SECTION 28 10 00

ELECTRONIC ACCESS CONTROL/ INTRUSION DETECTION

Continental Access
A Division of the Napco Security Group
355 Bayview Avenue
Amityville, New York 11701
Phone (631) 842-9400
Fax (631) 842-9135

http://www.cicaccess.com

Email: sales@cicaccess.com

Specifiers: Click on the ¶ icon in the WORD toolbar to reveal detailed instructions

PART 1 - GENERAL

1.1 SUMMARY

A. Section Includes:

1. A general description, functional requirements, characteristics, and criteria present in the CardAccess 3000 Access Control, Alarm Monitoring & Video Surveillance System. The specification provides all necessary information to produce a complete proposal for a sophisticated, easy to-use, multi-tasking, multi-user Access Control System (ACS) with features that include, but are not limited to, Alarm Monitoring, Photo-ID Badging Management, Visitor Management, CCTV Integrated Management, DVR Integration, NAPCO Alarm and Fire panel Integration and Trilogy Networx wireless lock integration. Continental Access manufactures CardAccess 3000 (Version 2.x) Security & Management Software which includes all Computer Hardware and Software, Intelligent Control Panels, Communication Devices, Card Readers/Keypads, Access Cards, Key Tags, Key Fobs, I/O Boards & Power Supplies as specified herein. All material will be listed in Continental Access catalogs.
2. CardAccess shall perform a wide variety of feature-rich functions. These functions are categorized into 'system modules', (integration of products), which include, but are not limited to:
   a. Access Control Management
   b. Alarm monitoring Management
   c. Burglar Alarm and Fire Panel Integration
   d. Photo Imaging/Badging Management
   e. CCTV and Digital/Network Video Recorder (DVR/NVR) Integration
   f. Full Audit Trail Management report
   g. Muster Reporting
   h. Personnel Tracking Management Report
   i. Visitor Management
   j. Advanced Scripting (linking) Interface
   k. Building Lock Down
   l. Vehicle Tracking & Reporting
   m. Graphical Dynamic Maps: Import & Viewing & Executable
   n. Automated Data Import and Data Export
   o. Full Time & Attendance
   p. Trilogy Networx Wireless Lock Integration

3. Controller Hardware: Controller Hardware shall be of a distributed architecture nature so that in the event of server failure the local controller will make all decision utilizing both the Facility code and the unique ID and be capable of:
   a. 2 to 16 card readers per panel
   b. 1,000,000 card holders per panel
   c. Card formats ranging from 26 bit to 256 bits
   d. Processing data at 52 MIBS, (million instructions per second)
   e. Download speeds to the controller not to exceed 6 minutes for 100,000 card records utilizing the 200 bit format
   f. IPV IV and IPV VI Ethernet communications. Support AES 128/256 encryption
   g. Time zone offsets

h. Reporting alarms to a central monitoring station via Ethernet without the assistance of an integrated alarm panel
i. Changing addresses of inputs and outputs for door control
j. Global I/O functions Communications of Ethernet TCP/IP, RS 232, RS -422 or a combination thereof

4. System Requirements:
   a. This Host PC shall contain the ACS software GUI, Data Server, SQL database and the host communications software module. The SQL database shall be able to be located on a remote server, for improved performance. The communications software module shall be able to be located on a remote server/s, for improved performance.
   b. The Host communications software shall be required to be fully compliant with Microsoft Windows ® 2003 Server, Advanced Server, XP Professional, Win 7 and Win 2008 and operate as a true 32-bit or 64 bit system.
   c. The Host PC shall communicate with the Access Control Panels using Communication protocols such as TCP/IP, RS-422 and RS-232.
   d. The ACS shall be able to support both a Database server and a Communication server either as one computer or multiple computers.
   e. The Card Access shall be capable of supporting a Primary server and a Secondary server for disaster recovery systems and shall not be limited by distance from Primary to Secondary.
   f. The ACS workstation PC shall contain the software, the GUI, and integration executables only.
   g. The ACS workstation shall have the ability to enroll card data automatically.
   h. Security key will be required on all Host communication server PCs in order for the system to operate. Lack of security key on the Host PC will cause the communication software and the GUI to shutdown. The user will be notified of the missing security key by means of a popup message.
   i. The Security key shall be available as either a hardware or software key.
   j. Security key will not be required at workstations.
   k. The Security key will determine both hardware and software limitations:
      1) Hardware License Limitations: The key will determine the number of workstations that will be able to connect to the system simultaneously.
      2) Software License Limitations: The key will determine the additional software features that a user can activate. The features will include:
         a) Max # of Secondary Communication Servers
         b) Max # of CCTV DVR/NVR Servers
         c) Time & Attendance
         d) Visitor Management Integration workstations
         e) Max # of Scripting servers & Script editing capability
         f) Max # of Napco Integration Servers
         g) API Interface
         h) PIV support

5. Database Partitioning:

   ACS shall support SQLExpress/SQL 2005/SQL 2008 R2 database, and shall allow virtually unlimited database partitioning.

   a. Database Partitioning shall support the ability to assign the following to individual partitions:
      1) Cardholders
      2) Controllers
      3) Workstations
      4) Card Readers
      5) I/O points
      6) Alarm Panels
      7) Access Levels
      8) Time Zones
      9) Communications Servers
      10) Dynamic Maps
      11) System Operators

6. Access Control Panels:

a. The Access Control System (ACS) panels shall support, through firmware updates, full system integration, providing full system integration to standard burglary Alarm and Fire Panels with 32, 96, and 255 Zone Control. This shall allow reporting to Police, Fire Department, and to the ACS.

b. The following latest panels shall be available:
   1) Two 2 Door Intelligent Reader Control Panel
   2) Four Door Intelligent Reader Control Panel
   3) Eight Door Intelligent Reader Control Panel
   4) Sixteen Door Intelligent Reader Control Panel
   5) Expansion Modules:
      a) The ACS panels shall provide for full Supervised Alarm Input Expansion Modules (16 Supervised Alarm Inputs).
      b) The ACS panels shall support Relay Control Expansion Module (16 Form C Relay Outputs, and 8 Non- Supervised Inputs).
      c) The ACS I/O Board shall support up to 3 expansion boards, each provides 16 Supervised Inputs and 16 Relay Outputs, for a total of 48 each.

7. Additional Devices:
   a. The ACS Access Panels shall support the following Add-On devices:
      1) Personnel Identification Devices, including, but not limited to:
         a) Prox-Cards
         b) Smart-Cards
         c) Key Fobs,
         d) CHUID card
         e) CAC card
         f) TWIC
         g) FIPS 201-1 card
         h) Barcode
         i) Mag-Stripe Cards
      2) Access Authorization Devices, including, but not limited to:
         a) Keypads,
         b) Prox-Readers,
         c) Smart-Card-Readers and
         d) Biometric Identification devices
8. System Description:
   a. The Access Control Unit (ACU) is a fully programmable, self contained, [16, 8, 4 or 2] door system that offers users flexibility, expandability and simplicity.
   b. The system shall consist of all the hardware necessary to provide access control and alarm monitoring for all controlled entry/exit points within a single facility or multiple facilities.
   c. The system shall be a complete distributed processing system with no reliance on the host PC for any decision making.

B. Related Sections:
1. Section [28 16 00 - Intrusion Detection].
2. Section [28 23 00 - Video Surveillance].
3. Section [08 71 00 – Door Hardware].

1.2 REFERENCES

A. National Fire Protection Association (NFPA):
70-2011 National Electrical Code The standard for the safe installation of electrical wiring and equipment in the united states.

B. Underwriters Laboratories, Inc. (UL):
294-5th Edition The standard of safety for access control system units

1.3 SUBMITTALS

Refer to Section *[]*.

A. Product Data: Provide complete product data which shall include the following:
   1. Manufacturer's data for all material and equipment, including controllers, local processors, computer equipment, access cards and any other equipment provided as part of the ACU.
   2. A system description, including analyses and calculations used in sizing equipment required by the ACU. Description to show how the equipment will operate as a system to meet the performance requirements of the ACU. The following information shall be supplied as a minimum:
      a. Central processor configuration and memory size
      b. Description of site equipment and its configuration
      c. Protocol description
      d. Hard disk system size and configuration
      e. Backup/archive system size and configuration
      f. Start up operations
      g. System expansion capability and method of implementation
      h. System power requirements and UPS sizing
      i. A description of the operating system and application software

B. Shop Drawings: Provide complete shop drawings which shall include the following:
   1. Indicate all system device locations on architectural floor plans. No other system(s) shall be included on these plans.
   2. Include full schematic wiring information on these drawings for all devices. Wiring information shall include conductor routing, quantities, and connection details at devices.
   3. Include a complete access control system one-line, block diagram.
   4. Include a statement of the system sequence of operation.

C. Functional Design Manual: The functional design manual shall identify the operational requirements for the system and explain the theory of operation, design philosophy, and specific functions. A description of hardware and software functions, interfaces, and requirements shall be included for all system operating modes.

D. Hardware Manual: The manual shall describe all equipment furnished including:
   1. General description and specifications
   2. Installation and check out procedures
   3. System layout drawings
   4. Manufacturer's repair parts list indicating sources of supply

E. Software Manual: The software manual shall describe the functions of all software and shall include all other information necessary to enable proper loading, testing, and operation. The manual shall include:
   1. Definition of terms and functions
   2. Use of system and applications software
   3. Initialization, start up, and shut down
   4. Alarm reports
   5. Reports generation
   6. Data base format and data entry requirements

F. Operator's Manual: The operator's manual shall fully explain all procedures and instructions for the operation of the system. The document shall be available on CD in electronic format and include:
   1. Computers and peripherals
   2. System start up and shut down procedures
   3. Use of system, command, and applications software

4. Recovery and restart procedures
5. Graphic alarm presentation
6. Use of report generator and generation of reports
7. Data entry
8. Operator commands
9. Alarm messages and reprinting formats
10. System access requirements

G. Maintenance Manual: The maintenance manual shall include descriptions of maintenance for all equipment including inspection, periodic preventive maintenance, fault diagnosis, and repair or replacement of defective components.

H. As Built Drawings: The Contractor shall maintain a separate set of drawings, elementary diagrams, and wiring diagrams of the ACU to be used for record drawings. This set shall be accurately kept up to date by the Contractor with all changes and additions to the ACU. In addition to being complete and accurate, this set of drawings shall be kept neat and shall not be used for installation purposes.

