in regard to clarification requests. Any such contact may be grounds for the disqualification of the submittal. Proposals must include a notarized No Contact/No Advocacy Affidavit (to be found in the "Submission Forms" section of this document).

9. **Bid Guaranty**

A. Each bid must be accompanied by a Bidder's Bond, executed by the Bidder and Surety Company licensed to do business in the State of Tennessee, or a certified check, in the sum of **not less than five percent (5%)** of the amount of the bid made payable to Sullivan County Trustee, and including the consideration of additive alternates, if any. Certified checks will be deposited by Sullivan County and refunded within ten (10) days after opening of bids with the exception of the two (2) lowest bidders. The remaining bid bonds or refund checks will be returned promptly after the Owner and the accepted bidder have executed the contract or, if no award has been made within thirty (30) days after the bid opening date, upon demand of the bidder of his bid. The successful bidder, upon his failure or refusal to execute and deliver the contract and bonds required within ten (10) calendar days after he has received notice of the acceptance of his bid, shall forfeit to the Owner, as liquidated damages for such failure or refusal, the security deposited with his bid.

B. The successful bidder will be required to execute the **Performance and Payment Bonds in** the amount equal to **One Hundred Percent (100%) of** the Contract Price.

10. **Insurance**

10.1 The successful Contractor shall provide proof of and shall always during the term hereof, maintain valid and in-force insurance policies and with coverage limits as set forth below:

A. Worker's compensation and employer's liability insurance with statutory coverage limits for the protection of all of Contractor's employees, including, without limitation, executive, managerial and supervisory employees, whether or not engaged in the performance of the Work.

B. Such policies of insurance for each and every motor vehicle to be used by the Contractor in the performance of the Work (the "Motor Vehicles"), with such policies of insurance for Contractor's Motor Vehicles to include no less than $1,000,000 in liability coverage.

C. A policy of general liability insurance covering loss resulting from the Contractor's direct and indirect activities hereunder (including those activities of any of its subcontractors) and covering property damage and injury to any person (including death) which or who might be damaged or injured as a result of, in conjunction with, or arising out of Contractor's performance of the Work. Bodily Injury Liability coverage (including death) and Property Damage Liability coverage shall be a minimum of $1,000,000 per occurrence and $2,000,000 in the aggregate per jobsite, project or location. This coverage shall be primary and non-contributory.

D. Coverage requirements shall be evidenced by one or more certificates of insurance naming Owner as an additional insured, which certificates or policy endorsements shall provide that the policies represented thereby may not be (i) canceled, (ii) allowed to expire, or (iii) altered with respect to the substantial terms thereof except upon thirty (30) days prior written notice to Owner. For purposes of this paragraph, “substantial terms” shall be deemed to include, but shall not be limited to the coverage limits and deductible of the applicable policy.

11. **Primary Insurance and Waiver of Subrogation**

A. Contractor (and its insurers) shall be primarily liable for the defense and payment of any claims as a result of, in conjunction with, or arising out of the performance of the Work. Contractor waives any and all of its subrogation rights against Owner, and any and all of its insurers in any such claims.

12. **Patent**

A. The Contractor shall hold and save Sullivan County and Sullivan County Department of Education, its officers and employees, harmless from liability of any nature or kind, including costs and expenses, for, or on account of, any patented or unpatented invention, process, article, or appliance manufactured or sued in the performance of the Contract, including its use by Sullivan County Department of Education, unless otherwise specifically stipulated in the specifications.

13. **Terms and Conditions of Award- General**

A. The terms and conditions imposed herein shall govern in all cases, and conflicting terms and conditions submitted by the Bidder may constitute enough grounds for rejection of the proposal.

B. Sullivan County Department of Education reserves the right to (a) accept or reject any and/or all submissions of proposals; (b) to waive irregularities, informalities, any technicalities; and (c) to accept any alternative submission of proposals presented which, in its opinion, would best serve the interest of the school department. Sullivan County Department of Education shall be the sole judge of the proposals, and the resulting agreement that is in the best interest, and its decision shall be final. The School System also reserves the right to make such investigation as it deems necessary to determine the ability of any submitting entity to perform the work or service requested. Information the School system deems necessary to make this determination shall be provided by the submitting entity.

C. Sullivan County Department of Education may award a contract, based on proposals received without further discussion of such a proposal. Accordingly, each proposal should state the most favorable terms from a price, conformance of specification requirements and functionality standpoint, which the Bidder can submit.

D. Sullivan County Department of Education reserves the right to reject any and/or all proposal(s) and negotiate with any Bidder in order to secure the system which best meets the needs and objectives of the Department of Education and not merely the lowest price as indicated.

E. **All work and all inspections must be completed by December 1, 2020.** The successful Bidder agrees to adhere to proposed and contracted schedules. The Bidder, however, will not be liable or deemed to be in default for any delays or failure in performances resulting directly or indirectly from any cause or circumstances beyond the Bidder’s reasonable control.

14. **Evaluation Criteria**

A. The final review of Bidder's proposal will evaluate the hardware content, conformance to the specification requirements and based upon an analysis of the system offered to determine which proposal best meets the needs and objectives of Sullivan County Department of Education.

B. The ability of Bidder to meet or exceed the functional requirements of the Request for Proposal will be evaluated.

C. Confidence that Bidder will be able to carry out all installation plans in a timely and efficient manner will be evaluated.

15. **Introduction**

A. Bidders are encouraged to come to the pre-bid meeting, verify all existing items listed as specified, and be familiar with the working conditions, hazards, and local requirements involved. Submission of bids shall be deemed evidence of such visit. All proposers shall take these existing conditions into consideration before bidding.

B. All materials, unless otherwise specified, shall be new, free from any defects, and of the best quality of their respective kinds. All like materials used shall be of the same manufacture, model, and quality, unless otherwise specified.

C. Manufacturer's names are listed herein to establish a standard. **The products of other manufacturers will only be acceptable if approved by the Department of Education five (5) days prior to bid**. These products must be of equal or better quality than the features specified herein, will serve with equal efficiency and dependability, and satisfy the purpose for which the items specified were intended.

D. Awarded Contractor shall furnish all labor and material for installation including but not limited to all programming, training, Certifications and Fire Marshall's written approval of final work.

E. Contractor shall be responsible for building security at the end of each workday and keeping the job site orderly and free of debris.

16. **GENERAL**

16 .01 Summary

A. The Access Control System shall be the key central component for managing physical security. The system shall provide a variety of integrated functions including access control, alarm monitoring, intrusion detection, visitor management and video integration.

16.02 Related Requirements

A. Lenel is the Access Control system listed. Any substitutions shall be submitted **five (5) days** prior for the School's approval.

16.03 References

A. Abbreviations

1. ACS: Access Control System
2. ADRC: Advanced Dual Reader Controller
3. AES: Advanced Electronic Encryption
4. API: Application Programming Interface
5. DAS: Direct Attached Storage
6. DHCP: Dynamic Host Configuration Protocol
7. DPS: Door Position Sensor
8. DRI: Dual Reader Interface
9. FASC: Federal Agency Smart Credential
10. FASC-N: Federal Agency Smart Credential Number
11. FICAM: Federal Identity, Credential, Access Management
12. FIPS: Federal Information Processing Standard
13. ICM: Input Control Module
14. IP: Internet Protocol
15. ISC: Intelligent System Controller
16. IDRC: Intelligent Dual Reader Controller
17. ISDC: Intelligent Single Door Controller
18. LAN: Local Area Network
19. LDAP: Lightweight Directory Access Protocol
20. NAS: Network Attached Storage
21. NFC: Near Field Communications
22. OCM: Output Control Module
23. ODBC: Open Database Connectivity
24. OPC: OLE for Process Control
25. OSDP: Open Supervised Device Protocol
26. PACS: Physical Access Control System
27. PIV: Personal Identity Verification
28. POE: Power-Over-Ethernet
29. RAM: Random Access Memory
30. REST: Representational State Transfer
31. REX: Request to Exit
32. RFID: Radio Frequency Identification
33. RIM: Reader Interface Module
34. SIA: Security Industry Association
35. SQL: Structured Query Language
36. SRI: Single Reader Interface
37. SSL: Secure Sockets Layer
38. TCP: Transport Control Protocol
39. TDE: Transparent Data Encryption
40. UPS: Uninterruptible Power Supply

B. Definitions

1. Alarm aggregation: A mechanism of combining several alarms into a single item (group) based on certain criteria.
2. Credential: Data assigned to an entity and used to identify that entity.
3. Designated One Person Control: Requires that a designated cardholder be present before anyone else is allowed to access a certain area.
4. Designated Two Person Control: Requires the presence of two cardholders, designated as special "Team Members", to restrict individuals from being alone in restricted or highly secure areas as well as restricting the type of personnel allowed in those areas.
5. Devices Global Hard Anti-pass back: Once access has been granted via a valid badge presentation, (1) a cardholder cannot present their badge to another entry card reader within the same area without first presenting it to the area ˡs exit card reader, and (2) any attempt to use any card reader in the same area other than exit card reader shall result in access denied and an alarm report.
6. First Card Unlock: Function where a pre-determined time zone activated unlock command is suppressed until a valid credential has been presented and granted access to the portal.
7. Global Soft Anti-pass back: As defined in Devices Global Hard Anti-pass back with the exception that the cardholder shall be allowed access to a new area for which he is authorized.
8. (Guard) Tour: One or more checkpoints (card readers or alarm inputs) checked during a guard's predetermined path.
9. Interlock group readers: Configuration for local, but not global, anti-pass back whereby only one door may be opened at a time within the area and an alarm is generated for any denied access.
10. Pass-Through: The ability assigned to a person's credential that allows them to access a door even if in lockdown state.
11. Occupancy Limit: Restricts the number of cardholders that shall be present in an area at any given time
12. Region: A separate instance of the distributed database.
13. Representational State Transfer (REST): A software architecture style consisting of guidelines and best practices for creating scalable web services.
14. RESTful API's (Application Programming Interfaces): Term given to Web services using the REST architecture.
15. Runaway detection: A situation when there are more than a specified number of alarms coming from a given device within a specified time interval.

16. Tailgate Control: Triggered when a person receives an access granted, an output will be fired momentarily for a single person or twice for two people, for a maximum duration of one second.

17. Timed Anti-pass back: Configurable wait time between an initial badge swipe and the time at which the same badge will be accepted again at the same card reader.

