SECTION 285300 – ACCESS CONTROL SYSTEM

PART 1 - GENERAL

1.1 RELATED DOCUMENTS

A. Provisions of the Contract and of the Contract Documents apply to this section.

1.2 SUMMARY

A. Provide as indicated on the Drawings and herein specified a complete and operable Access Control System. Readers shall consist of proximity readers, proximity reader/keypads, and other access control system devices. Upon correctly entering a personal ID code or presenting a proximity card or keyfob, the system shall grant access to a controlled device or resource

B. County has standardized on Identicard Premisys access control. Provide Identicard Premisys access control system that will work as a stand-alone system and will not be integrated with existing County system. Coordinate with the Owner all the card, keyfob, and other credential types being used by the Owner and provide a complete and fully-functional system that will work with those existing credentials.

C. The Access Control System shall be installed in accordance with all applicable NEC, and local building codes. All equipment shall be UL labeled. All equipment shall be compatible

D. The Access Control System shall interface to the Fire Alarm System as required to meet all required Fire and Life Safety Codes

E. The system shall include, but not be limited to, the following
   1. Proximity card readers
   2. Proximity card & keypad combo readers
   3. Control Processors
   4. Alarm monitoring modules
   5. Output relay modules
   6. Access control proximity cards & key fobs
   7. PC running the Card Access System's Software
   8. All required licenses to function completely and expand 25%.
   9. I.D. Photo Access Cards with identification images and logos
   10. Support Biometric readers
   11. Support Magnetic stripe card readers
   12. Support keypads & pin pads

F. Provide archive/purge and backup utilities for database maintenance.

G. The Access Control System's database shall be fully integrated with the database of the Security Management Server (SMS), allowing the token user's Name, not ID code, to be logged by the SMS upon any use of a token reader. The system shall log all access control events, including access granted, access denied and duress codes used. All access control events shall be associated with the token user's Name. Provide secure lock operation and maintain audit trail, even when the server or the network is unavailable.

H. The Access Control System's database, shall be capable of a minimum of 5,000 user accounts. The Access Control System shall be capable of supporting 100 client licenses. Access Control system database shall be Microsoft SQL 2008 or better.

I. The Access Control System shall be a robust, user-friendly, easily expandable solution. Users shall be added, modified, and deactivated using a Windows-based GUI interface. Each user shall be given customized access rights to controlled devices and other resources based on the time of day, day of the week, and restricted dates. In addition, users must be able to be assigned to customized user groups, which system administrators shall be able to create in order to streamline the access management process and tailor it to their own needs.

J. The Access Control System shall integrate seamlessly with the Security Control System to visually alert operators when a door has been accessed via the reader system and shall allow Touchscreen operators to isolate (disable) individual readers to prevent access. The SMS shall be able to log requests at doors with an isolated reader. Users shall be capable of entering Duress Codes at proximity reader/keypads, which shall activate a duress alarm at that location on one or more Touchscreens. The same level of integration shall also be seen on the SMS, which shall record the user's Name and time when a resource is accessed, and shall include a full range of reporting features. Login to the Access Control software shall be password protected and access shall be logged to the SMS.

K. The access system shall not directly open any doors in the detention areas of the building. It shall make door open requests of the PLC System. The PLC System shall verify interlocking of the requested door and status of the reader prior to any unlocking.

L. The system shall also have a fully integrated, Windows-based help system. The system shall also have context sensitive help.

M. The system shall have a lockout feature after an invalid access code has been entered four times on a keypad.

N. The system shall be programmable with a master code so that access can be granted through a card reader/keypad combo device with only the master keypad code and no proximity card.

O. Provide hardware and software as a single integrated application for all of the following:

1. Online locks that are programmed and controlled via a central computer which communicates via the network to controllers which are then wired to the individual door locations.

2. Offline locks which may become disconnected from a central computer system, but are managed and programmed by the same software application.

1.3 CARD ACCESS VIEWING STATION COMPUTER:

A. Central Equipment: Provide a Central File Server with Card Enrollment equipment as indicated on the drawings. This file server shall be permanently connected to PLC via Ethernet. All central equipment power shall be provided from emergency circuits. Additional UPS or Battery Backup power shall be provided for all central equipment to provide error free operation. Central equipment shall include but not be limited to the following:

1. Intelligent Controller: Supports up minimum of 8 readers. Firmware for 10,000 cardholder records and 1,000 transactions. Shall support both proximity readers and keypads simultaneously for each door. Systems shall be capable of optionally supporting LAN or WAN communications using TCP/IP.