1.4 QUALITY ASSURANCE

A. Regulatory Agency Sustainable Approvals
1. NFPA 70 National Electrical Code
2. UL 294 Access Control System Units

B. Qualifications
1. Manufacturers:
   a. The manufacturers of all hardware and software components employed in ACS shall be established vendors to the access control/security monitoring industry for no less than ten (10) years.
2. Suppliers:
   a. Only the manufacturer's equipment that is explicitly mentioned in this specification is supplied. Substitutes are not allowed.
   b. Equivalence: No item shall be substituted without the prior written and approved documentation that assures that the substituted part/parts are exactly the same, technically and aesthetically speaking. The substituted parts must provide the same or significantly improved performance.
3. Installers/Applicators/Erectors:
   a. Dealers:
      1) All bidders must be a Certified Access Control Integrator by the manufacturer.
      2) All technicians and engineers involved in the project must be trained and certified on the ACS software and associated interfaces by the manufacturer prior to the bid.
      3) All bidders must have 5 years installation experience on the ACS product lines.
      4) The Integrators of the ACS products shall have been in the Access Control business for a minimum of 15 years, and have supplied access control systems/components of similar configuration, size and complexity.
      5) All bidders must maintain a technical support group for providing round the clock technical assistance.
   b. Contractors:
      1) The contractor of the access control system will meet the following requirements:
         a) He will have had a minimum of 5 years of experience in installing, commissioning and supporting access control systems of similar size, configuration and complexity.
         b) He will have at least two technical staff members who have been trained and certified by the manufacturer to install and support this system.
         c) He will maintain an adequate supply of replacement parts for all system components installed, as recommended by manufacturer.
         d) The installing contractor shall be responsible for the following:

i. Determining operational requirements and planning/designing the system.
ii. Installing and integrating Access Control, Alarm Monitoring, Alarm Systems, DVR/NVR, Time and Attendance, Visitor Management interfaces and related security and door hardware.
iii. Configuring local access panels and ACS host communications.
iv. Installing proper communication connections between the host system, access panels, and the related hardware.
v. testing the security management system communication and operation.
vi. Training system operators.
vii. Testing the security management system

e) The subcontractor shall have been regularly engaged in the installation and maintenance of integrated access control systems similar in size and scope to that is outlined herein for a period of no less than five (5) years.

f) The subcontractor shall supply manufacturer's documentation attesting to the fact that his/her firm is a competent factory trained service branch capable of maintaining the system with reasonable service time.

g) The subcontractor shall provide a minimum of three (3) references whose systems are of similar complexity and have been installed and maintained by the subcontractor in the last five (5) years.

h) There shall be a local representative and factory authorized local service organization, which will carry a complete stock of parts and provide maintenance for these systems. Local shall be defined as an area in a [ ] mile radius of [ ] with a response time of [ ] hours.

4. Alternates:
   a. Only the manufacturer's equipment that is explicitly mentioned in this specification is supplied. Substitutes are not allowed.
   b. Equivalence: No item shall be substituted without the prior written and approved documentation that assures that the substituted part/parts are exactly the same, technically and aesthetically speaking. The substituted parts must provide the same or significantly improved performance.

1.5 DELIVERY, STORAGE & HANDLING

A. Ordering: Comply with manufacturer's ordering instructions and lead time requirements to avoid construction delays.

B. Delivery: Deliver materials in manufacturer's original, unopened, undamaged containers with identification labels intact.

C. Storage and Protection: Store materials protected from exposure to harmful weather conditions and at temperature and humidity conditions recommended by manufacturer.

1.6 WARRANTY

A. The Access Control Panel shall be warranted for at least 12 months from the date of system acceptance.

B. Extended warranty terms at reasonable rates shall be available from the installing dealer.

C. The system integrator shall be the focal point of all service issues or questions (with the manufacturer's full support). The system integrator shall directly support software for the selected system product family.

D. Technical support from the manufacturer to the system integrator will not be reliant on a software maintenance agreement between the system integrator, end user to the manufacturer.

PART 2 - PRODUCTS

2.1 MANUFACTURERS

A. Manufacturer List:
1. Continental Access (A Napco Security Group Company)
   355 BayView Ave, Amityville, N.Y. 11701;
   Telephone: (631) 842-9400;
   Fax: (631) 842-1961;
   Website: www.cicaccess.com.
2. Alarm Lock (A Napco Security Group Company)
3. Napco (A Napco Security Group Company)
4. Salient
5. CA View
6. Que Accounting
7. Stopware
8. Fargo
9. EPISoft
10. Code Bench

2.2 SERVER CONFIGURATION

A. Server PC Requirements**:** Minimum Server PC requirements shall be as specified in the table below:

	Server (1-4 Workstations)	**Server (5-19 Workstations)**	**Server (20-49 Workstations)**
Processor	Pentium Dual Core, 2.6GHz (min)	Xeon Quad Core 2.0GHz (min)	2 x Xeon Quad Core 2.0GHz (min)
Ram	2.0 GB Min/ 3GB+ for Win7 and Win Server 2008	4.0 GB Min	8 GB Min
Hard Drive	300 GB	500 GB	Raid 5 - 3 drives minimum
USB Ports	4 Min	4 Min	4 Min
Serial Ports	Optional - 1 expandable to 64	Optional - 1 expandable to 128	Optional - 1 expandable to 128
Parallel Ports	Optional - 1	Optional - 1	Optional - 1
Mouse	PS2 or USB	PS2 or USB	PS2 or USB

Monitor	17" SVGA (1024x768)	17" SVGA (1024x768)	17" SVGA (1024x768)
DVDROM	48x/16x	48x/16x	48x/16x
DVDR	24x/8x	24x/8x	24x/8x
Sound	Optional but Stand-Alone recommended	Optional	Optional
Network Card	100/1000 Mb NIC Ethernet	100/1000 Mb NIC Ethernet	100/1000 Mb NIC Ethernet
Operating System	Win XP Pro w/SP3, Win 7 Pro 32/64 bit, Win 2003 Server 32/64 bit, or Win 2008 Server 32/64 bit.	Win XP Pro w/SP3, Win 7 Pro 32/64 bit, Win 2003 Server 32/64 bit, or Win 2008 Server 32/64 bit.	Win XP Pro w/SP3, Win 7 Pro 32/64 bit, Win 2003 Server 32/64 bit, or Win 2008 Server 32/64 bit.
Database	MSSQL 2005/2008 R2 Express or MSSQL Server 2005/2008 R2 for higher performance	MSSQL Server 2005/2008 R2 recommended	MSSQL Server 2005/2008 R2 recommended
Backup	Tape / CD / DVD / Network	Tape / CD / DVD / Network	Tape / CD / DVD / Network
System Size	This is the recommended PC server specification for a system with up to four workstations. It can be used for a stand-alone system, a workstation or a CA3000 Server. For high transaction environments some specifications may change.	This is the recommended PC specification for a CA3000 Server supporting up to nineteen workstations. For high transaction environments some specifications may change.	This is the recommended PC specification for a CA3000 Server supporting up to forty nine workstations. For high transaction environments some specifications may change. For larger systems please consult with Continental Access.
Notes:	(1) If using SQLExpress, the database size should not exceed 4GB. (2) Disk drive usage is dependent on the number of transactions kept in backup. (3) Additional RAM will improve performance (4) It is best to perform badging and other integration functions on a workstation, not the server.		

2.3 SYSTEM DESCRIPTION

A. The Access Control System (ACS) shall be capable of:
   1. Managing the security operations for a single site or for multiple sites.
   2. It shall consist of all the software and hardware necessary to provide access control and alarm monitoring for all controlled entry/exit points within a single facility or multiple facilities.
   3. The system shall provide full access grant or deny access authorization capabilities without the need for real-time communications with the control panels.
   4. The system will monitor alarm events and display them to the system operator for processing.

B. The system shall be designed such that entry/exit points may be added in [one, two, four or eight door] increments.

C. The system shall provide full system integration to ACS, CCTV, third party DVR/NVR Digital Video Management, Alarm and Fire panels, Time and Attendance, Visitor Management, Trilogy Networx Wireless and Data Exchange services. The system shall allow reporting to Police, Fire Department, and to the ACS.

2.4 SYSTEM SPECIFICATIONS

A. High resolution graphics:
   1. The system shall support unlimited high resolution graphics with Disk-Limited and user-programmable color dynamic graphic map display capable of showing floor plan, location of alarm device, and alarm instructions.
   2. The mapping software shall be able to run independent of the ACS software.
   3. The independent dynamic mapping software must utilize the same database as the ACS software.
   4. Floor plans shall be created in .JPG, .BMP, .emf, .wmf or .ico formats, and can be imported from other systems.
   5. All of the graphic maps will be displayed on the CPU monitor. Systems requiring separate display monitors or PC's to display the floor plans will not be acceptable. The operators must be able to perform the falling functions without use of the ACS software:
   6. Add and delete devices on the dynamic maps
   7. Make custom icons as devices and add to the dynamic maps
   8. Open up live video on the dynamic maps by right clicking and choosing live video
   9. Unlock and lock doors from the dynamic maps
   10. Turn on/off devices from the dynamic maps
   11. Respond to alarms from the dynamic maps
   12. Add and delete dynamic maps according to permissions by operator log on
   13. Utilize a Log On that is identical as the Log On given by the system administrator for the ACS with all permissions that were assigned and all restriction that were assigned.
   14. All events/action shall become part of the ACS transactional history database

B. Information Storage: All programmed information as well as transactional history will be automatically stored onto a local or remote hard disk for later retrieval. The system will warn the operator when the database size approaches maximum capacity. The system shall be capable of using multiple ACS site databases as needed by the system users.

C. Information Archive/ Retrieval: The CPU shall be capable of transferring all programmed data and transactional history to any removable media or logical disk drive. All programmed data can be restored from disk/CD, Tape Drive etc, in case of system hardware failure. As an option, the system shall be able to offer additional support by means of a redundant mirrored system backup retrieval, for virtually instantaneous switchover in an emergency. There shall be no distance limitation for the secondary server to the primary server.

D. Communication: The system shall be capable of supporting the following communication types:
   1. Serial Port type (RS232/RS422) connections
   2. LAN/WAN (10/100/1000) Hard-wired & Wireless connections
   3. Fiber Optics
   4. TCP/IP IPV IV and IPV VI protocols

   Note: A Host Server shall be able to employ any combination of the above communication types.

E. COM Port/Serial type (RS232/RS422) Connections:
   1. The PC shall have a minimum of two serial ports.
   2. The system (consisting of a Host and 7 Remote COM Servers) shall be able to support up to 2048 Com ports, each Com Server supporting 256 Ports. In case all of the 256 ports are to be used for serial communication, you need to employ Com Port expansion cards. Each expansion card will be able to provide expansion in increments of 32 Com Ports.
   3. Each com port will be able to support hard wired direct connect or modem connections. An additional 256 ports per Host or Com Server can be used for modem specific ports, for up to 512 total ports.
   4. Each COM port must be able to have password protection as an option.
   5. The system operator will be able to enter a password for each COM port.