18. Time zones: Time-based periods, encompassing time of day, day of the week and holidays, which are stored on the ISC and control hardware behavior, cardholder access, online mode of the readers, activation of outputs, masking of inputs, and logging events to the database.

19. Two Person Control: Restricts access to certain areas unless two (2) cardholders are present, where the second badge must be presented within a designated time interval of the first to provide access,

C. Reference Standards

1. Underwriters Laboratories

   a. UL 294 - Standard for Access Control System Units

   b. UL 1076 - Standard for Proprietary Burglar Alarm Units and Systems

   c. UL 1981 - Standard for Central-Station Automation Systems

   d. UL 1610 - Central Station Automation System Software

2. ISO/IEC 14443-3:2011 - Identification Cards
3. ADA — Americans with Disabilities Act

4. National Fire Protection Association

   a. NFPA 70 National Electric Code

   b. NFPA 101 - Life safety Code
   c. NFPA 731 - Standard for the Installation of Electronic Premises Security Systems

5. Institute of Electrical and Electronic Engineers

   a. IEEE 802.3 Ethernet Standards

6. National Institute of Standards and Technology (NIST)

   a. Federal Information Processing Standard Publication 140-2 — Security Requirements for Cryptographic Modules

   b. Federal Information Processing Standard Publication 197 — Advanced Encryption Standard

   c. Federal Information Processing Standard Publication 201 — Personal Identity Verification

   d. SP 800-1 16 A Recommendation for the Use of PIV Credentials

7. Security Industry Association

    a. Open Supervised Device Protocol (OSDP)

8. Video

    a. IEC 10918 - JPEG

    b. ISO / IEC 14496-10, MPEG-4 Part 10 (ITU 1-4.264)

D. Submittals

1. Informational Submittals

    a. Product Data

    b. Manufacturer product data sheets

    c. Manufacturer product instructions, and installation and operating manuals

    d. Shop Drawings

        1) Complete set of proposed drawings, identifying equipment locations, types of cabling, numbers of conductors, raceway locations, and termination points of each conductor.

        2) Complete listing of proposed devices, indicating interconnection equipment locations and specifying terminal/connecter termination locations.

        3) Operational narrative of each component/system.

2. Record Documentation:

3. Closeout Submittals

    a. Final listing of doors, locations, and normal status in MS Excel format.

    b. Complete set of supplier's operating instructions, installation instructions, and troubleshooting guide, to include but not be limited to instructions for:

    c. Schematic drawings depicting type and location of interface equipment/components, 1. number of cables and conductors, raceway locations, types of connectors, circuit requirements and type and dimensions of enclosures.

16.04 Quality Assurance

A. Contractor qualifications:

1. Company with a minimum of 5 (Five) years system design, engineering supervision, and installation experience in the access control industry.

2. Contractor must be a current, authorized reseller for the Access product and manufacturer, and provide evidence thereof.

3. Contractor Must Retain Business Address within Fifty (50) Miles of Project Location.

B. Manufacturer Qualifications

1. The Access Hardware and software manufacturer(s) shall have delivered security management products for at least 10 (ten) years, and shall have a sufficiently large and diverse installed base to ensure competence in delivering, deploying, and supporting systems of this type and scale throughout their expected service life.

16.05 Manufacturer Capabilities

A. Advanced Services - The Access Manufacturer shall have an in-house Advanced Services group available to contract for:

1. Professional engineering services to include on-site or remote advanced support, enterprise planning and advanced deployments, system design, supporting software tools, database migrations and conversions, emergency service, system assessments.

2. Remote Management and Embedded Services to include project management and coordination, contract management, VAR coordination, and Manufacturer resource coordination

3. Custom applications and reports.

B. 3rd Party Product Certification Program

1. The Access Manufacturer shall have a Partner Program that allows other products to develop interfaces to the Security Platform based on a RESTful Web Services API.

a. Third-party integrations shall have been certified by Access Manufacturer personnel.

b. Each new revision or version of the third-party system shall be subject to recertification.

2. Interfaces developed shall be tested and certified by the Access Manufacturer for each new version of product released.

The Certification Program shall have integrations which include, as a minimum, Command and Control, Key Management, Fire Detection, Intrusion, Elevator and Critical Communication products, and the capability to integrate with other security and non-security products, as desired by the customer.

C. Global Support Capability

1. The Access Manufacturer shall have dedicated global support mechanisms in place to provide local support to any installation covered by this specification, regardless of location throughout the world.

2. The Access Manufacturer shall have multiple independent Value-Added Reseller (VAR) options to support customers in each market.

3. The Access Manufacturer shall have a proven and demonstrable history of deploying Enterprise-scale solutions to Global customers.

4.

16.06 Warranty and Support

A. Manufacturer shall warrant that the physical media on which the Software is distributed, if applicable, is free from defects in materials and workmanship and that the Software will function in substantial accordance to the Documentation that accompanies the Software for a period of one (1) year from the date of shipment of the Software to the reseller. This limited warranty is void if failure of the Software results from accident, abuse, modification, misapplication, misuse, abnormal use, or a virus.

B. Hardware warranties shall be provided by the original manufacturer of the specific hardware device or component.

C. Manufacturer shall offer a supplemental software support program to include software updates and upgrades.

16.07 License

A. The Access shall only require a single license key to be present on the database server for the Access to operate.

1. A license key on the database server shall determine the number of client workstations that shall be able to connect to the Access and access its functionality.

a. The license key shall either be a physical device or a software license key.
b. License keys shall not be required at the client workstations.

2. The Access shall allow the Access user the ability to activate, return, or repair the software license key.

3. The software license shall only be used on a physical computer or in a VMware virtual environment.

PRODUCTS

16.08 Manufacturer

A. LenelS2

1. 1212 Pittsford-Victor Road, Pittsford, NY 14534-3820
Phone: +1-585-248-9720
info@lenel.com

2. Products

a. Security Management Software: Version 7.5 OnGuard

16.09 General Description

A. The Access control System shall be the key central component for managing physical security access control, contractor management & system wide alarms.

B. Scalability

1. The Access Control shall be capable of processing an unlimited number of credential readers, scalable from single site to multiple sites.

C. Database

1. The Access Control shall be based upon one or more independent secure SQL database instances, one of which has been designated as the system master.

D. The Access Control shall provide a variety of integrated core functions to include:

1. regulation of access and egress
2. provision of identification credentials
3. video management
4. monitoring and managing alarms related to both access control and intrusion
5. visitor management

E. Integrations — The Access Control shall employ a RESTfuI, Web Services API to enable the integration of select third party products and functions with the core functions of the Access Control.

F. Communication Security

1. All communication paths within the Access Control shall support encryption to provide end-end communication security.

G. User Login and Authentication

1. The Access Control shall offer both a native capability to manage system users, as well as the option to authenticate system users through an external Active Directory, LDAP, or OpenlD Connect (OIDC) system. Solutions that do not support OpenlD Connection authentication of system users shall not be acceptable. System shall also allow for denial of login after a specified number of failed retries.
2. System shall also log the user out of any browser clients after a specified period of inactivity.
3. Customizable login message and ability to link to external websites or documents.

H. The Access Control should provide the ability for control of expiration and complexity for the User Account Passwords internal to the system such that system could comply with existing NIST and NERC guidance.

Complexity options to include: Upper/Lower Case, Numeric, Special Characters, Minimum Length, Prohibited List, and Password history

Expiration options to include: Number of days as well as administrator enforced update of password.

I. Operational Efficiencies

1. The Access Control shall offer a self-service portal for employees to request access and for area owners to approve, hold or deny requested access. This web portal shall also offer administrator-configurable self-service functions for cardholders such as PIN change, setting up a visitor and visit record, and resending a mobile credential to their mobile device.
2. Transactions shall be reportable within the Access Control.
3. The Access Control shall offer an expedient means to identify access rights provided in violation of corporate policies and to automatically revoke access rights for these violations.
4. The Access Control shall offer a browser-based analysis tool that collects system data for comprehensive system health monitoring and displays it on a customizable, intuitive dashboard.

16.10 Architecture

A. Open Architecture — The Access Control shall support an 'open architecture' allowing for additional support of products outside of the vendor proprietary options.

1. Access Control shall support hardware that is non-proprietary such that other vendors could readily offer support for these devices. Access Control Panels that are only supported by a single Access Control provider shall not be acceptable.
2. Access Control shall support a RESTful Web Services Application Programming Interface (API) that supports the opportunity for 3rd party integration. Access to this API should be managed through a program to ensure that certified integrations utilize this API appropriately.
3. The Access Control shall, when possible, leverage open or industry standards for device and system design.

B. System Topology

1. The Access Control shall include a central or distributed server component for managing security and any associated integrations.

   a. The Access Control
   b. Server shall function as an application server for connectivity of workstation based or browser-based clients for support of configuration and management.

2. An input or output linkage feature shall allow linking of input points to output control points.

3. Tasks shall be accessible from compatible client workstations on the network utilizing any of the following:

a. Traditional client-server architecture, using either Windows clients or browser clients for common day-to-day tasks,

b. Support for federated system architecture (multi-server, multi-database) where the Access Control supports the expansion of the system architecture and allows for user deployment based upon their system architectural needs.

c. Centralized distribution (publishing) of applications using Windows Terminal Server and Citrix® on Windows, UNIX, Linux or Apple Macintosh based systems through any compatible internet browser application and/or by means of a mobile computing platform using a wearable computer, Tablet PC, or mobile device.

4. Redundancy – The Access Control shall support the following means of fault tolerance and Access Control redundancy:

   a. Hot Standby Servers -A Primary Server shall be the main server that is in use when the Access Control is operating under normal conditions, and the Access Control shall mirror its database information to a Backup/Secondary Server.

      1) Field hardware shall be configured for both the Primary Server and the Backup Server, which shall each recognize the same TCP/IP ISC address on the network.

      2) Upon sensing Primary Server failure, the Backup Server shall automatically initiate itself as the Primary Server and shall begin communication with the Field Hardware.

         a. Frequency of check for Primary Server failure: 5 seconds

         b. Resynchronization time upon Primary Service restoration: 5 minutes maximum

   b. Cluster/Warm Standby — A Primary Server shall be the main server that is in use when the Access Control is operating under normal conditions.

      1) Field hardware shall be configured for both the Primary Server and the Backup Server, which shall each recognize the same TCP/IP ISC address on the network.

      2) Upon sensing Primary Server failure, the Backup Server shall bring the necessary services online and shall begin communication with the Field hardware.