2. Access Control Software shall operate on Windows 7 or better. Software shall include Administration, Event Monitoring, Status Windows, and multiple application windows open simultaneously, Software shall also include the following.

1.4 SOFTWARE FEATURES

A. User Configuration Functions: A user shall include any individual that uses the access control system to access resources, such as a door, software application, or Touchscreen. A user shall also include an administrator who is using the access client software to add users and set permissions and rules. User configuration functions shall include the following:
   1. Creating a New User
      a. Provide a User Configuration screen that shall allow the operator to create a new user or display information about current users. The information fields displayed shall include the following; Last Name, First Name, Middle Name and ID Number. The ID Number shall be any combination of letters and numbers up to a maximum of 50 characters
      b. Optionally, a User Type shall be capable of being selected: Types shall include (None), Staff, and Visitor. A user type of Inmate or Staff must be selected when using the work release or time and attendance tracking features respectively
      c. Any custom user information shall be capable of being entered into the Additional Information tab
      d. An image shall be capable of being associated with a user and stored in the SMS database for retrieval from the client software or touchscreen(s)
   2. Modifying a User (Searching)
      a. Provide a means to modify information about existing users
      b. Provide a User Search dialog box that, by default, displays all active users in the database. The User Configuration screen for each user shall be displayed upon the selection of a user in the database
      c. Provide a means to facilitate a more refined search. The operator shall be capable of selecting a field (i.e. – Last Name, First Name, ID Number, token, etc.) to search on in a “Search” list and typing the desired text in a “For” box. The operator shall also be capable of searching for deactivated accounts by means of a checkbox selection
   3. Acquiring an Image for a User
      a. Provide a means to capture an image and associate it with an individual user in the database
      b. Provide an Image Acquire screen that shall allow an operator to capture an image via an image capture device (i.e. – USB camera). Provide a drop-down list of available image capture devices
      c. Provide a preview window that displays a live video stream. Depending upon the options available for the selected image capture device, provide Format, Source, Compression, and Display buttons to allow the operator to fine-tune the video stream
      d. Provide an Image Capture button for the operator to select once the user is positioned properly in the preview window. Once selected, the image shall appear in a separate user image window. Provide a means to assign the captured image to the user
   4. Importing an Image for a User
      a. Provide a means to import an image and associate it with an individual user in the database

b. Provide an Import Image screen that shall allow an operator to import an existing image. Provide a window for the operator to browse to an existing image and open the image once it is found
c. Provide an outlined area (or box) showing the size of the user image window. If the imported image is larger than the user image window, the operator shall be able to relocate the image box by holding down the left mouse button and dragging the box to the desired location within the image. Provide a means to assign the imported image to the user

5. Assigning Permissions to a User
   a. Provide a means to allow users access to system resources
   b. Provide an Assign Permissions tab within the User Configuration screen. This screen shall show a list of all system resources. Each resource shall include a checkbox to allow access to that particular resource. Provide a "filter" box with drop down menu to allow the operator to select and display a particular type of resource. Resource types shall include, but not be limited to, the following; Doors, Touchscreens, Access Control System Client software, SMS client, etc
   c. Provide Check All and Uncheck All buttons for the operator to select to simplify the assignment of permissions
6. Assigning a User to User Groups
   a. Provide a means to allow users to be assigned to User Groups. A User Group shall be defined as a specific group of users who share the same permissions and rules. When a user is assigned to a group, they shall receive the same permissions and rules that the group has, in addition to their own individual permissions and rules. Users shall be capable of belonging to more than one user group
   b. Provide an Assign Groups tab within the User Configuration screen. This screen shall show a list of all user groups in the system. Each group shall include a checkbox to assign the user to that particular group
7. Assigning Rules to a User
   a. Provide a means to assign rules to a user. Assigning rules to a user shall allow the user's permissions to be restricted to specific days of the week, as well as specific times of the day. Provide a means to have a user's access to activate or expire on a specific day or prevent them from using permissions on restricted dates
   b. Provide an Assign Rules tab within the User Configuration screen. Provide an 'Allow access only on selected days of the week' checkbox for users that are allowed access only on specific day(s). Provide checkboxes for each day of the week for the operator to select for days they want the user to have access on
   c. Provide an 'Allow access only during time range' checkbox for users that are allowed access only during specific times. Provide time configuration boxes for 'No earlier than' and 'No later than' that include the time in hours, minutes and seconds. Provide indications for "AM" and "PM"
   d. Provide an 'Unrestricted Access' checkbox to select for users that have no access restrictions based on the time of the day and the day of the week
   e. Provide an 'Access has activation date' checkbox for users that have permissions that should not begin until a later date. Provide a drop-down calendar tool to set the activation date
   f. Provide an 'Access has expiration date' checkbox for users that have permissions that should expire on a certain date. Provide a drop-down calendar tool to set the expiration date
   g. Provide an 'Allow access on restricted dates' checkbox for users that are allowed access on restricted dates