6. When operating in this mode, the ACS door controllers will not accept communications from any host PC, workstation or communications server that does not provide the correct password.
7. The system operator will be able to individually assign this password to selected panels.
8. The COM port password will be encrypted both in the system database and in the Access Control Panel.

F. LAN/WAN (10/100/1000) & Fiber Optics Communications:
1. The Host PC shall support LAN (local area connection).
2. The system (consisting of a Host and 7 Remote COM Servers) shall be able to support up to 2048 LAN ports, each Com Server supporting 256 LAN Ports.
3. Each port shall support typical Cat 5 LAN Connection or Fiber Optics LAN connections.
4. Each LAN port shall be able to have password protection.
5. The system operator will be able to enter a password for each LAN port
6. When operating in this mode, the ACS door controllers will not accept communications from any host PC, workstation or communications server that does not provide the correct password.
7. The system operator will be able to individually assign this password to selected panels.
8. The LAN port password will be encrypted both in the system database and in the Access Control Panel.

G. Printers: The system shall support page printing of reports by any page printer that can be installed, configured and supported by the Microsoft Windows ® operating system. The system shall also support printing of alerts or any events above a user selected priority.

H. Mouse: The ACS shall use PS/2 or USB mouse configured under and supported by the Microsoft Windows ® operating system.

I. Workstations: The system shall support up to 150 additional active remote workstations. These stations shall be capable of monitoring alarms, running CCTV Integration, DVR Integration, Alarm and Fire panel integration, Scripting, Video Badging, Time and Attendance and Visitor Management. Video Badging Full integration shall use the same SQL database and hence no multiple entries will be needed. The ACS Management software shall overlook all database administrative tasks, of all system workstations including:

J. Access Control Management
1. Alarm monitoring Management
2. Burglar Alarms and Fire Panel system Management Integration
3. Photo Imaging/Badging Management
4. CCTV Integration Management
5. System Administration Management (except archiving)
6. Personnel Tracking Management Reports
7. Visitor Management
8. Conditional Badging Management
9. Muster System Management ('Who's IN' report)

K. Networking: The system shall provide networking operation via local area networks (LAN) or Wide area networks (WAN), both wired and wireless (802.11g standard), using the standard features of Microsoft Windows ® 2003/2008, XP Professional or Windows 7 networking software.

L. Licensing: The ACS shall offer you the following licensing options:
1. The system shall provide one Server license.
2. Client/user workstation licensing for [5, 10, 25, and up to 150] workstations shall be available as an option.
3. Additional licensing for up to 7 additional COM Servers shall be available as an option.
4. The system shall support concurrent usage of all system workstations as per the license limitations. System operators will be able to perform independent functions on each workstation. The system allows access to only one particular table for additions, deletions or editing, one user at a time.

M. Database:

1. The database shall be Microsoft SQLExpress (Database Engine) or optionally Microsoft SQL Server 2005/2008 R2.
2. It shall be scalable. Systems initially installed using Microsoft MSDE/SQL shall be field upgradeable to Microsoft SQL Server 2005/SQL 2008 R2.
3. The database will fully integrate with the Government PKI database for validation of a card and automatically remove access privileges when the card holder information is moved to the Government Revocation list.

N. Access Control Panel: The Access Control Panel system shall be scalable and operate efficiently over a wide range of facility sizes and applications. Systems utilizing a remote module at the door that reports back to the controller will not be accepted. The Access Control Panels shall be capable of:
1. Entry/exit points will be able to be added without the need to replace any system hardware or controllers.
2. Controllers may be selected and added in increments of [1, 2, 4, 8 or 16] door configurations to provide the maximum flexibility and cost effectiveness.
3. Distributed, intelligent, fully independent controllers will be able to be used to provide fully distributed decision and authorization capabilities.
4. In the event the host PC cannot communicate with any/all controllers, no degradation in security shall occur.
5. Reading multiple cards formats simultaneously with no degradation of “time to unlock”.
6. Multiple reader formats/readers shall be read at a single controller simultaneously.
7. Reading bit structures from 26 bit to 256 bits.
8. Storing up to 1,000,000 card holder records.
9. Reading the FIPS-201-1, PIV, TWIC and CAC card formats.
10. Shall be capable of Time Zone Offsets for those panels deployed in different time zones.
11. Unlock times not to exceed .5 seconds after a valid card read.
12. Download speeds to be at 921 kbps allowing for 40,000 cards to be downloaded in less than two minutes.

2.5 SOFTWARE CAPACITIES

A. System software and language development software exist, and are industry accepted, allowing the customer to choose the Language desired by the user. There can be full customization of the following:
1. Software GUI Screens.
2. Icons.
3. Communication messages, and Reports.
4. The Operating system shall be 32 bit multi-user / multi-tasking capable of operating in a non-proprietary CPU.
5. The application software shall be written in a standard, industry accepted language. All System functions shall be accessible via Microsoft Windows ® XP Professional compliant menu-accessed screens. Systems requiring command string control or complex syntax will not be acceptable. Systems shall not be dependent upon external input, other than keyboard.

B. Each system shall be capable of supporting:
1. Over 2000 Serial/LAN Communication Ports and over 4000 Ports Total.
2. Over 32,000 Readers.
3. Unlimited Cardholder database (SQL Version-limited only to Hard drive capacity).
4. 150 Workstations.
5. 255 Time Schedules each w/least 10 start/stop intervals.
6. 5 Holiday types with 100 user-definable holidays each (500 Total).
7. Unlimited System operators.
8. 30,000 access levels per panel.
9. Over 256,000 supervised inputs.
10. Over 256,000 relay outputs.
11. Over 16 thousand global link (output) programs.

12. Up to 10 facility codes per Access Control Panel or 100,000 system facility codes per panel with Facility Code/Badge Concatenation.
13. Unlimited operator passwords with definable privilege levels.
14. Unlimited .wav files for alerts
15. Unlimited color dynamic graphic maps.
16. Unlimited RS-232 interface ASCII commands to a CCTV system, which provides automatic, alarm activated camera switching, and Live Camera image Capture.
17. Unlimited number of floors for Elevator Control.
18. Cardholder activation/cancellation dates.
19. Unlimited number of CCTV DVR Servers.
20. Unlimited number of CI Scripting(linking) Servers.
21. Unlimited number of Napco Alarm Servers.
22. Unlimited number of Time Zone Offsets.

2.6 SYSTEM SECURITY

A. Password: The system software shall be capable of identifying unlimited temporary or permanent operators. Passwords may be up to 20 alphanumeric characters, and will be case sensitive.
   1. Password Security: Permanent passwords will be able to be provided only by the operators. The administrator may only provide a temporary one-use initial password, which must be changed by the operators, when they log on. Operators will be allowed to change their passwords any time. Operator password invalidation will be required in cases of suspected operator security breach (which can occur when the operator is not on site or is otherwise unable to logon) in order to enforce immediate change of password. When an administrator adds a new operator, the concerned operator's password may not be left blank and must be set to a temporary value that can be used only once. When a temporary password has been provided by the administrator, the New Password dialog will be displayed after the temporary password has been entered.
   2. An operator record will be required to have a unique name, to allow the use of same passwords by different operators. If duplicate passwords are not allowed, security can be compromised. For example, a 'password already in use' message will reveal one of the existing passwords, which is of course a security violation. No secret information is revealed by saying, 'Operator name already in use, please enter a different name'.
   3. The system administrator will have the capability to require an operator to change his/her password. The system administrator may invalidate the operator's password. The operator will then be required to provide a new password during his next logon.
   4. System Operators will have the ability to change any workstation settings, from whichever station they are working on.
   5. The system administrator may assign an operator to a group. As a result, the operator will be able to view/ change and create items that are assigned to the particular group only.
   6. The system will record in the Audit Trail database, the time at which an operator logs into/out of the system, as well as any changes that were made by the user during login.

B. System Operators:
   1. Privilege levels: Each operator will be able to be assigned any combination of up to 100 user programmed privilege levels. Operator Control will be limited by the following access rights:
      a. Disable
      b. View Only
      c. Create Only
      d. Create and Edit

C. Personnel Database Security: The system administrator will be able to restrict each operator's privileges to View, Create or Create/Edit each field in the Personnel database.

D. Audit Trail of Database Changes:

1. The system shall record changes to the database, including the date, time, operator name and description of the record changed.
2. The audit trail shall track event messages record additions, deletions and revisions. The record will contain a date/time stamp for the change, the logged on operator's name, table name, action identifying the change, and a description based on the 'Name' field of the record such as, user name, operator name, panel name, reader/door name and workstation where the change was made.
3. The system shall allow for browsing of Audit Trail. The dialog box will contain a database grid component that will display the records of the Audit Trail Table.
4. The system shall NOT allow the Audit Trail table to be edited.

2.7 SOFTWARE SPECIFICATIONS

A. The system shall integrate with various facility management functions such as:
   1. Burglar and Fire Alarm Panel
   2. CCTV Cameras
   3. HR interfaces
   4. Government PKI databases
   5. Time and Attendance
   6. Asset Tracking
   7. CCTV DVR recording devices so that, all available functions may be controlled from any ACS workstation connected to the network

B. The system shall be capable of handling large multi-site corporations across Local (LAN) and Wide Area Networks (WAN) while utilizing AES 128/256 bit encryption.

C. The system software shall be true 32 bit software.

D. The system shall support both Microsoft SQL Express and Microsoft SQL 2005/SQL 2008 R2. Microsoft SQL Express is the system default. But, Microsoft SQL 2005/SQL 2008 R2 shall be available as an option.

E. The system shall support multiple languages offering the following privileges.

F. The system operator will be able to select the desired language from a pull down list of available languages.

G. The system shall be able to remember individual operator settings and automatically switch to the appropriate language for the logged on operator.

H. The system shall support use of different languages at each workstation.

I. The system shall be capable of switching between languages without the need to re-boot the system.

J. Communications: In addition to the normal hardwired configurations, the system shall allow selection of all modes of polling, (LAN/WAN, Hardwire, Wireless network, and Dial up) if needed from one single host server, allowing for a combination of polling modes. The System shall allow full flexibility of controller polling from the Host server, and also shall allow an additional Remote Com server (Network LAN/WAN) for remote polling. The system shall support the following alternative communications modes:
   1. Network:
      a. All communications shall be capable of AES 128/256 bit encryption
      b. The system shall have the capability to communicate with system controllers from the Host PC on the network via a Local (LAN) or Wide Area Network (WAN). Multiple communications servers may be run concurrently within the system utilizing AES 128/256 bit encryption.
      c. Controllers communicating over a network via LAN/WAN will be able to be password protected.
      d. Controllers shall have the capability of having two Ethernet connections. One being primary and one being secondary for redundant communications paths.