      3) Shared media devices, either single or dual, shall be employed to house the hard disk used by bother servers.

         a. Resynchronization time upon Primary Service restoration: 5 minutes maximum

c. Disk Mirroring - This configuration shall allow data to be stored on dual hard disks running simultaneously.

d. RAID Level 10 - The Access Control shall offer a Fault Tolerant Redundant Array of Independent Disks Level 10 (RAID Level 10) with a hot standby disk.

1) Redundant components: disk storage, controller channels, high efficiency power supplies

e. Distributed Intelligence - In the event Access Control communications is lost or the database server fails, Intelligent System Controllers shall provide complete control, operation and supervision of the system's monitoring and control points.

1) Should the downtime exceed the capacity of the Field Hardware buffer and events are overwritten, an alarm shall appear in the Alarm Monitoring Window notifying the System Operator that events were overwritten.

C. Inter-site Communications

1. The Access Control shall support a distributed system (application and database) installation to support geographical or logical separation and management of installations while maintaining a centralized system for reporting.

a. Each distributed system shall support operation of the local clients and hardware, and provide configuration, event, and transactional events to the central system.

b. The Access Control shall use a message architecture to transfer necessary incremental credential data from one site to another. This architecture shall provide data queuing, guaranteed delivery, and secure transmission of this data.

D. External Interaction of Data

1. The Access Control shall be able to connect to and interface bi-directionally with external data sources utilizing the following methods:

a. ASCII with support for XML formatted text exchange

b. Real-time exchange of data via Active Directory or LDAP

c. Software Application Programming Interface (API)

E. Database - The Access Control shall utilize a single supported relational database.

1. Acceptable databases: Microsoft SQL, Oracle

2. Acceptable operating systems: Microsoft Windows Servers or Clients

3. Protection of 'Data at Rest' within the database shall be provided via SQL Transparent data encryption (TDE) and shall be supported to perform real-time I/O encryption and decryption of the database and database log files.

4. The Access Control database server shall support an unlimited number of cardholders and visitors limited by the available memory, storage, and processing of the devices. The Access Control database server shall support an unlimited number of system

events and System Operator transactions in the history file limited only by available hard disk space. The Access Control database server shall support an unlimited number of system events and System Operator transactions in the history file limited only by available hard disk space.

5. The Access Control shall support bi-directional data interface to external databases in real-time or in a batch mode basis.

   a. The Access Control shall support a one-step download and distribution process of cardholder and security information from the external database to the Access Control database and through the system to Intelligent System Controller (ISC) databases.

   b. If a required communication path is broken, the data shall be stored in a temporary queue and shall be automatically downloaded once the communication path is restored.

F. Security

1. Each page in the cardholder record shall be permission protected.

2. Each field in the database shall be permission protected.

3. All cardholder PIN codes within the system shall be encrypted.

G. A Network Account Management Module shall integrate Access Control cardholders with external user network accounts, allowing System Administrators to perform a set of administrative tasks in Windows domains from the System Administration Module, and to create a link between physical access control and logical domains.

H. The Access Control shall allow, through standard API toolkits, System Administrators to expose specific Access Control data and events that are relevant to IT information or other third-party systems or to allow, System Administrators to accept and process information exposed from the IT information or other third-party systems.

16.11 Core Functionality

A. Access Control - access granted or denied decisions, define access levels, and set time zones and holidays. The Access Control shall support features such as area control (two-man control, hard, soft, and timed anti-pass back), database segmentation, and time zone or holiday overrides.

1. Configuration

   a. Credentials

      1) Access Control credential management functionality shall allow:

         a) enrollment of cardholders via traditional thick client and/or by a browser-based credential application for the storage of cardholder records in the database

         b) formatting of cardholder records

         c) capturing of images, biometric data, and signatures

d) user-defined fields in the cardholder record

e) issuance/reissuance of traditional plastic badges and/or mobile credentials using information in the cardholder record. It shall be possible to print to a designated, configured badge printer from both browser-based and Windows clients. This mechanism shall be based on a print server architecture supported by the Access Control. Solutions requiring a printer directly connected to the device on which the browser client is used shall not be acceptable.

f) import or export of cardholder data from internal or third-party systems

i. data delimiter:	definable
ii. import-export filters:	selectable

g) assignment and modification of access rights and levels

h) definition of cardholder escort requirements

i) cardholder use limits

j) user definition of extended individual strike and door held open times

k) deactivation of credential following a period of non-use

l) furnishing and management of digital certificates for smart cards

m) searching for records and images based on any fields in the database

2) Field types: text, date, numeric, drop-down lists

b. Access Levels shall consist of a combination of readers and time zones.

1) Minimum number of supported access levels per controller:

32,000

2) Minimum number of supported access levels per badge: 255

3) Card readers shall be assignable to any or all access levels.

4) Each access levels shall have the option for "First Card Unlock".

5) Temporary access levels — Within the constraint of number of access levels, the Access Control shall have provision for access levels with definable start and end dates.

6) Precision access levels — Beyond the constraint of number of access levels, the Access Control shall be able to assign access levels with unlimited card reader and time zone combinations.

7) Access Groups — The Access Control shall provide for access groups, assignable to an alphanumeric name, containing up to 32 access levels.

8) Time zones — Pre-defined card reader settings shall have the flexibility to be overridden or modified for locking state and required authentication means.

c. Holidays shall be assignable via an embedded calendar with an alphanumeric name and to individual time zones.

1) Minimum number of holiday assignments: 255

2) Number of holiday group types: 8

3) Repeat frequency: annual

4) Daylight Savings Time: definable for automatic time conversion

5) Span: configurable for multiple days

d. Time zones

1) The Access Control shall be capable of creating time zones, each with intervals assignable to any day of the week.

a) number of times zones: 255

b) Intervals: 6 minimum

2) Time zones shall be allowed to belong to any or all access levels so that the time zone only has to be defined once.

e. Scheduling - The Access Control shall have a scheduling utility to allow System Administrators to schedule actions to occur on a one-time or a recurring basis and to maintain a log of actions executed.

f. Field Hardware

1) The Access Control shall allow for a Windows-based configuration of the following types of field devices which participate in the access control function:

a) Intelligent System Controllers (ISC's)

b) Input Control Modules (ICM's)

c) Output Control Modules (OCM's)

d) Access card readers

e) Integrated lock-readers

2) The Access Control shall provide a device discovery utility to aid in configuration.

a) Scope: local subnet or multiple subnets

b) Display categories: brand, discovery service, device status, device type

c) Available functions: ping, reboot, default password check, version discovery, launch device web server, save credentials, update IP address

3) When a field hardware device is configured, the device shall appear in a graphical system overview tree and be available in drop down lists which support operator access.

4) The Access Control shall have the ability for bulk add, modify, and delete privileges for ISCs and card readers to allow for the ease of addition and maintenance of themes.

5) The System Administrator shall have the ability to group field devices into monitor zones.

6) System status update frequency shall be configurable.

g. Alarm Masking Groups - System Administrators shall be able to create groups of alarm inputs that enable them to mask or unmask multiple Input Control Module inputs and card reader inputs simultaneously.

1) Alarm Masking Groups shall be able to be masked or modified as a group or as individual points.

2) Alarm masking shall support two-man control.

3)	Number of Alarm Masking Groups:	maximum 64 per ISC
4)	Alarm inputs:	maximum 128 per Alarm Masking Group

h. Event Linkage — The Access Control shall support a global linkage feature whereby any input or output or event shall be linked to any other input or output or event, with the following additional characteristics:

1) support global I/O function lists, consisting of sequences of up to six actions

2) association with panel areas

i. Graphical Maps - The Access Control shall support graphical maps that display device or group status, function lists and video cameras dynamically in real-time, and support the following:

1) configuration to appear on command or when specified alarms are acknowledged

2) graphical map creation software that allows the import of map backgrounds from supported file formats

3) associate various maps with each area to provide for the creation of a map hierarchy

4) user-defined text and icons

5) configuration of map icon shape and color to represent the state of the associated device

2. Badging — Access Control badging functionality shall allow for the creation of different badge types based on a database field, the linking of that field to a badge type to automate the process of credential production, and the use of security colors, chromakey, and ghosting, to allow quick identification of personnel access authority.

a. The Access Control shall have the ability to create and maintain badge designs, with tools and support for image import and export, ghosting, signature capture, bar code, and smart card chips.

1) Image formats: all standard industry image formats

2) Support image processing and effects with a pre-defined effects gallery.

3) A badge layout and creation module shall support custom badge designs by the User.

b. Additional badging related functionality shall include the following:

1) assignment of access levels and access groups, including bulk assignment, modification, or deletion of access levels

2) custom badge layout

3) mobile and remote badging

4) printing: print limits, batch printing

5) magnetic stripe encoding using any of three tracks

6) support for all industry standard bar code formats

c. Credential images shall be digitized using industry standard JPEG image compression and printed using a high quality and direct card printing process.

d. The System Operator shall have the following functions available when enrolling cardholders: choose a badge type, select access levels, enter personal identification numbers (PIN), and/or any other user-defined fields.

e. A badge form shall keep a complete history of every badge that was assigned to the cardholder's record to include cardholder badge ID, issue code, badge type, badge status, activation and deactivation dates and times, PIN numbers, embossed numbers, and anti-pass back information.

3. Ingress and Egress

a. Individual Use

1) Access Cards

a) Card types supported:

i. proximity — 30 mil thickness, ISO compliant
ii. smart cards — contact and contactless

- MIFARE – 1kB (8 kb) and 4 kB (32 kb)
- DES fire
- HID I-Class
- U.S. Government FIPS 201 and HSPD-12 compliant, including TWIC

iii. PIV standard formats

iv. Mobile Credentials to be installed and used from a smart phone

b) Data formats supported:

i. Magnetic stripe – with card number, facility code, and issue code combinations up to nine-digit card number and two-digit issue code
ii. Wiegand – all industry standard variations
iii. HID Corporate 1000 – 32 bit and 48 bit
iv. 200-bit BCD FASC-N output of FASC-N readers
v. 75-bit Wiegand Binary output of GSA approved FASC-N readers
vi. Custom

c) The Access Control shall support the provisioning and usage of Mobile Credentials.

i. Mobile Credentialing shall be configurable from the Access Control to include:

- name for the credential service
- URL for issuing credentials
- Requirements for certificate-based authentication and/or Username password to access web portal

ii. Supported mobile credentials:

- Lenel – Blue Diamond
- HID
- Allegion

d) The Access Control shall support desktop smart encoding and inline smart encoding for relevant affected reader technologies.

e) The Access Control shall support a card reader cipher mode, emulating the presentation of a card credential by manually entering their badge ID.

f) The Access Control shall support a configurable denied access attempts counter for each card reader.

g) Extended Held-Open Time — Authorized cardholders shall have the ability on demand to extend the time for which a door is help open after access is granted for up to 30 minutes.

h) An alarm shall be generated upon an attempt to use any badge that is not marked active in the Access Control.

2) Biometrics shall support multi-factor (or alternate) identification through the measurement and comparison of human characteristics including fingerprints, hand geometry, iris imaging, and facial features. The Access Control shall have the capability to verify the identity of enrolled individuals using products from approved manufacturer partners.

a) Capture of biometric data (template) shall be accomplished via the biometric device or associated reader.

b) Cardholder biometric data (template) storage means smart card; in access controller; in the biometric partner database.

3) Request to Exit (REX) - The Access Control shall be able to provide an event when a REX is initiated

4) The Access Control provide the ability to alert the System Operator when a cardholder does not present their credential at a required location in a designated period.

5) Pre-Alarm - The Access Control shall support a card reader pre-alarm feature which sounds a tone prior to a door held open alarm for a configurable period.

a) The Access Control shall allow operator response instructions to be specified for each type of alarm and delivered via text and/or audio.

b. Area Control - The Access Control shall support area control implementing functionality affecting more than one person, and have the following elements:

1) Global and Local Hard Anti-pass back

2) Global and Local Soft Anti-pass back

3) Timed Anti-pass back

4) Two Person Control

5) Designated One Person Control

6) Designated Two Person Control

7) Tailgate Control

8) Occupancy Limit

9) Interlock group readers

4. Elevator - The Access Control shall provide elevator control using standard access control field hardware that will permit the restriction of cardholder access to certain floors while also allowing general access to other floors, with the following additional functions:

   a. Allow, at the elevator, the use of any card reader and card reader modes used on any other card reader in the Access Control

   b. Track which floor was selected by an individual cardholder for auditing and reporting purposes

   c. Provide an option where the floors of a building are able to be configured into logically divided sections (floor groups) to prevent passenger requests between designated sections.

5. Field Devices

   a. Interface

      1) The Access Control shall be equipped with the access control field hardware required to receive alarms and administer access granted or denied decisions.

      2) The Access Control shall be capable of interfacing with the following field devices:

         a) Intelligent System Controllers (ISC)
            i. LNL-X3300

         b) Intelligent Single Door Controller (ISDC)
            i. LNL-X2210

         c) Intelligent Dual Reader Controller (IDRC)
            i. LNL-X2220

         d) Advanced Dual Reader Controller (ADRC)
            i. LNL-X4420

         e) Input Control Module (ICM)
            i. LNL-1100-S3

         f) Output Control Module (OCM)
            i. LNL-1200-S3

         g) Single Reader Interface Module (SRI)
            i. LNL-1300-S3

         h) Dual Reader Interface Module (DRI)
            i. LNL-1320-S3

         i) Power over Ethernet (POE) Enabled Door Controller
            i. LNL-1300e

j) Wireless Gateway Interface

i. PIM400-1501-KlT

k) Communication Star Multiplexer

i. LNL-8000

l) Network ready power supplies and enclosures

m) Intelligent and combination locks

n) Intrusion Cable Devices:

i. LNL-CK

3) Migration boards.

4) The Access Control must be able to retrieve device serial numbers from field hardware, excluding card readers, biometric readers, and keypads.

b. Data download

1) The Access Control shall provide for the downloading of data to the ISCs. Downloads shall load Access Control information (time zones, access levels, alarm configurations, etc.) into the ISC's first, followed by cardholder information and card reader configurations.

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

c. Permission control - The Access Control shall allow System Administrators to set permission control for individual devices within a monitoring zone for command override.

d. Device grouping — The Access Control shall support device grouping for uniform command and control of groups of devices within the system.

e. Card readers

1) Options to include:

a) User commands

b) Door strike, REX and DPS functionality

c) Duress actions

d) Alarm masking

e) Logging requirements

f) Selection as "In" or "Out" reader

g) Use limits

2) The Access Control shall provide connectivity to, proximity/mobile ready, Smart Card and smart card/mobile ready readers which provide continuous

supervision and monitoring of reader processor and wiring integrity by means of a non-proprietary communications protocol standard.

3) The Access Control shall support encrypted reader to panel communications using the SIA OSDP Secure Channel protocol.

f. Input Control Modules (CM's) options to include:

1) Alarm masking

2) Local linkage of inputs and outputs

3) Output activation rules

4) Input configuration for Guard Tour

5) Entry (latched, not latched) and Exit delay modes

g. Intelligent System Controller (ISC) capabilities shall include:

1) Administrator functions to group, add, modify, or delete ISC's in the system

2) Ability to update firmware or replace hardware while maintaining complete hardware and data configuration settings

3) A distributed intelligence redundancy mode, whereby the ISC, configured with a UPS battery to maintain the unit for 24 hours, participates with other ISC's to provide complete control, operation and supervision of the system's monitoring and control points in the event of Access Control server failure.

a) cardholder capacity: configurable up to 1,000,000

b) event capacity: configurable up to 50,000

h. A system Operator shall have the option to manually control the output points or input points connected to the Access Control.

i. The Access Control shall support a real-time graphical system status tree or list window that graphically depicts configured field hardware devices.

6. Distributed Access Level Management

a. The Access Control shall provide a browser-based interface for the assignment of access rights to individuals or groups of cardholders, using a simple user-interface paradigm suitable to general employee use, and not requiring specialized training on the Access Control

b. The Access Control administrator shall have the ability to designate for which areas a manager has assignment rights. These rights shall then be reflected in the browser interface accessible by the area manager, such that only areas for which they have authority are available for assignment.

c. The browser-based tool for access rights assignment by area managers shall have the ability to search for cardholders and to view cardholder details, constrained by the permissions of the manager

B. Alarm Monitoring - The Access Control will provide the ability to monitor system and device Alarms/Events, Field Hardware Command and Control and Status Monitoring and system support functions, for the use of the operators of the system.

1. The Access Control shall provide monitoring options thru workstations installed or browser-based clients.
2. An Alarm Monitoring window shall provide System Operators information about the time, location, and priority of an alarm and provide the ability to sort pending and new alarms based on event detail.
   a. Detail shall include at a minimum: Date/Time, Description, Priority, Controller, Device, and person.
3. Alternate alarm view windows shall be available to support: Alarm or Badge Activity Monitoring, Event Tracing (Live/Historical), and Alarms Pending Response
   a. Operators shall be able to acknowledge alarms from any alarm view window.
4. Monitor support shall include the ability to view live and recorded surveillance video and link video to alarm events.
5. Monitor support shall include options for comparison of the in-person cardholder to their stored image either in person or via live video. Cardholder Verification and Video Verification.
6. The Access Control shall allow a System Operator to:
   a. monitor alarms in their assigned monitor zone and to perform field device control actions on specified devices in that zone from either thick client, web client or mobile client platform
   b. delete the alarm from the alarm monitoring window without acknowledging the alarm
   c. enter and edit an Acknowledgement note detailing the cause of specified alarms and the actions taken
   d. activate, deactivate, or pulse outputs configured and associated with a card reader
   e. mask or unmask each individual card reader door forced open alarms, door held open alarms, and associated auxiliary alarm inputs
   f. display a cardholder record with the stored cardholder's image
   g. verify that a person using a credential matches their stored photo
   h. open multiple cardholder verification windows to cover multiple readers at the same time
   i. initiate several traces of cardholders, assets, and/or field hardware devices while monitoring alarms
   j. initiate an historical trace for a device, specifying a date and time range

k. filter alarms from the trace window to include access granted, access denied, system, duress, and area control alarms and by alarm source

l. perform a trace on any ISC, ICM, Alarm Input, Credential, Intrusion Detection Device, Monitor Zone, or card reader

m. manually override card readers, alarm points, and relay outputs

n. combine, enable, or disable alarms for aggregation

o. acknowledge or delete a group of aggregated alarms

p. view runaway devices

7. System Administrators capabilities shall include:

   a. set permission control for individual devices within a monitoring zone for command override

   b. assign default monitor zones to monitoring workstations

   c. option to define monitor zones to include sub devices of an ISC

   d. configure how the Access Control handles the annunciation of alarms on an individual alarm or event basis

   e. set display parameters for unacknowledged alarms

8. Notifications - Upon alarm, the Access Control shall allow for:

   a. automated sending of texts or e-mail messages

   b. forwarding alarms to another location.

9. Annunciation - The System Administrator shall have the ability to configure how the Access Control handles the annunciation of alarms on an individual basis.

   a. These attributes and actions shall be assignable on a 'global' basis to all devices that share an alarm description.

10. System Administrators shall be able to route and re-route device alarms and events to defined monitoring client workstations on the network, regardless of where the alarm is generated in the field.

11. A real-time graphical system status tree on the screen shall indicate the status of devices to reflect secured, unsecured, in alarm, or offline and provide command and control functions for authorized users.

12. Output control operations shall be available to lock, unlock or pulse control points.

13. An automatic cardholder call-up feature shall allow the quick search and display of images in the database.

14. Logging

   a. All alarms and events in the Access Control shall, by default, always be recorded in the database.

1) System Administrators shall have the ability to select on a time zone basis, the times required for the Access Control to log specific events to the database.

2) System Administrators shall have the option for Alarm or Events to be set to log or not to log alarms or events by individual reader or input.

b. A System Operator journal shall be available to log important daily events.

15. A trace function shall be available for System Operators to locate and track activity on specific cardholders, assets, video cameras, or card readers. An image comparison feature must be provided for use in conjunction with a CCTV interface.

16. The Access Control shall support a Test Mode for Alarm Inputs, Door Forced Open, and Access Grants to verify that all inputs within the group are operational.

C. Intrusion Detection

1. The intrusion detection function shall employ keypad used in conjunction with a card reader, both supplied from the Manufacturer.