2. Dial IN/OUT:
   a. When operating in dial mode, the system shall automatically download to the controllers any changes that may be made to the configuration or operational databases.
   b. It will be possible to schedule uploads and downloads in accordance with the following schedules. The modes may be mixed.
      1) By schedule: At any time a schedule previously programmed into the system may be used to initiate a dial-out to the controller.
      2) On The Hour: A dial-out may be automatically initiated each hour, on the hour.
      3) Twice Daily: Dial outs to the controllers may be initiated twice daily, one at Noon and the other at midnight.
      4) Daily: A dial out may be initiated each day at noon-time.
         a) It will be possible for the system operator to initiate a manual dial out connection to any controller connected via telephone line, at any time.
         b) Controllers connected to the system via telephone lines may initiate dial in connections to their host PC in case they detect alarm events that have been previously programmed as high priority events.
         c) Controllers connected to the system via telephone lines may initiate dial in connections to their host PC in case the controller (Access Control Panel) transaction buffer is 75% full.
         d) Controllers being communicated with over telephone lines will be able to be password protected.
         e) The system shall support a minimum of two dial-out lines.
         f) The system shall support a minimum of two dial-in lines.

2.8 SYSTEM SOFTWARE FEATURES

A. Anti-Pass back:
   1. The system shall support the following modes of anti-passback:
      a. Global System Wide Anti-Passback: The user may enter at any IN reader and/or leave using any OUT reader in the system. Up to 250 + Anti-Passback areas shall be supported.
      b. Hard Anti-Pass back: The cardholder will not be able to use his/her card consecutively at either an In or an Out reader. Doing so will generate an event message and the system will deny access to the cardholder. The cardholder must be In before swiping Out, and vice-versa.
      c. Soft Anti-passback: Will allow the cardholder to access an (In) or (Out) door consecutively, but the system will generate an error message.
      d. Duration Use (timed) Anti-Passback: The system shall have the capability to restrict the use of an In or an Out reader for a particular card-holder, for a certain duration of time. When applied to an APB type reader, this duration will determine the amount of time (minutes) that a badge that is in APB violation, will be rejected. If a badge is rejected due to APB violation, the use of this badge in the same direction-type reader will continue to be rejected until the duration use time expires. After the expiration, the badge holder will be permitted passage at the reader.
      e. Nested Anti-Passback: The system shall support multiple zones of anti-passback within the same building I.E. Independent zones of anti-passback where one in read from one zone does not affect another zones setting.
      f. APB Reset: The system shall be capable of a global reset of all cardholders in the system. This can be done by schedule, or manually.
      g. Nested Anti-Passback: The system shall be capable of nested anti-passback.

B. Dedicated Access:
   1. The system administrator will be able to assign one or more readers to Badgeholders individually.
   2. The personnel database supports the assignment of unique groups of doors and time schedules to each badge holder.

C. Database Partitioning:

1. The system shall support partitioning of database. System administrators will have the capability to restrict operators from viewing, adding, editing or deleting data, or system configurations.
2. The system shall support the assignment of multiple operators to the same database partition.
3. Database Partitioning should allow the administrator to assign each Operator Privilege to the followings folder tabs:
    a. Forms Control: This tab shall provide access to all system database menus and menu items dependent on operator privileges. The menus and their items at minimum are:
        1) System
            a) Language
            b) System Settings
            c) Achieve/ Restore
            d) Audit Trail
        2) Control
            a) Doors
            b) Relays
            c) Links
            d) Disable Alerts
            e) Schedule Changes
        3) Access
            a) Personnel
            b) Badge Holders IN (Muster)
            c) Access Groups
            d) Find Usage
        4) Administration
            a) Badge Formats
            b) Facility Codes
            c) Photo ID
            d) Schedules
            e) Holidays
            f) Groups
        5) Operators
            a) Operators Privilege
            b) Operators Response
            c) Operator Instructions,
            d) Operator Instruction Links
            e) Maps
        6) Configuration
            a) Panels
            b) Readers
            c) Inputs
            d) Relays
            e) Links
            f) Com Ports & LAN WAN (IP Address)
            g) Modems
            h) DVR server
            i) Napco Server
        7) View
            a) Toolbars
        8) Help
            a) CardAccess 3000 Help
            b) About CardAccess 3000
        9) Alert Signal Menu
            a) Silence
        10) Control Menu
            a) Control Devices
        11) Status Menu

a) Remove Entry

12) Remove Station Menu
    a) Remove Off- Line Workstation
13) Personnel Fields Control:
    a) Batch Modify
    b) Access Time
    c) Access Group 1
    d) Access Group Expire Date
    e) Access Group 2
    f) Access Group 2 Expire Date
    g) Access group template
    h) APB In
    i) APB Out
    j) APB Exempt
    k) APB Set Next
    l) APB Settings
    m) Activation Date
    n) Badge Number
    o) Badge Photo Type
    p) Capture Signature
    q) Company ID
    r) Department
    s) Duration Use
    t) Embossed
    u) Enabled
    v) Escorted
    w) Expiration Date
    x) Facility Code
    y) First Name
    z) Group
    aa) Hire Date
    bb) Initial Download
    cc) Last Access
    dd) Last Name
    ee) License
    ff) Location
    gg) Phone
    hh) Phone Extension
    ii) Photo Modify
    jj) Photo Import
    kk) Photo Preview
    ll) Photo Print
    mm) Photo Export
    nn) Clear Photo
    oo) Clear Signature
    pp) Pin (Keypad Pin Number)
    qq) Print Photo Copies
    rr) Re-Issue
    ss) Remarks & Note Field
    tt) Shunt Group
    uu) Shunt by Reader
    vv) Shunt Inactive
    ww) Shunt Shunting
    xx) SSN (Social Security)
    yy) Stay On Panel
    zz) Supervisor

aaa) Tracked
bbb) Badge Use Limit
ccc) User Field 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12 thru 48
ddd) Vehicle Tag
eee) Dedicated Access Group Name
fff) Dedicated Access
ggg) Dedicated Access Group Assignment
hhh) Vehicle

14) Database Partitions: This tab should allow partitioning of all system database groups below:
a) Personnel Group
b) Panels/Door Controllers Group
c) Readers Group
d) Alarm Inputs Group
e) Relay Outputs Group
f) Links (If Than) Macros type Group
g) Access levels Group/Groups
h) Time Schedules Group
i) DVR's/CCTV
j) Napco panels

D. Vehicle Tracking:
1. The system shall support tracking the use of a vehicle by a particular operator.
2. The system administrator will be able to link a particular vehicle to a particular vehicle operator.

E. Event Printing: The system shall support printing of alerts or any events above a user selected priority.

F. Printer Types: The system shall be capable of supporting three types of printers.
1. Report Printers: Reports requested by the operators will be sent to these printers. These printers may reside anywhere on the network.
2. Event Printers: Individual events will be routed to any of the event printers in real time.
3. Dye-sublimation Video Badging type of printer: These can be single/double sided printers. The system software shall support many different printer driver manufactures, and will be compatible with any of the following Continental Access printer models:

G. Scheduled Reports:
1. The system shall be capable of running unattended scheduled reports, automatically. Operator intervention shall not be required.
2. The system shall support the creation of report templates. These templates will be saved by the system for repeated retrieval and use by the system operators.

H. Badge Validator (Enable/Disable):
1. The system operator will be able to program a reader as a 'Badge Validator reader. Badges presented to this reader are automatically enabled or disabled on consecutive card swipes.

I. Auto Acknowledge Priority Set Point:
1. The system operator will be able to set a priority level between 1 and 99 as an automatic acknowledge point.
2. All alerts that have been assigned a priority lower than the set point will be automatically acknowledged by the system.
3. The system operator will be able to easily modify this set point as well as, enable or disable it.

J. Groups:
1. The system administrator will be able to perform manual control based on groupings of Personnel, Panels/Controllers, Readers, Inputs, Relays and Links.

2. The system administrator may assign one or all of these items to named groups. The system operator will be able to select any/all of these items by selecting the name of the desired group, and perform system functions in a 'batch mode' on all of them.
3. The system administrator may partition the system using Groups.

K. Access Group Templates:
1. The system administrator will be allowed to select any existing access group and use that group as a template for creating a new similar access group.

L. Default Relay and Input Assignments:
1. The system shall provide default settings for relay and input assignments. This default programming will be populated each time a reader is programmed.
2. The system shall allow the operator may choose to modify these default settings as required.

M. Import:
1. The system shall support importing of personnel data from other databases.
2. The system shall be capable of recognizing any flat file that contains ASCII data.
3. The operator will be able to select the field separation character.

N. Export:
1. The system shall support exporting of all system events. The operator will have the option of selectively exporting any/all event record types.

O. Auto Import/Export:
1. The system shall support automatic import/ export of data to and from the ACS database. The system operator may set up specific files to 'import (from)' or 'export (to)'. These files may be on a local drive or network drive.

P. Elevator Control:
1. The system shall be capable of controlling access to building elevators by making use of Access Groups with no special controller being used.

Q. Archive and Restore of Data:
1. Data Archive:
   a. The system shall allow archiving of the data required to configure the system. The operator will be able to choose to archive all configuration data or, selectively back up this data by category.
   b. The operator will be able to archive events as well. The entire Events data will be able to be archived or, only select event types can be backed up based on a period of time.
   c. The system shall offer the option of storing the archived events/configuration data in the local database or, in a database present on a remote site.
   d. The operator shall be capable of setting up archive database backups by a schedule for automatic backups.

2. Data Restore:
   a. The system shall allow restoration of all previously archived data. The operator will be able to restore all configuration data or, restore only select data by category.
   b. The system shall allow the administrator to restore data from any location where an archive was previously done, and will still be available to the system via network connection.

R. Scheduled Changes:
1. The system shall be capable of scheduling time changes to Readers, Inputs, Relays and Links, automatically. The system will be able to execute these scheduled changes without the need for operator intervention.
2. The system also shall provide the operator the flexibility to control the scheduled change by a single device or a 'Group' of devices.

3. The system operator may program these changes for the current year or any year in the future that the operating system can support.

S. Badge Holders IN (Muster List):
1. The system shall be capable of providing a list of all badge holders currently logged as IN the building.
2. The list shall include the Name, Location and Time of the badge holders' last IN transactions.
3. The default readers for this list shall be all readers. The operator will have the privilege of selecting any reader in the system for the list, provided, the reader has been programmed to report 'In' and 'Out' events.
4. The operator shall be able to print a report of this list directly from the Badgeholders IN screen to any printer on the system or it can be generated automatically in response to an event or input.

T. Find Usage:
1. The system shall enable the administrator.
   a. To determine the time schedules and access groups that will be contained within a particular Access Control Panel.
   b. To determine the exact counts of badges, access groups and time schedules that will be contained within a particular Access Control Panel.
   c. To determine the presence of any Time Schedules or Access Groups that will no longer be used by the system.

U. Badge Formats:
1. The system shall accommodate various badge data formats, simultaneously, by allowing the system operator to enter into the system, the information about the data contained within a particular badge.
2. The system shall support multiple badge formats, simultaneously.
3. The Badge Format function shall support American Banking Association (ABA), FIPS 201-1, PIV II, CHUID TWIC and Wiegand data formats.
4. The system software shall have the capacity to download a minimum of ten (10) user defined badge formats to each panel. These formats will allow for the use of several card technologies, simultaneously. Alternately, the system shall support 100,000 system facility codes per panel with Facility Code/Badge Concatenation.

V. Alarm Monitoring Management and Alert Processing:
1. The system shall support 99 levels of alert priority. The system administrator will be able to assign these priorities uniquely to any alert or event in the system.
2. The administrator may partition the events by user. Only events from the panels and readers in the operators' partition will be viewable.
3. Each priority will be uniquely identified by color that is hard-coded in the software.
4. The alert display screen will be divided into two sections.
   a. Those alerts requiring intervention by the system operator will be placed in the 'Pending Alerts Grid'. These events will remain in the Pending Alerts grid until such time the operator makes a determination, or the system Auto-Acknowledge function determines that the event should be automatically acknowledged by the system. When an event is auto-acknowledged, the system will append to the event record the date and time the event was auto-acknowledged, the operator that was logged on, and an indicator that the event was auto-acknowledged.
   b. Alerts not requiring operator intervention will be placed directly in the 'Events Grid'. The Events grid allows the operator to view the current and past events.
5. The system administrator will be able to force the operators to enter a response for each event the operator processes. The administrator may predefine response messages which the operator may choose from, or the operator can enter his/her own response.
6. The Events grid will contain button controls for sorting and viewing of events. The buttons will be:
   a. Recent: This button will display the most recent / latest events. (This can be set per user).
   b. Browse Mode: Once the user has logged in, the system shall automatically put the Events grid in Browse. This mode will 'freeze' the event screen for browsing.

c. Previous/Next: When sorting on a header there will be two buttons (PREVIOUS) and (NEXT). The Previous button will display the previous day's transactions. The Next button will advance you to the next day's events.
d. Photo/Map: If the Photo/Maps option is enabled, the system should automatically display each user's photo and/or map.

7. Each alert record will provide the following information:
   a. Class, Description, Location, Date, Priority, and Operator that acknowledged the alert and the time it was acknowledged either through the ACS software or the ACS stand alone map software directly on the Map.
8. Alarm Description: Each alarm point may be defined with a plain text description of up to 40 characters.
9. Alarm Enabling: Alarm points will be enabled during user-definable time schedules and they can be manually silenced from any workstation.
10. Additional Alarms: The system shall also generate alarms for the following:
    a. Enclosure tampering
    b. Access Control Panel communication loss/restore
    c. Alarm tampering (supervised)
    d. Alarms shall be capable of utilizing events generated by the ACS software.
11. Alarm supervision: When using supervised alarm points, the system shall monitor for "OPEN", SHORT", and "GROUND FAULT" in addition to NORMAL/ABNORMAL conditions.
12. ASCII Output-CCTV Remote Control
    a. Alarm points will have the capability to output an ASCII text command for CCTV switched interface.
    b. This command/output will be user-definable and transmitted on alarm points going into abnormal state, returning to a normal state, or both, and for specified reader events as well.
13. Maps/Floor Plan Assignments
    a. The system operator will be able to choose to assign a floor plan to each alert/ event. This floor plan will help in showing the exact location of the event. The system shall be capable of displaying these floor plans automatically or manually by the operator.
    b. If the event is a badge event, in addition to the floor plan, the system will be able to automatically or manually display an image of the badge holder both from the database and live from the CCTV interface.
    c. The system operator will be able to choose to disable the floor plans function in case it is not being used.
    d. The maps shall be capable of running without the ACS software running.
    e. The system operator shall be able to assign icons to devices such as:
       1) doors
       2) card readers
       3) Cameras
       4) Alarm points to include perimeter protection systems
       5) Controllers
       6) Automatic gates
       7) Any device that is controlled by the ACS
    f. The system operator shall be able to, from the map software
       1) Acknowledge alarms
       2) unlock doors
       3) pull up live video from any camera
       4) open automatic gates
14. The system operator will be able to acknowledge pending alerts one at a time or automatically acknowledge all pending alerts.
15. The system operator will have the advantage of filtering events to display only the category of interest.
16. Event display modes:
    a. Tracking Mode will allow the operator to view events activity displayed on the screen as they occur.
    b. Browse Mode will prevent the incoming events from scrolling on the screen. The highlighted event the operator wishes to dwell on will remain stationary on the Events grid. All events may be sorted alphanumerically.
17. Manual Control will be available for every event, which appears in the Event or Pending Alerts Grid display that relates to a door, relay or link.

18. The operator will be able to quickly sort event records by clicking on the column header above the record field he wishes to sort by.

W. Web Browser interface
1. The web browser shall be able to be used remotely and allow for all programming functions offered by the ACS software.

X. Scripting
1. The ACS software shall have a scripting GUI that allows for:
   a. automatic lock down of all doors
   b. send e-mail messages on events or alarms
   c. attach events to linking alarms
   d. attach alarms to linking actions
   e. automatically arm and disarm the Intrusion Detection System
   f. disable any or all card readers
   g. Choose an individual card or input to automatically perform and event when the card is presented to a reader/s or the input goes active in a normal or abnormal state.

Y. Continental FIPS 201, TWIC, FRAC & NIST 800-116 Credential Validation with the CoreStreet Approach
1. Continental Access System shall be capable of PIV enabling to the CA 3000 software as to validate the card with the Government PKI database and the TWIC Hot List database. This function shall be done at the database on every cardholder within the system at the time of enrollment with checks, no longer than 18 hours, of the revocation list.
   a. The checks that shall be accomplished are:
      1) Path discovery – The path from the PIV certificate to an embedded trust anchor.
      2) Path signature verification – establishing that every certificate in the path is genuine and not counterfeit.
      3) Data object signature verification – establishing that every signed data object on the card was signed by a trusted issuer (e.g. certificates, fingerprint template, facial image template) to ensure they are genuine and not counterfeits.
      4) Cross checking data object identifiers – all signed data objects on the PIV card have an identifying number (FASC-N) unique to that card. Checking that each data object contains the same FASC-N (or CHUID) ensures they all belong to the same credential.
      5) Various PKI conformity and freshness checking (key usage, expiration dates, etc.)
      6) PIN check –to ensure the card holder is bound to the credential to mitigate the threat of lost or “shared” cards.
      7) Private Key challenge – to ensure the certificate is bound to the token to which it was issued and has not been copied or cloned.
      8) Biometric check – to ensure the card holder is the same person that was issued the PIV card. This mitigates the threat of “shared” cards and disclosure of the card’s PIN.
      9) Periodic checking of the revocation status of the PIV Authentication certificate.
      10) Periodic revalidating the full path – to ensure all of the certificates in Access Control database remain valid and have not been revoke.
2. Validation during enrollment shall include all of these checks to ensure at the highest level possible that all enrollees are in fact who they claim to be. This would typically be done as a function at or in conjunction with the PACS head-end.
3. Validation at the time of access shall involve a subset of these checks depending upon the assurance level required and authentication mechanism chosen for the specific access point being addressed.

Z. Hardware Definitions:
1. Menu configurations: The System software shall allow for the configuration and programming of the Access Control Panel through the use of a simple graphical user interface (GUI).
2. Access Control Panel Memory Allocation: The allocation of memory for cardholder data, event storage, time schedules and access groups within each Access Control Panel will be user-definable from the ‘Configuration’ menu.

3. Auto-Baud: The system shall allow for advanced baud rate 'syncing' capability with all Access Control Panel's on the system.
4. Auto Panel Type detection:
   a. The system will be capable of determining the type of panel (Access Control Panel) that is connected to a given COM port.
   b. The system shall automatically populate this information in the database.
   c. The system shall limit the number of readers to be programmed based on the panel type.

5. Interactivity:
   a. The system software shall allow, through the optional use of interactivity, less frequently used cardholder records to be automatically stored at the host CPU rather than the Access Control Panel in order to optimize Access Control Panel memory space.
   b. The system operator will be able to configure an Access Control Panel to operate in Interactive mode. When operating in this mode, if an invalid badge is presented to the reader, the panel will query the database to determine if the badge holder is valid in the host database. If so, the data will be sent to the Access Control Panel and an access grant/ deny decision will be made by the Access Control Panel.
6. Access Control Panel Nodes: The system software shall allow up to 512 nodes of Access Control Panels. All of these nodes will be capable of dial-Out communication. A Node will consist of one COM Port with up to two (2) modem connections to support both incoming and outgoing connections. Therefore, you will be able to have two nodes for each COM port.
7. Database Updates: The system software will be able to automatically download/upload information to the Access Control Panels while the Access Control Panels are in communication with the host CPU. A data download will be able to be initiated manually also.
8. Workstations: The system software shall be capable of reporting selectable data by type and by time schedule to any combination of the system workstations simultaneously.
9. Serial Ports: All serial ports will be able to be configured from an easy- to follow menu. Serial ports will be user friendly and selectable for Modem or Cable users, allowing Baud Rate select, and password for each Serial port. Systems requiring in depth knowledge of the operating system or CMOS setup for port configuration are not acceptable.
10. LAN Connections: All LAN Connections will be able to be made from an easy to follow menu.

AA. Time Schedules:
1. Setup: The system software shall have the capacity for 255 user-definable time schedules. Each time schedule will allow for a maximum of 10 individual time intervals.
2. Assignment: The time schedules will be able to be assigned to:
   a. Cardholders
   b. Inputs
   c. Outputs
   d. Doors
   e. Link Programs
   f. Schedule Changes: Readers, Inputs, Relays & Links
   g. Access Groups

BB. Holidays: The system software shall support a minimum of 5 sets of 100 holidays. Holidays are considered as the eighth day of the week, and have different user-definable parameters from the normal designations for that particular day. A holiday will be capable of starting at any time/hour during a 24-hour day. Systems requiring holiday start time of midnight are not acceptable.