2. The Alarm Monitoring interface shall be able to control the intrusion detection function.

3. Intrusion zone point types:

a. 24-hour point

b. Interior point

c. Perimeter point

4. Arming options:

a. Exit delay

b. Entry delay

c. Forced

5. Actions under User command:

a. Disarmed

b. Disarmed Fault

c. Armed Away

d. Armed Stay

e. Armed Instant

f. Forced Armed Away

g. Force Armed Stay

h. Force Armed Instant

i. Entry Delay

j. Exit Delay

k. Alarm

l. After Alarm

m. Chime

n. Silence

6. System Administrators shall have the ability to define Alarm Mask Groups for sets of points to be treated as an intrusion area.

    a. Indication of events from these points shall be masked (disarmed) or unmasked (armed).

7. The Access Control shall support Intrusion Mask Groups to contain individually configured intrusion points and to have the capability reporting of arming mode and state for the group.

8. Alarms shall be reported for the intrusion mask group by the Access Control based on the current arming mode and state of the intrusion mask group,

D. Third Party Application Programming Interface (API)

1. Software Integrations

    a. Software integrations shall be based upon a RESTful Web Services API.

    b. Access control integrations shall provide for the following functionality:

        1) Full Alarm Management - Send and Receive and Acknowledge alarms

        2) Full identity/card management (add/modify/delete) identities, cards, visitors, access permissions, etc.

        3) Main command and control operations including — Set Reader modes

        4) Add/modify/delete of operator/user permissions of the system

        5) Access to device and other security system configuration (e.g. panels, readers, segments, badge types, etc.)

        6) API support for the same functions as used by manufacturer's browser clients, such that it is possible to implement the same features and functions as the manufacturer, but in custom applications or integrations.

2. Hardware Integrations

    a. Hardware integration shall be based upon native API plug-ins that allow for 3rd parties to map their hardware into the access system to extend the supported device set including but not limited to, Fire, Intrusion, Intercom, Video, Cameras, Readers, etc.

    b. Integration shall provide full support for alarms, hardware status, and command and control for integrating third-party devices into the alarm monitoring software

c. Video integration shall allow for both third-party video to be integrated into the Access Control as well as Access Control video to be accessed by a third-party.

16.12 Optional Capabilities — The Access Control shall allow for the inclusion of additional capabilities.

A. Conversions and Migrations - Manufacturer shall offer the capability to migrate systems from the following manufacturers (equipment)

1. Mercury
2. Honeywell
3. GE Security / Infographics ACU
4. GE Security / CASI - M Series
5. Johnson Controls - Tyco (Software House@)

B. U.S. Federal Government

1. The Access Control shall be compliant with US Federal Government Personal Identity Verification Authentication Standards for readers and credentials as defined in FIPS 201-2 to include the following criteria:

   a. The solution proposed must be listed on the FICAM (Federal Identity, Credential, Access Management) Approved Products List.

   b. The solution proposed must support certificate authentication of the FIPS-201 credentials at each entry, through a connection from the Access Control components to the Federal Bridge. Systems that rely on an additional hardware component whose primary function is solely the validation of credentials shall not be acceptable.

   c. Cryptographic portion of the Access Control approved through the NIST FIPS 140-2 cryptographic validation program.

C. Smartphone-based Mobile Credential Support

1. The Access Control user screens shall include the ability to issue, modify and revoke smartphone-based mobile credentials. Solutions requiring "dual-enrollment" of mobile credentials in a cloud or web app as well as the Access Control are not acceptable.
2. Mobile credentials shall be supplied on a "pool" basis, where specific credentials can be removed and replaced with new credentials at no additional cost.
3. It shall be possible to reissue a credential to a different mobile device for the same user at no additional cost Solutions that require the purchase of a new credential when a user gets a new phone are not acceptable.
4. The mobile solution shall include the ability to add Bluetooth to existing Wiegand readers via an add-on module.
5. The system shall have the ability to create a custom email template that will be sent to the cardholder

a. Email shall include link to download the mobile credential application, instructions to install and configure the mobile app, and a one-time password to authenticate the mobile application to the credential server

6. A System Administrator with appropriate user permissions shall have the ability to create a friendly name for each mobile reader, to be displayed in the mobile app

7. The mobile app and credential installed on the cardholder's phone shall be compatible with Android and iPhone mobile operating systems.

   a. The app shall be available for download from the "App Store" and the "Google Play Store".

      1) The mobile app shall synchronize with the credential server to validate authenticity at least once every 48 hours

      2) Mobile app shall use a Bluetooth signal to establish a connection to the mobile reader

         a) Connections between phone and reader shall be encrypted using at least 128bit AES encryption

      i The encrypted connection shall protect against and not allow a "record and Playback (Blue Snarfing)" attack as well as protect against other Bluetooth vulnerabilities.

      ii. The mobile solution shall have annual cyber security risk assessments and penetration testing, performed by at least two independent cybersecurity auditing firms.

   b) The mobile application will display to the cardholder readers that are currently within Bluetooth range.

      i. The mobile app will allow a cardholder to adjust sensitivity which will increase or decrease the range of discoverable readers.

      ii. The mobile app shall give preference to the readers that are:
         - Closest in range
         - AND most frequently used

      iii. The Mobile application shall have the ability to send a notification when a chosen reader is in range, even when the phone is locked.
         - It shall be possible to unlock the door directly from the notification, with appropriate authentication to the mobile device (pin, face, or fingerprint, depending on device).

      iv. The cardholder shall have the option to change the name displayed on their device for each reader.

      v. The mobile app shall allow for a cardholder to remove specified readers from their view.

vi. The mobile application shall allow for the user to create a route of doors to be reached in a pre-defined order, and that route or path may be automatically or manually started.

- Once that route or path has started the user shall be able to keep their phone in their pocket or bag and once in range of reader, the phone will automatically send the credential to the reader device with no user interaction.

vii. The mobile application shall also allow the user to present their phone as a badge to the reader, at a user-defined distance. In this mode of operation, no further interaction with the mobile device shall be required.

D. Third Party Integrations

1. The Access Control shall support multiple certified integrated third-party interfaces with hardware and software vendors to include the following functional areas:
   a. command and control
   b. communications
   c. elevator
   d. fire alarm
   e. identity and access management
   f. intercom
   g. intrusion detection and alarm
   h. IP video cameras
   i. key management
   j. license plate recognition
   k. monitoring and dispatching
   l. RFID
   m. readers
   n. recording appliances
   o. sensor inputs
   p. time and attendance
   q. video analytics
   r. video management systems

2. The Access Control shall provide a set of standard RESTful Web Services Application Programming Interfaces (API's) and supporting documentation that allows hardware manufacturers and software application developers to interface their products into the Access Control.

3. Third party interfaces shall be integrated to provide a single graphical user interface, single source code base, and a single database for configuration, alarm, and event storage.

a. The Access Control shall allow alarms and events from the third-party systems to report into the same main Alarm Monitoring window as access control alarms.

b. Third-party hardware alarms and events shall be stored in the Access Control database for audit trail and reporting purposes.

4. Data available through these interfaces shall be organized for optimum performance with one application accessing a single bank of data.

5. Any changes to system hardware shall be instantly available across the entire Access Control.

E. The Access Control shall support OPC, BACnet and SNMP protocols.

1. An industry standard OPC Server utility shall allow the export of Access Control alarms and events to industry standard OPC Clients.

16.13 Communications

A. The Access Control shall communicate with the ISCs via TCP/IP through IPv4 or IPv6 protocols.

B. Download communication between the Access Control and the ISC shall be fully multi-tasking and shall not interfere with operational functions.

C. Upon loss of communications between the Access Control Server and an ISC, an alarm shall be created with a time stamp.

1. Upon re-established communication, the Access Control and the ISC shall automatically resynchronize from the point of communication loss without operator intervention.

2. The Access Control shall support Dual Path communications between the Access Control Server and the ISC's to allow for a fully functional redundant communication path.

a. During a fail over period, the ISC shall periodically check to see if the primary path has been re-established and will automatically switch back upon a successful connection.

b. Alarms shall be generated upon loss or restoration of communications.

D. Encryption — The Access Control shall provide encrypted communication capabilities as follows:

1	Credentials to Reader:	DESFire EVI or EV2, or HID iCLASS or SEOS
2.	Reader to Downstream Panels:	OSDP Secure Channel Encryption
3.	Downstream Panels to ISC:	AES-128 bit or AES-256 bit
4.	Data on ISC	AES-256-bit Encryption of Data at Rest
5	ISC to Access Control Server:	AES-128 bit or TLSI.2 with AES-256 bit
6.	Access Control Server to Client:	HTTPS
7.	Client to Printers and Badge Encoders:	Encrypted encoder communications

16.14 System Management

A. System Configuration - The Access Control shall provide system icons and/or menu selections for each function requiring configuration of Access Control Access Control options or peripherals including client workstations, field hardware, network functions, communications, and reports.

1. A set-up assistant utility shall be available for the initial system configuration prior to first log in.
2. The Access Control shall support configuration setup wizards to guide System Administrators through the configuration of the access control module of the system.

B. In addition to capabilities previously mentioned herein, System Administration capability shall include the following:

1. Customize cardholder, asset, and visitor forms.
2. Import customized map backgrounds and custom icons
3. Bulk delete cardholder records
4. Limit System Operator functions and actions, including searching the database
5. Configure client workstation applications and settings
6. Assign System Operator passwords, log on credentials and permissions and provide operator history

C. The Access Control shall provide support for single sign-on capability, whereby System Administrators or System Operators may authenticate into Access Control applications using their Windows domain account.

D. System Administrative tasks including defining client workstation and Operator permissions, access groups, time zones, reports, and maps shall be available from any client workstation on the network.

E. Graphical Features

1. The Access Control shall display a graphical representation of configured field hardware (including ISCs, fire panels, intrusion detection devices, personal safety devices, intercom systems, and Central Station alarm receivers), digital video hardware, access levels, time zones, access groups, holidays, and card formats.
2. System Administrators shall be able to modify a device that is depicted on the graphical system overview tree or see its properties by double-clicking on the related icon, causing the Access Control to bring them to the appropriate form.

F. The Access Control shall provide context-sensitive help files to guide System Administrators and System Operators in configuration and operation.

G. Logging - The Access Control shall provide full System Operator activity tracking/logging of critical keyboard functions to include date/time, Operator, activity program, function, and database changes.

1. System Operator functions to log shall include System Operator login and System Operator logout; Additions, Changes, and Deletions to Cardholder Management; New Badge, Print Badge, and Update Badge.

2. Configuration changes to log shall include all functional modules within the Access Control.

3. The Access Control shall log activity of System Operators performing Access Control alarm monitoring including alarms acknowledged, alarms cleared, output control activity, trace, and other functions.

H. Reporting — The Access Control shall have a rich reporting function, storing its reports in the database and viewable from any client workstation with permissions.

1. The Access Control shall provide an ad hoc customized report generator, allowing the creation of reports using the relational database structure.

2. The Access Control shall support an industry standard, off the shelf, custom report writer.

I. Archiving - The Access Control shall allow System Administrators to archive offline history files. Offline files shall include access events and System Operator transactions that have been purged from the reportable database.

16.15 Hardware Requirements

A. The Manufacturer shall publish a summary of recommended server hardware to accommodate the performance requirements of the Access Control server software.

B. The Access Control server software shall be capable of running in a virtual or cloud environment.

17. **EXECUTION**

17.01 Preparation

A. The network design and configuration shall be verified for compatibility and performance with the Access Control.

B. The network configuration shall be tested and qualified by the Contractor OR 3rd Party Network Installation Contractor prior to system installation.

C. Server performance parameters shall be compared with Manufacturer requirements for the Access Control.

17.02 Installation

A. Contractor shall follow manufacturer published installation and configuration instructions and guidelines.

B. System shall be configured in accordance with manufacturer-supplied hardening guide. Access Control systems for which the manufacturer does not provide a hardening guide shall not be acceptable.

17.03 Storage

A. Server and system hardware devices and components shall be stored in an environment where temperature and humidity are in the range specified by the Manufacturer.

Attachment B Graphical Maps

Supported File Formats

The OnGuard system supports the following image formats:

- Adobe Photoshop PSD - AutoCAD DXF
- CALS Raster CAL
- Encapsulated Post Script EPS - Fax/Delrina WinFax FAX
- GEM/Ventura IMG
- IBM IOCA (Image Object Container Architecture) (first page supported only) ICA
- JPEG/JIFIF File Interchange Format JPG, JIF
- Kodak Photo CD PCD
- Kodak Flash Pix FPX
- Lead CMP
- Macintosh PICT PCT
- Mac Paint MAC
- Microsoft Paint MSP
- Portable Network Graphics PNG
- Targa RAS, TGA
- TIFF (Tagged Image File Format) TIF, MPT
- Windows Bitmap BMP, DIB

- Wlndows Metafile EMF, WMF
- WordPerfect Graphic WPG

18. OnGuard Standard Access Control Reports

OnGuard natively has 145 standard reports. All reports are stored in the access control database and are able to be viewed from any client workstation with proper permissions. Our software allows system users to e-mail reports based on system events or on a user-defined schedule. The standard reports that are included with the OnGuard are described below:

1. Access Denials and Grants by Reader Report:

   The Access Denials and Grants by Reader Report shall provide information on all access denials and granted events including time, card reader, badge, and cardholder name, sorted by card reader.

2. Access Denials, Grants, and Other Badge Events Report:

   The Access Denials, Grants, and Other Badge Events report shall provide information on all badge related events including time, reader, badge, and cardholder name.

3. Access Denied Event Report:

   The Access Denied Event Report shall provide information on all access denied events including time, card reader, badge, and cardholder name. It shall also include the following events: Interlock Area Busy, Cannot Open Door: Interlock Area Busy, Exit Request Denied: Interlock Area Busy, and DURESS - Interlock Area Busy.

4. Access Denied Events, by Reader:

   The Access Denied Events, by Reader Report shall provide information on all access denied events including time, card reader, badge, and cardholder name, sorted by card reader. It shall also include the following events: Interlock Area Busy, Cannot Open Door: Interlock Area Busy, Exit Request Denied: Interlock Area Busy, and DURESS - Interlock Area Busy.

5. Access Granted Events Report:

   The Access Granted Events Report shall provide information on all access granted events including time, card reader, badge, and cardholder name.

6. Access Granted Events by Reader Report:

   The Access Granted Events by Reader Report shall provide information on all access granted events including time, card reader, badge, and cardholder name, sorted by card reader.

7. Access Groups Report.

   The Access Groups Report shall provide information on all access groups and the access levels contained in each group.

8. Access Groups with Levels Report:

The Access Groups with Levels Report shall provide information on all access group definitions including access level details.

9. Access Level Assignments to Cardholders Report:

The Access Level Assignments to Cardholders Report shall list each access level with a listing of each cardholder that has that access level assigned to them.

10. Access Levels Assignment to Cardholders, By Segment Report:

The Access Levels Assignment to Cardholders, By Segment Report shall provide information on all cardholders with access levels, sorted by segment. Only personnel with assigned access levels shall be included in the report. This report shall also summarize the total number of badges that will need to be downloaded to each segment. This report only shall only work on a system utilizing database segmentation.

11- Access Levels Report:

The Access Levels Report shall provide information on all access level definitions.

12. Access Panels Report:

The Access Panels Report shall provide information on all access panel definitions.

13. Active Visits by Cardholder Name Report:

The Active Visits by Cardholder Name Report shall provide information on all visits that are currently active (not signed out) grouped by cardholder name.

14. Active Visits by Host Name Report:

The Active Visits by Host Name Report shall provide information on all visits that are currently active (not signed out) grouped by Host Name.

15. Active Visits by Visitor Name Report:

The Active Visits by Visitor Name Report shall provide information on all visits that are currently active (not signed out) grouped by Visitor Name.

16, Alarm Acknowledgments Report:

The Alarm Acknowledgments Report shall provide information on all alarm acknowledgments including the alarm information and acknowledgment notes.

17. Alarm Acknowledgements:

The Alarm Acknowledgments shall provide information on all alarm acknowledgments including the alarm information and acknowledgment notes, sorted by Definition.

18. Alarm Acknowledgments by System Operator Report:

The Alarm Acknowledgments by System Operator Report shall provide information on all alarm acknowledgments including the alarm information and acknowledgment notes, sorted by System Operator.

19. Alarm Acknowledgements by Panel Report:

The Alarm Acknowledgments by Panel Report shall provide information on all alarm acknowledgments including the alarm information and acknowledgment notes, sorted by Intelligent System Controller Panel.

20. Alarm Configuration Report:

    The Alarm Configuration Report shall provide alarm configuration summary information.

21. Alarm Input Events Report:

    The Alarm Input Events Report shall provide information on all alarm input events sorted by date.

22. Alarm Panel Inputs Report:

    The Alarm Panel Inputs Report shall provide information on all alarm panel inputs grouped by access panel and alarm panel.

23. Alarm Panel Local Linkage Report.

    The Alarm Panel Local Linkage Report shall provide information of all input and output linkages within an (CM.

24. Alarm Panel Outputs Report:

    The Alarm Panel Outputs Report shall provide information on all alarm panel outputs grouped by access panel and alarm panel.

25. Alarm Panels Report:

    The Alarm Panels Report shall provide information on all alarm panel definitions grouped by access panel.

26. All Cardholders with Logical Access Report:

    The All Cardholders with Logical Access Report shall list all cardholders that have linked accounts through logical access.

27. All Events Over Time Report:

    The All Events Over Time Report shall provide a listing of all event types over time.

28. All Events Over Time with Local Panel Time Report:

    The All Events Over Time with Local Panel Time Report shall provide a listing of all event types over time. This report also shows the time an event occurred in the panel's time.

29. All Events Over Time with Unique Alarm ID Report:

    The All Events Over Time with Unique Alarm ID Report shall provide a listing of all event types with a unique alarm ID over time.

30. Anti-Pass back Events Report:

    The Anti-Pass Back Events Report shall provide a listing of all anti-pass back events over time

31. Area Anti-Pass Back Configuration Report:

The Area Anti-Pass Back Configuration Report shall provide a listing of all anti-pass back areas, including the reader entrances and exits.

32. Area Configuration Report:

The Area Configuration Report shall list all areas, including the reader entrances and exits.

33 Area Entrance History Report:

The Area Entrance History Report shall provide a history of all cardholders enter anti-pass back areas, sorted by area and date.

34. Asset Classes Report:

The Asset Classes Report shall provide information on all asset classes and the asset groups to which they belong.

35. Asset Events Report:

The Asset Events Reports shall provide information on all asset events.

36. Asset Groups Report:

The Asset Groups Report shall provide information on all asset groups and the classes they contain.

37. Asset Types Report:

The Asset Types Report shall provide information on all asset types defined with all associated subtypes.

38. Assets by Scan ID Report:

The Assets by Scan ID Report shall provide information on all assets grouped by Scan ID.

39. Assets by Type Report:

The Assets by Type Report shall provide information on all assets grouped by asset type and subtype.

40. Assigned Assets by Cardholder Report:

The Assigned Assets by Cardholder Report shall provide information on all currently assigned assets grouped by cardholder.

41. Assigned Assets by Scan ID Report:

The Assigned Assets by Scan ID Report shall provide information on all currently assigned assets grouped by Scan ID.

42 Assigned Assets by Type, Scan ID Report:

The Assigned Assets by Type, Scan ID Report shall provide information on all currently assigned assets grouped by type and Scan ID.

43. Audio Notifications and Instructions Report:

The Audio Notifications and Instructions Report shall list all audio notifications and instructions in the database.

44. Badge Type Configuration:

    The Badge Type Report shall provide a listing of all Badge Types.

45. Badges by Deactivation Date Report:

    The Badges by Deactivation Date Report shall list all badges by deactivation date. Shall be used to determine which badges are about to deactivate.

46. Badges Without Access Levels Report.

    The Badges Without Access Levels Report shall provide information on all Badges that do not have any access levels assigned to them. Badges with access levels assigned to them shall not be listed in this report.

47. Card Formats Report:

    The Card Formats Reports shall provide information on definitions of all Magnetic and Wiegand card formats in the Access Control.

48. Cardholders Access to Readers Report:

    The Cardholders Access to Readers Report shall provide a listing of each card reader along with which cardholders have access to that card reader. Includes associated access level and time zone.

49. Cardholder Exit or Entry Report:

    The Cardholder Exit or Entry Report shall provide information on all user-defined Exit or Entry information on a per cardholder basis. It shall list the time a cardholder swipes their badge at a designated 'In' reader and the time they swiped their badge at the corresponding designated 'Exit' reader.

50. Cardholder Photo Gallery Report

    The Cardholder Photo Gallery Report shall provide cardholder names and photos, sorted by last name.

51. Cardholder Time and Attendance Report:

    The Cardholder Time and Attendance Report shall pair each in-time with an out-time for cardholders gaining entry to time and attendance readers.