CC. Door Definitions:
1. Door Descriptions: Each door shall have a user-definable description of up to 40 characters.
2. Anti-Passback: The Anti-Passback feature shall have the capability of doing nested anti-passback. Each door may be assigned any one of the Anti-pass back states mentioned below:
   a. IN
   b. OUT
   c. NEUTRAL

3. Reader Modes: In addition to the normal mode, each reader will be able to be programmed to respond in the following modes:
   a. ESCORT: Visitors or non-supervisory personnel may only gain access after presenting a valid card, followed by an authorizing cardholder presenting his/her card.
   b. TWO-PERSON: Two valid card reads will be required for access.
   c. DURATION-USE: A user-definable time period may be set to reject successive card reads by the same cardholder.
4. Access Modes: Each door may be programmed to switch automatically between the following modes of operation, based on a user defined time schedule:
   a. CARD ONLY
   b. CARD + PIN
   c. FREE ACCESS
   d. COMMON 4 DIGIT KEYPAD ENTRY
   e. CARD OR CARD # THRU KEYPAD
5. Duress: If a reader is operating in “CARD + PIN” mode, the duress feature will allow an alternate code to be entered into the keypad for access. The system will then generate an alert that may be linked to control relays for the notification of the duress alarm.
6. Door Alarms: Each door may be programmed to generate FORCED DOOR and DOOR OPEN TOO LONG alarms. These alarms will be able to be allowed to have a time delay as required.
7. Door Alarm Annunciation: In addition to generating an alarm message, the following conditions may activate an output for annunciation:
   a. FORCED DOOR
   b. DURESS
   c. DOOR OPEN TOO LONG (DOOR AJAR)
   d. VOID CARD
   e. DENIED CARD
   f. ANTIPASSBACK
   g. INPUT DOOR ALARM
   h. TAMPER
8. Card Data: The system software shall allow for card numbers up to 19 digits.
9. Facility Codes: The system software shall allow for up to 10 facility codes per-panel to be used in the system simultaneously. All 10-facility codes can be downloaded to the Access Control Panels to function in a stand-alone mode, with or without the PC. Alternately, 100,000 system facility codes per panel with Facility Code/Badge Concatenation shall be supported. Systems supporting only one (1) facility code will not be acceptable.

DD. Cardholder Database:
1. The cardholder database will contain all information required to control the cardholders’ access to the facilities.
2. The system administrator will be able to restrict a system operator’s privileges to disable, view-only, create-only, and create/edit.
3. Cardholder Records: Cardholder records will consist of a minimum of the following:
   a. Card Number: The actual badge number assigned to the badge holder.
   b. First and Last Name
   c. Issue level: This indicates the number of times a particular badge number has been issued to a badge holder.
   d. Up to (6) Access Groups: Each badge record will be able to be assigned up to six access groups.
   e. User-Definable PIN Code: A badge holder will be able to select his/her own PIN code. The PIN code must have a minimum of 4 digits
   f. Facility Code: The system shall be capable of accommodating various facility codes within the system. A badge holder will be able to be assigned one of the ten available facility codes.
   g. Anti-Passback Location and Status: This field shows the badge holder’s current anti-passback status, Exempt from APB, In or Out, and the last In/ Out door they were allowed to enter or exit.
   h. Activation Date: The system administrator will be able to enter a date in this field to enable the concerned badge automatically.

i. Expiration Date: The system administrator will be able to enter a date in this field to disable the concerned badge automatically.
j. Badge Use Limit: The system administrator will be able to limit the number of times a badge holder can use his/her badge. In order to do this, the administrator needs to enter a number from 1 to 999 into the Badge Use Limit field.
k. Photo: The system shall permit importing of existing photos or capturing new photos of the personnel, into the cardholder database. The administrator will be able to configure the system such that, presentation of a badge will display the concerned badgeholder's image, in the personnel record.
l. Track Status: When this field is checked, the system will display an event message regardless of any other system setting(s).
m. Last Valid Access: This field will display the last reader, location, date & time at which the particular badge was last used.
n. 48 User Definable and Searchable Text/Data Fields: The system shall include a minimum of 48 user fields divided into 4 tabs in the cardholder database. These fields can be employed for searching personnel records.
o. Duration Use: When this field is checked, the badge holder will not be able to gain entry through an APB reader for the specified duration use time. The duration use time will be variable and will be able to be set by the system operator.
p. Escort: When this field is checked, any badge holder flagged as Escort required, can gain access at the concerned reader, only when accompanied by a non-escort badge holder. The badge holder being 'escorted' will have to present his/her badge prior to the escorting badge holder.
q. No transaction will be generated until both badges are presented at that reader. A time limit will apply between the two badge swipes.
r. Extended 'Access Time' (for ADA Compliance): When checked, the badge holder shall be allowed an extended amount of time to gain access through the door. The system operator will be able to fix any length of time up to 255 seconds.
s. Anti-Passback Override: The system shall allow the system operator to exempt individual badge holders from the anti-passback rules.

4. Batch Modify: The system software shall allow groups of cards to be created/modified by using a card number range.
5. Searching: The system shall allow the operator to quickly find cardholder records by clicking on field titles and entering the criteria being looked for directly into the data field.
6. Alarm Shunting: The system shall facilitate shunting of alarms by allowing certain badge holders to shunt an input/ group of inputs automatically, on presentation of the concerned badge, at a reader.
7. Extended Shunt: If a shunt card is presented at an alarm shunt reader, the value of the Shunt Timeout will be used to determine how long, in minutes & seconds, the door may be opened before a "Door Open Too Long" alert is sent to the host PC.

EE. Reports:

1. Report Types: User-definable data reports will include, but are not limited to, the following information:
   a. Cardholder data
   b. Events
   c. Alert responses
   d. Access Groups
   e. Facility Codes
   f. Holidays
   g. Hardware
   h. Time & Attendance
   i. Operators
   j. Time Schedules
   k. Panels
   l. Operators
   m. Badgeholders In (Muster List)
   n. System settings
2. Transaction Reports: Transaction reports will be available for the following:

a. Card transactions
b. Alarm transactions
c. Event transactions
d. Operator activity

3. Search Criteria: The database shall be structured such that the operator can determine the search parameters based on variables available on the individual report menu. Systems requiring the user to type complicated search strings will not be acceptable.
4. Hardware Report: The system shall have the capacity to generate one comprehensive report that shows the exact configuration of all installed and programmed hardware.
5. Export Report Capability: The system shall support the export of custom reports to Excel, HTML and/or Text file data types.
6. Badgeholders IN (Muster) Report: The system shall support the Badgeholders IN report to be run automatically with the use of an Input.

FF. Help Screens:

1. Online help: The system software shall have online help available at any point requiring operator input. The help screen shall be accessible by using the standard Microsoft Windows help system. These help screens shall contain context sensitive information that will allow the operator to enter correct data without consulting the manual.

GG. System Status:

1. Real time status: The operator shall be able to monitor via graphical screens, the status of the following in real time:
   a. Inputs
   b. Outputs
   c. Doors
   d. Workstations on/off line
   e. Napco Panels

HH. Graphical Floor Maps:

1. Graphics File Format: The floor plans will be configured in a .JPG, .BMP. .DWF & .Ico formats to allow for the importation of existing drawings.
2. Icons: The system shall allow the operator to assign doors, inputs, relays, links and Access Control Panels to these floor plans to indicate the exact location of the event.
3. Operation: Upon activation of a selected input or door alarm, the system shall be able to automatically view the associated floor plan with the alarmed icon blinking on the monitor.
4. Acknowledging Alarms: System operators must be able to acknowledge alarms on the map
5. CCTV: Any camera represented on the map will be able to be viewed by simply right clicking the mouse and choosing view camera.

II. NAPCO Burglar Alarm and Fire Integration:

1. The NAPCO panels that will be supported are the GEM P3200, P9600, X255 and the GEMC 128, 9600 and 255. The integration will support receiving event information from the NAPCO panels, as well as arming and disarming of NAPCO panels from the CardAccess 3000 system. Arming and disarming of NAPCO panels may be by means of reader(s) in the CardAccess 3000 system, as well as manually through an interface similar to the current manual control interfaces in the CardAccess 3000 GUI. It allows unlimited number of cardholders to be programmed for arming and disarming.
2. General Description: The integration will include CardAccess 3000 GUI (Display Screen) to display NAPCO alert types. All events generated will have to be configured to display pending status, priority and/or response required. All these changes must be made through the CardAccess 3000 configuration screens and stored in the same database as the CardAccess 3000 system.
3. Hardware and Communications
   a. There must be one physical serial port for each NAPCO panel to be connected via serial communications or, the NAPCO panel must be capable of interfacing over an existing network via a Napco Netlink TCP/IP interface module. All network communication will be encrypted.

b. All settings changes will be logged in the current ACS Audit Trail table. New audit trail types will denote changes in the NAPCO integration. These changes will be available in the audit trail display as well as in reports. This includes arming and disarming of NAPCO panels, and configuration changes.
c. Visual indication of the alarm area armed/disarmed status will be available at the ACS reader.

4. Communication Software Module
   a. Will receive events from the NAPCO panels.
   b. Will perform arming and disarming functions on the NAPCO panels.
   c. The system shall handle permissions on the NAPCO panels.
   d. Will have the ability to select any Napco event to trigger a CardAccess 3000 event and/or activate DVR recording through CA3000.
   e. Will have the ability for the user to partition Napco panels by privilege level.
5. Configuration Screens:
   a. The configuration screen will allow the user to set up the link between the NAPCO panels and the CardAccess 3000 system. The configuration screens will be available through the CardAccess 3000 GUI in a manner similar to the existing configuration screens in the CardAccess 3000 GUI.
6. Arming and Disarming (Manual Control):
   a. The operator will be able to Arm/Disarm any Napco panel area from the CardAccess 3000 Manual Control menu.

JJ. CCTV Remote Control:
1. Generic Control: The system shall support any CCTV switching system that accepts RS232 ASCII commands through a serial connection.
2. Configuration: The system software shall allow the transmission of at least one 80 character ASCII text string, onto a CCTV control device, via an RS232 port on the workstation.
3. Assignment: Each input and door within the system has the option of transmitting a unique user defined control string of up to 80 characters, onto a CCTV control device.