52. Cardholders by Badge Type Report:

    The Cardholders by Badge Type Report shall provide information on all cardholders sorted by badge type. No access levels are shown in this report and cardholders that have not been assigned a badge type will not be reported.

53. Cardholders by Last Name Report:

    The Cardholders by Last Name Report shall provide information on all cardholders sorted by last name, with badges but not access levels. Only personnel with badges assigned shall be included in this report,

54. Cardholders Located in Each APB Area by Date Report:

The Cardholders Located in Each APB Area by Date Report shall provide a list of all cardholders located in each anti-pass back area, sorted by area and date.

55. Cardholders Located in Each APB Area by Name Report:

The Cardholders Located in Each APB Area by Name Report shall provide a list of all cardholders located in each anti-pass back area, sorted by area and cardholder name.

56. Cardholders with Access, by Badge Type Report:

The Cardholders with Access, by Badge Type Report shall provide information on all cardholders with access and precision access levels, sorted by badge type. Only personnel with active badges and access levels shall be included in this report.

57. Cardholders with Access by Last Name Report:

The Cardholders with Access by Last Name Report shall provide information on all cardholders with access and precision access levels, sorted by last name. Only personnel with active badges and access levels shall be included in this report.

58. CCTV Instructions Report:

The CCTV Instructions Report shall provide summary information on all CCTV instructions in the database.

59. Continuous Video Report:

The Continuous Video Report shall provide a listing of all of the times continuous video is archived.

60. Current Visits Report:

The Current Visits Report shall provide a list of all currently signed in visits.

61. Destination Assurance Configuration Report:

The Destination Assurance Configuration Report shall provide a listing of all card readers configured for Destination Assurance with their associated lead times to proceed to the next defined card reader.

62. Destination Assurance Exempt Cardholders Report:

The Destination Assurance Exempt Cardholders Report shall provide a listing of all cardholders who are exempt from following Destination Assurance procedures.

63. Device Status Events Report:

The Device Status Events Report shall provide information on all status events for all devices in the Access Control.

64. Dialup Events by Panel Report:

The Dialup Events by Panel Report shall provide information on all dialup related events grouped by Intelligent System Controller.

65. Dialup Last Connect Time Report:

The Dialup Last Connect Time Report shall provide a list of all online dialup panels and the last time that they were connected to the Access Control database server.

66. Elevator Access Denials and Grants Report:

    The Elevator Access Denials and Grants Report shall provide information on all elevator related access denied and granted events including floor selected, timet card reader, badge, and cardholder name.

67. Elevator Dispatching Devices and Terminals Report:

    The Elevator Dispatching Devices and Terminals Report shall provide a listing of all elevator dispatching devices with the configured terminals.

68. Elevator Floor Assignments to Cardholders Report:

    The Elevator Floor Assignments to Cardholders Report shall list all cardholders that have access to an elevator floor list.

69. Emergency Events Report:

    The Emergency Events Report shall provide a listing of all emergency events over time.

70. Event Codes Report:

    The Event Codes Report shall provide information on all event code templates and event code mapping configurations.

71. Event Count by Panel Report:

    The Event Count by Panel Report shall provide a count of all events grouped by Intelligent System Controller. This report shall include a pie chart breakdown.

72. Fire Device Input or Output Report:

    The Fire Device Input or Output Report shall provide a listing of all fire inputs and outputs grouped by panel and fire device.

73. Global APB or Mobile Verify Occupancy by Date Report:

    The Global APB or Mobile Verify Occupancy by Date Report shows the last known area accessed by each cardholder, sorted by date and time.

74. Global APB or Mobile Verify Occupancy by Name Report:

    The Global APB or Mobile Verify Occupancy by Name Report shows the last known area accessed by each cardholder, sorted by cardholder.

75. Global I/O Linkages Report:

    The Global I/O Linkages Report shall provide a listing of all global I/O linkages, including the input events and output actions.

76. Guard Tour Configuration Report:

    The Guard Tour Configuration Report shall provide a listing of all configured guard tours, including checkpoints, actions, and messages.

77. Guard Tour History Report:

The Guard Tour History Report shall provide a listing of all events associated with checkpoints that happened for each guard tour.

78. Hardware Panels Report:

    The Hardware Panels Report shall provide information on all top level hardware panels grouped by category including access panels, fire panels, intercom panels, personal safety panels and central station alarm receivers.

79. Holidays Report:

    The Holidays Report shall provide information on all system holiday definitions.

80. ILS Lock Authorizations by Cardholder Report:

    The ILS Lock Authorizations by Cardholder Report shall list ILS lock authorization levels assigned to cardholder/badgej sorted by cardholder.

81. ILS Lock Authorizations by Level Report:

    The ILS Lock Authorizations by Level Report shall list ILS lock authorization levels assigned to cardholder/badge, sorted by level.

82. ILS Lock Battery Status by Status:

    The ILS Lock Battery Status by Status shall list battery status of ILS locks grouped by battery status (Low to High), wireless gateway, and battery percent.

83. ILS Lock Characteristics Report:

    The ILS Lock Characteristics Report shall list ILS lock configuration details.

84. ILS Lock Communications Report:

    The ILS Lock Communications Report shall list ILS lock wireless diagnostics.

85. ILS Lock Ownership Report:

    The ILS Lock Ownership Report shall list ILS locks owned by a cardholder.

86. Intercom Functions Report:

    The Intercom Functions Report shall provide information on all defined intercom functions.

87. Intercom Stations Report:

    The Intercom Stations Report shall provide information on all intercom stations, grouped by intercom exchange.

88. Intrusion Command Authority — Advanced Report:

    The Intrusion Command Authority — Advanced Report shall list all cardholders that have access level assignments configured to use advanced intrusion command authority.

89. Intrusion Command Authority — Global Report.

    The Intrusion Command Authority — Global Report shall list all cardholders who are assigned access levels with global intrusion command authority.

90. Intrusion Command Events Report:

The Intrusion Command Events Report shall list all events associated with intrusion commands including device, cardholder name, and badge.

91. Intrusion Detection Areas Report:

The Intrusion Detection Areas Report shall provide a listing of all intrusion areas grouped by panel.

92 Intrusion Detection Devices Report:

The Intrusion Detection Devices Report shall provide a listing of all intrusion devices grouped by panel,

93. Intrusion Panel User Groups Report:

The Intrusion Panel User Groups Report shall provide a listing of all intrusion user groups grouped by panel.

94. Last Location of Cardholders Report:

The Last Location of Cardholders Report shall provide information on the last card reader accessed by each cardholder, sorted by cardholder name.

95. Locked Video Events Report:

The Locked Video Events Report shall list all system events with associated locked video events.

96. Maps Report

The Maps Report shall provide a list of all available maps in the database.

97. Mobile Verify User Transaction Log Report:

The Mobile Verify User Transaction Log Report shall provide a chronological log of all performed transactions.

98. Mobile Verify User Transaction Log by Operation Report:

The Mobile Verify User Transaction Log by Operation Report shall provide a chronological log of all performed transactions grouped by operation.

99. Mobile Verify User Transaction Log by User ID Report:

The Mobile Verify User Transaction Log by User ID Report shall provide a chronological log of all performed transactions grouped by User ID.

100. Module Details Report:

The Module Details Report shall provide information about module definitions, grouped by parent panel.

101. Module Summary Report:

The Module Summary Report shall list all modules, grouped by parent panel.

102. Monitor Stations Report:

The Monitor Stations Report shall provide information on all monitoring stations defined in the Access Control including which monitor zones and access panels are assigned to the monitoring station.

103. Monitor Zones Report:

The Monitor Zones Report shall provide information on all monitor zone definitions.

104. Panel's Report:

The Panel's Report shall provide information about Panel definitions.

105. Overdue Visits Report:

The Overdue Visits Report shall provide a listing of all scheduled visits that have not signed in.

106. Overstayed Visits Report:

The Overstayed Visits Report shall provide a listing of all visitors logged into the facility, but whose badge or visit has expired.

107. Permission Profiles Report:

The Permission Profiles Report shall provide information on permission profile definitions.

108. Personal Safety Transmitter Assignments Report:

The Personal Safety Transmitter Assignments Report shall provide information on all personal safety transmitters and their assignments to cardholders and assets.

109. Personal Safety Transmitters Report:

The Personal Safety Transmitters Report shall provide information on all personal safety transmitters.

110. Personnel in the Database Report:

The Personnel in the database Report shall provide information on all personnel in the database with basic information.

111. Personnel Without an Active Badge Report:

The Personnel Without an Active Badge Report shall provide information on all personnel in the database that do not have an active badge assigned to them.

112. Personnel with Organizational Details Report:

The Personnel with Organizational Details Report shall provide information on all personnel in the database with organizational details. This report is designed to work with the Access Control standard cardholder layout.

113. Personnel with Personal Details Report:

The Personnel with Personal Details Report shall provide information on all personnel in the database with personal details. This report is designed to work with the Access Control standard cardholder layout.

114. Point of Sale Registers Report:

The Point of Sale Registers Report shall provide a listing of all Point of Sale Registers configured in the Access Control.

115. Precision Access Groups Report:

The Precision Access Groups Report shall provide information on all precision access group definitions.

116. Reader Assignment to Cardholders Report:

The Reader Assignment to Cardholders Report shall provide a listing of all card readers assigned to a cardholder, sorted by cardholder.

1 17. Reader Command Programming Configuration Report:

The Reader Command Programming Configuration Report shall list all command programming readers along with the associated user and instant commands.

118. Reader Status Events Report:

The Reader Status Events Report shall provide information on card reader status events, grouped by card reader.

119. Reader Time zone Schedules Report:

The Reader Time zone Schedules Report shall provide information on all card reader time zone scheduling for card reader modes.

120. Readers Report:

The Readers Report shall provide information on all card reader definitions grouped by access panel.

121. Receiver Account Alarm Activity Report:

The Receiver Account Alarm Activity Report shall provide information on all alarm activity for receiver accounts including notes and elapsed times.

122. Receiver Account Areas Report:

The Receivers Account Areas Report shall provide a listing of all receiver account areas, grouped by receiver account.

123 Receiver Account Groups Report:

The Receivers Account Groups Report shall provide a listing of all receiver account groups and the receiver accounts contained in each group.

124. Receiver Account Zones Report:

The Receivers Account Zones Report shall provide a listing of all receiver account zones, grouped by receiver account

125. Receiver Accounts Report:

The Receiver Accounts Report shall provide a listing of all receiver accounts in the Access Control.

126. Receiver Accounts that Failed to Report:

The Receiver Accounts that Failed to Report shall provide a listing of receiver accounts that failed to report during their duration.

127. Receiver and Receiver Account Events Report:

The Receiver and Receiver Account Events Report shall provide a listing of all events that occurred on a receiver or receiver account.

128. Segment Badge Download Summary Report:

The Segment Badge Download Summary Report shall provide information on each segment by listing the number of badges that must be downloaded to the access panels in that segment. This report shall only work on systems utilizing database segmentation.

129. Segments Report

The Segments Reports shall provide a listing of all segments defined in the Access Control along with their options.

130. SNMP Agents Report:

The SNMP Agents Report shall provide a listing of all SNMP Agents configured in the Access Control.

131. SNMP Management Information Base Configuration:

The SNMP Management Information Base Report shall list all MIB data grouped by enterprise.

132. System Servers Report:

The System Servers Report shall provide a listing of servers defined on the system.

133. Text Instructions Report:

The Text Instructions Report shall provide information on all text instructions defined in the Access Control.

134. Time zones Report:

The Time zones Report shall provide information on all time zone definitions.

135. User Permissions Report:

The User Permissions Report shall provide information on all Access Control users and their permissions.

136. User Transaction Log Report:

The User Transaction Log Report shall provide a chronological log of all transactions performed on the Access Control by users.

137. User Transaction Log by User ID Report:

The User Transaction Log by User ID Report shall provide a chronological log of all transactions performed on the Access Control by users grouped by User ID.

138. Users with Area Access Levels to Manage Report:

The Users with Area Access Levels to Manage Report shall list all Area Access Manager users and the access levels that they manage.

139. Video Cameras Device Links Report:

The Video Cameras Device Links Report shall provide information on all device links for each video camera.

140. Video Cameras Report:

The Video Cameras Report shall provide information on all video cameras grouped by digital video recorder.

141. Video Events Report:

The Video Events Report shall provide information on all Access Control events with associated video events.

142. Video Servers Report:

The Video Servers Report shall provide information on all digital video recorders.

143. Visits History Report:

The Visits History Report shall provide information on all visits enrolled into the Access Control.

144. Visitors Report:

The Visitors Reports shall provide information on all visitors in the Access Control.

145. Windows Event Log Errors Report:

The Windows Event Log Errors Report shall provide information on all errors logged by the Access Control to the Windows event log.

ITB Cost Analysis
Access Control Management System

Emmett Elementary - Total Cost $_____________

Central High School – Total Cost $____________

Ketron Elementary – Total Cost $_____________

Access Control System bid: __________________

Estimated Completion Date: ____

The undersigned is an authorized representative of the company services indicated above and certifies that the information and accompanying documents in this ITB submittal are accurate and true.

The undersigned has read and understands the extent and character of the prerequisites and has conformed to the specified content and format requirements.

The undersigned further acknowledges that failure to submit an Invitation to Bid which conforms to the specified content and format requirements will be sufficient cause to disqualify the company. Additionally, material deficient or incomplete response will be cause to disqualify the bid.

Legal Name of Proposer:____
PLEASE PRINT

Address:____

Phone____________ / Fax____________ / E-Mail______________________________

Authorized Signature:______________________________ Date:_______________

Name and Title of Signer:____

Tennessee Contractor's License Number_______________ Expiration Date___________

Note: Failure to use these response sheets may disqualify your submission.

EXCEPTIONS

OFFICE OF THE SULLIVAN COUNTY PURCHASING AGENT

COMPANY/CONTRACTOR AFFIDAVIT FORM 00010

THE AFFIANT STATES TO SULLIVAN COUNTY, TENNESSEE:

I (WE) HEREBY CERTIFY THAT IF THE CONTRACT IS AWARDED TO OUR FIRM THAT NO MEMBER OR MEMBERS OF THE GOVERNING BODY, ELECTED OFFICIAL OR OFFICIALS, EMPLOYEE OR EMPLOYEES OF SAID SULLIVAN COUNTY, TENNESSEE, OR ANY PERSON REPRESENTING OR PURPORTING TO REPRESENT SULLIVAN COUNTY, TENNESSEE, OR ANY FAMILY MEMBER INCLUDING SPOUSE, PARENTS, CHILDREN OF SAID GROUP, HAS RECEIVED OR HAS BEEN PROMISED, DIRECTLY,OR INDIRECTLY, ANY FINANCIAL BENEFIT, BY WAY OF FEE, COMMISSION, FINDER'S FEES OR ANY OTHER FINANCIAL BENEFIT ON ACCOUNT OF THE ACT OF AWARDING AND/OR EXECUTING THE CONTRACT.

THE UNDERSIGNED HEREBY CERTIFIES THAT HE/SHE HAS FULL AUTHORITY TO BIND THE COMPANY AND THAT HE/SHE HAS PERSONALLY REVIEWED THE INFORMATION CONTAINED IN THIS REQUEST FOR PROPOSAL (RFP), INCLUDING ALL ATTACHMENTS, ENCLOSURES, APPENDICES, ETC AND DO HEREBY ATTEST TO THE ACCURACY OF ALL INFORMATION CONTAINED IN THIS RFP, INCLUDING ALL ATTACHMENTS, ENCLOSURES, EXHIBITS, ETC.

THE UNDERSIGNED ACKNOWLEDGES THAT ANY MISREPRESENTATION WILL RESULT IN IMMEDIATE DISQUAUFICATION FROM ANY CONTRACT CONSIDERATION.

THE UNDERSIGNED FURTHER RECOGNIZES THAT THE SULLVIAN COUNTY PURCHASING AGENT HAS THE RIGHT TO MAKE THE CONTRACT AWARD FOR ANY REASON CONSIDERED IN THE BEST INTEREST OF SULLIVAN COUNTY.

This certification shall be included with the bid document 00300. Failure of this properly executed document to be included with the bid shall render the bid as incomplete and void.

COMPANY NAME ____

NAME (PRINT) ____ PHONE ___________

TITLE____ FAX ______________

SIGNATURE ____DATE_____________

~~~~~~

(TO BE COMPLETED BY NOTARY)

STATE OF: ___________________________

COUNTY OF: __________________________

Before me personally appeared ____________________, with whom I am personally acquainted (or proved to me on the basis of satisfactory evidence), and who acknowledged that such person executed the foregoing for the purposes therein contained.

Witness my hand and seal at office this day of __________, 20___

____

Notary Public

*My commission expires:*_____________________________
~~~~~~

DRUG-FREE WORKPLACE AFFIDAVIT

STATE OF __________________

COUNTY OF ________________

The undersigned, principal officer of ______________________________, an employer of five (5) or more employees contracting with _____________ County government to provide construction services, hereby states under oath as follows:

1. The undersigned is a principal officer of ________________________________ (hereinafter referred to as the "Company"), and is duly authorized to execute this Affidavit on behalf of the Company.

2. The Company submits this Affidavit pursuant to T.C.A. § 50-9-113, which requires each employer with no less than five (5) employees receiving pay who contracts with the state or any local government to provide construction services to submit an affidavit stating that such employer has a drug-free workplace program that complies with Title 50, Chapter 9, of the *Tennessee Code Annotated.*

3. The Company is in compliance with T.C.A. § 50-9-113.

Further affiant saith not.

____

Principal Officer

STATE OF ________________________
COUNTY OF ______________________

Before me personally appeared ____________________________, with whom I am personally acquainted (or proved to me on the basis of satisfactory evidence), and who acknowledged that such person executed the foregoing affidavit for the purposes therein contained.

Witness my hand and seal at office this _____________ day of _______________, 20______

____

Notary Public

My commission expires:_______________________

OFFICE OF THE SULLIVAN COUNTY PURCHASING AGENT

BACKGROUND CHECK COMPLIANCE FORM

Contractors shall comply with Public Chapter 587 of 2007, as codified in Tennessee Code Annotated 49-5-413, which requires all contractors to facilitate a criminal history records check conducted by the TBI and FBI for each employee prior to permitting the employee to have contact with students or enter school grounds when students are present.

Any person, corporation or other entity who enters or any employee of any person, corporation or entity who enters into or renews a contract with a local board of education or child care program on or after September 1, 2007, must:

(1) Provide a fingerprint sample
(2) Submit to a criminal history records check to be conducted by the TBI and FBI.

TO BE COMPLETED BY RESPONDING CONTRACTOR

COMPANY or INDIVIDUALS (NAME) ____

ADDRESS ____

PHONE _________________ FAX _________________ LICENSE NUMBER/S __________________________

I agree to abide by Chapter 587 of 2007, as codified in Tennessee Code Annotated 49-5-413 and certify that I am authorized to sign. The undersigned further agrees if bid/contract is accepted, to furnish any/all Background Check Information on himself and all of his employees as required by law and/or at the request from the Office of the Sullivan County Purchasing Agent. I hereby agree to release all criminal history and other required information to Sullivan County, TBI and FBI in accordance with Tennessee law and further certify that all information supplied by me is true and accurate. I agree to release and hold harmless the above mentioned governmental entities for the use of this information related to the purposes mandated under Tennessee law. I further certify that I have obtained acceptable criminal history information on all current employees and will obtain said information on all future employees associated with the performance of work defined in the bid/contract, pursuant to TCA and that neither I nor any employee of the Company is prohibited from direct contact with school children for the reasons enumerated in TCA 49-5-401 et seq.

SIGNATURE ____ TITLE _____________________________

PRINTED NAME ____DATE _____________________________

TO BE COMPLETED BY NOTARY

STATE OF ______________________

COUNTY OF ______________________

Before me personally appeared ________________________________, with whom I am personally acquainted (or proved to me on the basis of satisfactory evidence), and who acknowledged that such person executed the foregoing for the purposes therein contained.

Witness my hand and seal at office this ____day of ______________, 20___.

____

Notary Public

My commission expires: ______________________________

IRAN DIVESTMENT ACT AFFIDAVIT

As per Tennessee Code Annotated, Title 12, and effective July 1, 2016:

By submission of this bid, each bidder and each person signing on behalf of any bidder certifies, and in the case of a joint bid, each party thereto certifies as to its own organization, under penalty of perjury, that to the best of its knowledge and belief that each bidder is not on the list created pursuant to §12-12-106.

____
Signature

____
Date