KK. Full DVR/NVR (Digital Video Recorder) System Integration:
1. CCTV Digital Video Management System Hardware shall be a fully configured, turn- key system available from Continental Access.
2. The Digital video management system must be fully integrated into the CardAccess 3000 system, allowing full viewing and playback from any of the selected CardAccess 3000 workstations. The digital video management system shall be able to perform all viewing, playback and video storage functions simultaneously.
3. The system shall allow video to be displayed on the same CardAccess 3000 monitor, and configuration can be performed with standard mouse and keyboard. The Digital video management shall be able to be configured using an interface application in CardAccess 3000 and shall allow recording of video either continuously or only during alarm events, or only while activity is present. Each camera will be able to record in different modes and on different schedules.
4. The system shall allow for time synchronization between the DVR Server and CA3000 Workstation PC's.
5. The Continental IView shall support IP address based cameras.
6. The system shall allow remote connections over LAN/WAN between all of the CardAccess 3000/CCTV DVR workstations, allowing full viewing and control of any of the Digital Video Recording servers.
7. The Digital video management system shall provide RS-485 or RS-422 communications for controlling compatible PTZ/dome devices from various manufactures. These devices will be controlled through the local or remote user interface in support of the system.
8. The system shall allow local and remote retrieval of video. User-defined parameters will allow searches by camera and based on the following:
   a. Time
   b. Date
   c. Alarm
   d. Motion
   e. Scene loss

9. Logic like such as Duress, Force Door, Void Badge, Valid Badge, Badge tracking, or Bypass shall be available. The interface shall permit full video storage management, hardware control, alarm configuration, and export of video and individual frames.
10. The system shall provide more than one Integral DVR model to be fully integrated with the CardAccess 3000 Security System, such as Integral DVXI/Digital Sentry, or Salient Complete-View that shall allow full system Integration with CardAccess 3000.
11. The system shall provide integration to Multiple DVR Manufacturers or Continental IView server for capturing and compressing video for safe storage and easy access from one single recording box.
12. The system Master Control/IView shall be a user-friendly software that will allow you to easily monitor and record video from multiple cameras.
13. The DVR RemoteView Functions will be possible with the help of the fully integrated DVR RemoteView window, running along with the CardAccess 3000 GUI.
14. The system shall display a minimum of four video windows for viewing remote cameras.
15. The system shall have a toolbar with options to select different Integral/Salient DVR servers, Search, Setup, Alarms and Schedule. No matter which manufacture of DVR is used, the Video window shall have the same 'look and feel' and shall contain at minimum, additional tabs for Search, Setup, Alarm and Schedule.

LL. Photo Import/Tracking:
1. The Photo Import & Tracking shall be a standard feature that is used in conjunction with the ACS software. The ACS does not require the operator to enter data more than once.
2. Events at the reader will display in real time and show a "split screen" of the stored cardholder image next to the "captured" image in case DVR or SmartView interfaces are being used.
3. The system shall be capable of importing images of the cardholders and will store them in the database. These images will be able to be recalled and displayed by the operator.
4. The system operator may choose to disable the imaging function if it is not being used by the system.

MM. First In/Last Out rule:
1. The Free Access schedule shall not energize until an authorized user with First In permissions shall enter an Access Control Door.
2. The Free Access schedule shall be able to be overridden when an authorized user with Last Out permissions presents a valid ID at an out reader.

NN. Door Lockdown:
1. The system operator shall have the ability to lockdown a door/facility with a drop down, user defined window of a series of doors. This action shall override the Free Access Time schedule and will not return to a Free Access Time schedule until the operator manual removes the lockdown command from the drop down menu.

OO. Visitor Control:
1. The system shall allow the administrator to create temporary badge records for use by visitors.
2. The visitor function shall provide for an activation date, at which time the visitor badge will become enabled and an expiration date at which time the badge will become disabled.

PP. Badging 3000 Video Badging:
1. The optional Badging3000 Video Badging package for CA3000 shall enable the users to easily capture cardholder images, add custom text and images, create custom card layouts and print ID cards or credentials with magnetic stripes, bar codes and smart chips.
2. Cardholder images will be able to either be captured remotely with a handheld digital camera and imported into the PC or directly captured via an internal frame grabber and video camera.
3. The following is a list of features that shall be supported:
   a. Drag-and-Drop WYSIWYG Badge Template Editor
   b. Desktop Automated Camera Capture
   c. Context Sensitive On-Line Help
   d. User Defined Badge Templates
   e. Printing:

1) Shall support any Windows-compatible printer
2) Will print both sides of a layout (duplex printing)
3) Will support CMYK
4) Landscape and portrait printing

f. Image Capture:
1) Direct camera drivers for Canon & Olympus cameras
2) Advanced Face-finding feature will automatically locate a face within an image then centers, crops and stores it.
3) Will support importing from file, AVI, TWAIN & WinTab
4) Will point and click configuration of image capture devices
5) Plug-in functionality according to plug-in driver capabilities
6) Chroma key support

g. Image Support:
1) Will support most industry standard image file formats
2) Will auto size static images to match size of object to physically Correct color and crop during image acquisition
3) Special effects
4) Red-eye removal
5) Image enhancement
6) Print images with watermarks

4. Additional Printing Support:
a. Multiple alignment choices and duplex printing on cut-out sheets
b. Point and click configuration of card printers and internal encoders
c. Magnetic stripes can be encoded at print time
d. Will easily copy, cut and paste elements between multiple design windows
e. Duplex printing with user-definable printing modes
f. Will select background color from standard and custom palettes
g. Vertical text option
h. Will draw lines, rectangles, round rectangles & ellipses
i. Will create dynamic text objects including database fields and expressions
j. Will create drop shadows
k. Will apply pre-defined ghost effect to static and dynamic images
l. User-definable fade or transparency levels with static and dynamic images
m. Will remove background pixels from static and dynamic images (close cropping)
n. Will add bar codes with user-definable properties and values
o. Unlimited user-definable image types
p. Will add static images with aspect ratio control
q. Full True Type and ATM font support
r. Will support all popular bar code types
s. Will support Symbol® PDF417

5. E-mail and Pager Notification:
a. The system shall allow the administrator to select alarm and/or badge activity event to be sent to a user via e-mail or pager/cell-phone.
b. The system shall allow the user a simple interface for email account setup.

6. Input and Activity Linking:
a. The system shall allow for ‘Activity Links’ that provide the capability to control relays based on an event.
b. Shall allow the CA3000 to be a direct replacement for the Sensormatic AC500 system.
c. Shall allow triggering of activity link in case any of the following events occur:
1) AC Power Fail/Restore
2) Input Abnormal/Normal
3) Input Supervisory Open/Short/Fault
4) Relay On/Off
5) Link Activate/Deactivate
6) Forced Door

7) Door Closed
8) Door Bypass
9) Door Free Access Start/End
10) Door Open Too Long
11) Door Key Code Entry
12) Manual Door Unlock/Lock
13) Manual Door Enable/Disable
14) Low/High Watermark
15) Valid Badge
16) Valid Badge Enabled
17) Valid Badge Disabled
18) Duress Access
19) Denied Void Badge
20) Denied Facility Match
21) Denied Time Of Day
22) Denied Issue Level
23) Denied Unauthorized
24) Denied PIN Violation
25) Denied APB IN/OUT
26) Denied Escort Match
27) Denied Reissue
28) Denied Vehicle Tag Match
29) Violate Exit Override
30) Violate Entry Override
31) Violate Time Of Day Override
32) Denied Interactivity Timeout
33) Activity Link ON/OFF

7. Category Counters: The Activity Link operation shall also include 16 category counters which allow the cardholder to trip a single or multiple activity links.
8. Watermarks: The watermark feature shall allow the system to 'count' the amount of cardholders/vehicles in a particular area. The user shall have the ability to set 'high' and 'low' marks for the system to increment and decrement the card/vehicle count. This can be used to disable a reader and disallow any further activity into the area until the watermark drops below the preset mark.
9. Local and Global Activity linking: The system shall support both local (within the same Access Control Panel) as well as global (spanning multiple Access Control Panels) Activity linking for maximum system flexibility.

QQ. Alarm Event Limit:

1. This feature shall allow the user to limit the number of repeat alarm events sent from a panel within a given period of time.
   a. The user shall have the ability to add a time delay on an alarm to lessen the number of alarms that will be sent to the Pending Alerts grid for an input that remains 'Abnormal'.
   b. This time delay setting shall be configurable and shall be in minutes.
   c.

RR. Variable Door Open/Shunt Time:

1. This feature shall allow the user to unlock a door, either through Manual control or a card read, for a period as short as one second or up to one hour.
   a. The system shall bypass the door input for the same time as the unlock time.
   b. The system shall allow for time increments in seconds up to 59 and then in minutes only up to 60.
   c. The system shall allow for the same manual control over relays.

SS.Application Programming Interface:

1. The system shall provide for an Application Programming Interface for third party integration.
2. The API shall be constructed as a standard Windows Dynamic Link Library (DLL) and will provide various functionalities in the form of function calls.

TT. Right-to-Left Language Support:
1. The system shall support Languages requiring a display from right-to-left including, but not limited to, Arabic and Hebrew.

UU. Access Control Panels: Continental Access Control Panels used by CardAccess 3000 are modular in design. The access control panels (or panels for short) are also referred to as controllers. Two door, four door and eight door panel versions are available.
1. General Features:
   a. PC Board: The Access Control Panel shall be a microprocessor controlled solid-state electronic device and will include a real time clock/calendar on board. The Access Control Panel shall be compliant with UL294, or an equal. A subset of the ACS database sufficient enough to support access and alarm functions for its designated readers and points will be able to be stored at the Access Control Panel. In the event of communication loss, the Access Control Panel will continue to function without any degradation in operation, and will provide storage for at least 1000 and utmost 210,000 transactions. These stored events will be uploaded to the CPU automatically upon the restoration of communications.
   b. Modem Communication: The Access Control Panel shall be capable of operating over standard telephone lines using external modems. An Access Control Panel will automatically initiate a dial and will upload stored information in case the storage buffer is 80% full or in case a user defined alarm condition occurs. The CPU shall have the ability to automatically request information from the remote Access Control Panels based on a user defined time schedule.
   c. Direct Communication: The Access Control Panel shall communicate via an RS232 or RS422 link directly to the ACS CPU. No additional interface equipment will be required. The Access Control Panel shall be capable of being configured in either repeat mode (serial) or in multi-drop mode. When in repeat mode, the distance between control panels shall be up to 4000 feet, communicating at 57,600 baud, without the use of modems or line drivers.
   d. Electrical Noise Suppression: The controller shall have “Built-In” electrical noise suppression devices to protect the on-board microprocessor from relay-generated transients.
   e. Electrical Surge Protection: The controller shall have “Built-In” electronic surge protection devices to protect controller circuitry to which external connections are made.
   f. Battery Backup: The Access Control Panel shall include, as a standard, at least 4 hours of battery backup. The Access Control Panel also shall include internal battery backup to maintain controller database, program, time and date during a power loss.
   g. Diagnostic LED’s: The Access Control Panel shall have an LED display to indicate power, processor heartbeat, and the transmission and receipt of programmed data.
   h. Biometric Readers/Card Readers/Keypads: The Access Control Panel shall support entry/exit points that allow for a keypad to be used in conjunction with the reader, and the keypad accepts user-definable PIN codes. Systems requiring additional ports for the addition of a keypad are not acceptable. The Access Control Panel shall be able to support multiple card technologies (such as Proximity, Smart Readers, Smart Cards, Biometric-Fingerprint, Iris Scan, Hand Geometry, Face Recognition, Magnetic Stripe, Wiegand, etc.) concurrently without the need for additional software or hardware.
   i. Inputs: Without the need for any additional hardware, each Access Control Panel will be able to monitor supervised alarm inputs. By means of software download, the Access Control Panel shall allow the user to decide whether the alarms must function as supervised or non-supervised inputs.
   j. Outputs: Without the need for any additional hardware, each Access Control Panel will be able to control user-definable Form C relay outputs.
2. Hardware Options:
   a. Alarm Expander Board: Additional inputs will be able to be made available by means of expansion boards mounted in the Access Control Panel enclosure. Each expansion board has a minimum of 16 supervised inputs. Up to three (3) expansion boards are allowed for each Access Control Panel.
   b. Relay Expander Board: Additional outputs will be able to be made available by means of expansion boards mounted either in the Access Control Panel enclosure, or in the additional enclosures. Each expansion board shall have a minimum of 16 Form C relay outputs and 8 inputs. The Super-Two, Superterm and Turbo Superterm Access Control Panels shall be allowed to have a maximum of three expansion boards.

c. Memory Expansion: An additional memory board (20Mb) shall be available, allowing the Turbo Superterm expansion to (1,000,000) cards.

3. Enclosure: The Access Control Panel enclosure shall have a hinged cover with key lock. A control panel input point will monitor an enclosure tamper switch.
4. Software Features:
   a. Facility codes: The Access Control Panel shall recognize up to ten different Facility Codes. These facility codes will be able to be defined and then assigned on a per cardholder basis or 100,000 system facility codes per panel with Facility Code/Badge Concatenation shall be selectable.
   b. Card Formats: The Access Control Panel shall be capable of storing up to 10 custom card formats. The Access Control Panel will be able to read the format of most Magnetic Stripe, Bar Code, Proximity or Wiegand Effect encoded cards and will allow an operator to specify parity, start sentinels, stop sentinels, field separators, facility code bits, issue level bits, and card number bits.
   c. Global Linking: The Access Control Panel will be able to store up to 64 unique linking programs. A link program will automatically trigger relay output(s) in response to alarm input(s). Inputs may be simple time schedule definitions or any one of up to five alarm inputs. In response, a maximum of five relays may be turned on/off, activated/deactivated, or relays may track the alarm input(s), for a length of time as defined by the user.
   d. Card Number Length: The Access Control Panel shall be capable of reading card numbers up to 19 digits.
   e. Time Schedules: The Access Control Panel shall have the capacity to store 255 time schedules, with each time schedule comprising of up to 10 time intervals. (The Access Control Panel thus will have the capacity to accommodate a total of 2550 time intervals). Each interval of time can consist of a range of days; seven days of the week, plus a Holiday Type Schedule. The Access Control Panel shall automatically manage time schedules based upon its internal clock.
   f. Holidays: The Access Control Panel shall allow for the definition of 5 sets of 100 Holiday Schedules, or exceptions to normal scheduling. Holidays will be able to be defined according to day of year and time of day. All holidays will be automatically incorporated into Time Schedule definitions.
   g. Holiday Types: The Access Control Panel shall allow for up to 5 Holiday types. Each Holiday type will consist of different Holiday schedules.
   h. Access Modes: Each card reader/keypad shall have the ability to operate independently in up to five different modes: Card only, Common Code only, Card plus PIN, Free Access & Card or Card # through keypad. These modes of operation will be able to be programmed from the ACS host computer and can automatically change according to time schedule assignment.
   i. Anti-pass back: The Access Control Panel shall support anti-pass back operation in which, the cardholders are required to follow a proper in/out sequence.
5. Controllers:
   a. Continental Access manufactures different kinds of Access Control Panels in 2, 4 and 8 door configurations.
6. General Features:
   a. PC Board: The aforementioned Access Control Panels shall be microprocessor controlled solid-state electronic devices and shall include a real time clock/calendar on board. They shall be compliant with UL294 or equal. A subset of the ACS database sufficient to support access and alarm functions for their designated readers and points will be able to be stored at the Access Control Panel. In the event of communication loss, the Access Control Panels will continue to function without any degradation in operation, and will provide storage for a minimum of 20,000 cardholders and at least 1000 transactions.
   b. Modem Communication: The aforementioned Access Control Panels shall be capable of operating over standard telephone lines using external modems. They shall automatically initiate a dial and upload stored transactions if the storage buffer is 80% full or if a user-defined alarm condition occurs. The CPU also shall have the ability to request information automatically from the remote Access Control Panels based on a user- defined time schedule.
   c. Network Communication: The aforementioned Access Control Panels shall support the use of network communication devices to provide communication over LAN and WAN systems.
   d. Direct Communication: The Access Control Panels shall communicate via an RS-232 or RS-422 link directly to the ACS CPU. No additional interface equipment will be required. The Access

Control Panels shall be capable of being configured in either repeat mode (serial) or in multi-drop mode. When in repeat mode, the distance between the control panels may not exceed 4000 feet. The control panels shall need to be communicating at 57,600 baud, without the use of modems or line drivers.

e. Battery Backup: As a standard, the Access Control Panels shall include at least 4 hours of battery backup (7AH). They shall also include internal battery backup to maintain controller database, program, time and date during a power loss.

f. Diagnostic LED's: The Access Control Panels shall have an LED display to indicate power, and transmission/receipt of programmed data.

7. Hardware Features and Options:
   a. Card Readers: At least 16 supported
   b. Keypads: Allowed for PIN Code entry by users
   c. Inputs: At least 24 supervised alarm inputs can be monitored without the need for any additional hardware
   d. Outputs: Without the need for any additional hardware, at least 17 user definable form C relay outputs can be controlled
   e. Alarm Expander Board: Up to 3 expander boards allowed, each can have a minimum of 16 supervised inputs
   f. Relay Expander Board: Up to 3 expander boards allowed, each can have a minimum of 16 Form C inputs Up to 3 expander boards allowed, each can have a minimum of 16 Form C relay outputs and 8 inputs
   g. Memory Expansion Additional Memory module [256k,2Mb or 4Mb] shall be available, allowing expansion up to 1,000,000 cards

VV. PRODUCT SUBSTITUTIONS
1. Substitutions: No substitutions permitted.

PART 3 EXECUTION

3.01 INSTALLATION

A. General: The contractor shall install all system components and appurtenances in accordance with Continental Access' instructions, and shall furnish all necessary interconnections, services, and adjustments required for a complete and operable system as specified and shown. Control signal, communications, and data transmission line grounding shall be installed as necessary to preclude ground loops, noise, and surges from adversely affecting system operation. Provide mounting hardware as required.

B. Installation: All low voltage wiring outside the control console, cabinets, boxes, and similar enclosures, shall be plenum rated where required by code. Cable shall not be pulled into conduits or placed in raceways, compartments, outlet boxes, junction boxes, or similar fittings with other building wiring.

C. Device Wiring and Communication Circuit Surge Protection: All inputs shall be protected against surges induced on device wiring. Outputs shall be protected against surges induced on control and device wiring installed outdoors, and as shown. All communications equipment shall be protected against surges induced on any communications circuit. All cables and conductors, except fiber optics, which serve as communications circuits from security console to field equipment, and between field equipment, shall have surge protection circuits installed at each end.

3.02 FIELD QUALITY CONTROL

A. Site Tests and Inspections:
1. General

a. The contractor shall perform pre-delivery testing, site testing, and adjustment of the completed ACS. The contractor shall provide all personnel, equipment, instrumentation, and supplies necessary to perform all testing. Written notification of planned testing shall be given to the owner at least [fourteen 14] days prior to the test and in no case shall notice be given until after the contractor has received written approval of the specific test procedures. Test procedures shall explain in detail, step-by-step actions and expected results demonstrating compliance with the requirements of the specification. Test reports shall be used to document the results of the tests. Reports shall be delivered to the owner within seven (7) days after completion of each test.

2. Performance Verification Test:
   a. The contractor shall demonstrate that the completed ACS complies with the contract requirements. Using approved test procedures, all physical and functional requirements of the project shall be demonstrated and shown.

3.03 CLOSEOUT ACTIVITIES

A. Training:
   1. General: The contractor shall conduct training courses for personnel designated by the owner. Training shall cover the maintenance and operation of the ACS. The training shall be oriented to the specific system being installed under this contract including central processor. Training manuals shall be delivered for each trainee with two additional copies delivered for archiving at the project site. The manuals shall include an agenda, defined objectives for each lesson, and a detailed description of the subject matter for each lesson. The contractor shall furnish audiovisual equipment and other training materials and supplies as necessary. Where the contractor presents portions of the course by audiovisual material, copies of the audiovisual material shall be delivered to the owner on the same media as that used during the training session. Up to [ ] hours of training shall be provided for in the base contract.

3.04 WARRANTY, MAINTENANCE, AND SERVICE

A. Warranty:
   1. The ACS shall be warranted by the contractor for one (1) year from the date of final system acceptance.

B. Maintenance and Service:
   1. The contractor shall provide all services required and equipment necessary to maintain the entire ACS in an operational state as specified for a period of one (1) year after formal written acceptance of the system, and shall provide all necessary material required for performing scheduled adjustments or other nonscheduled work.
   2. Description of Work:
      a. The adjustment and repair of ACS includes computer equipment, software updates, signal transmission equipment, access control equipment, facility interfaces, and support equipment. Responsibility shall be limited to contractor installed equipment. Provide the manufacturer's required adjustments and other work as necessary.

C. Personnel:
   1. Service personnel shall be qualified to accomplish all work promptly and satisfactorily. The owner shall be advised in writing of the name of the designated service representative and of any change in personnel.

D. Inspections:
   1. The contractor shall perform two inspections at [six (6)] month intervals or more often if required by the manufacturers. This work shall be performed during regular working hours, Monday through Friday, excluding Federal holidays. These inspections shall include:
      a. Visual checks and operational tests of the central processor, local processors, monitors, keyboards, system printers, peripheral equipment, ACS equipment, power supplies, and electrical and mechanical controls.

b. Clean system equipment, including interior and exterior surfaces.
c. Perform diagnostics on all equipment.
d. Check and calibrate each ACS device.
e. Run system software and correct diagnosed problems.
f. Resolve previous outstanding problems.

E. Emergency Service:
1. The owner will initiate service calls when the ACS is not functioning properly. Qualified personnel shall be available to provide service to the complete ACS. The owner shall be furnished with the telephone number where the contractor's service supervisor can be reached at all times. Service personnel shall be at the site within four [4] hours after receiving a request for service. The ACS shall be restored to proper operating condition after one [1] calendar day.

END OF SECTION

DISCLAIMER: Specification requires the sole professional judgment and expertise of the qualified Specifier and Design Professional to adapt the information to the specific needs for the Building Owner and the Project, to coordinate with their Construction Document Process, and to meet all the applicable building codes, regulations and laws. CONTINENTAL ACCESS (A NAPCO SECURITY GROUP COMPANY) EXPRESSLY DISCLAIMS ANY WARRANTY, EXPRESSED OR IMPLIED, INCLUDING THE WARRANTY OF MERCHANTABILITY OR FITNESS FOR PARTICULAR PURPOSE OF THIS PRODUCT FOR THE PROJECT.