8. Assigning Tokens to a User
    a. Provide a means to assign tokens to a user. Assigning Tokens to a user consists of assigning items such as a PIN code, Duress Code, proximity card number, password, etc. that the Access Control System uses to identify a user
    b. Provide an Assign Tokens tab within the User Configuration screen. All tokens assigned to a particular user shall be displayed on this tab
    c. Provide information fields for the following tokens: Proximity Card, Personal Identification Number, Duress Code and User Name and Password
    d. Provide a Proximity Card field that shall be used to assign a proximity card or keyfob ID number to the user. For this feature, a proximity reader enrollment station may be used. The operator shall activate an Enroll button and swipe a proximity card or keyfob at the enrollment reader. The proximity ID will appear in the field when the card or keyfob is read
    e. Provide a Personal Identification Number field that shall be used to assign a unique number to a user for use with proximity readers with a keypad option. Upon correct entry of a personal identification number at a keypad, the user shall be granted access to the resource. The personal identification number shall be up to a maximum of 12 digits long, and unique for all users
    f. Provide a Duress Code field that shall be used to assign a unique number to a user for use with proximity readers with a keypad option. Upon correct entry of a duress code at a keypad, the local and Central Control Touchscreen(s) shall be notified that a duress alarm exists. The duress code shall be a maximum of 13 digits long
    g. Provide User Name and Password fields that shall be used to assign a unique user name and corresponding password for the purpose of accessing Touchscreens and the access control system client software
    h. Provide for a replacement card to automatically invalidate the user's previous lost card
9. Creating a New User Group
    a. Provide a means to create User Groups, which shall allow the operator to easily assign the same permissions and rules to many users
    b. Provide a Group Configuration screen that shall allow the operator to create a new group or display information about current groups. The information fields displayed shall include the following; Group Name
10. Modifying a User Group (Searching)
    a. Provide a means to modify information about existing user groups
    b. Provide a User Group Search dialog box that, by default, displays all active user groups in the database. The User Group Configuration screen for each user group shall be displayed upon the selection of a user group in the database
    c. Provide a means to facilitate a more refined search. The operator shall be capable of selecting a field (i.e. – Group Name, Resource Type, Resource Name) to search on in a "Search" list and typing the desired text in a "For" box
11. Assigning Permissions to a User Group
    a. Provide a means to allow user groups access to system resources
    b. Provide an Assign Permissions tab within the User Group Configuration screen. This screen shall show a list of all system resources. Each resource shall include a checkbox to allow access to that particular resource. Provide a "filter" box with drop down menu to allow the operator to select and display a particular type of resource. Resource types shall include, but not be limited to, the following; Doors, Touchscreens, Access Control System Client software, SMS client, etc

c. Provide Check All and Uncheck All buttons for the operator to select to simplify the assignment of permissions

12. Assigning Rules to a User Group
    a. Provide a means to assign rules to user groups. Assigning rules to a user group shall allow the user group's permissions to be restricted to specific days of the week, as well as specific times of the day. Provide a means to have a user group's access to activate or expire on a specific day or prevent the group from using permissions on restricted dates
    b. Provide an Assign Rules tab within the User Group Configuration screen. Provide an 'Allow access only on selected days of the week' checkbox for user groups that are allowed access only on specific day(s). Provide checkboxes for each day of the week for the operator to select for days they want the user group to have access on
    c. Provide an 'Allow access only during time range' checkbox for user groups that are allowed access only during specific times. Provide time configuration boxes for 'No earlier than' and 'No later than' that include the time in hours, minutes and seconds. Provide indications for "AM" and "PM"
    d. Provide an 'Unrestricted Access' checkbox to select for user groups that have no access restrictions based on the time of the day and the day of the week
    e. Provide an 'Access has activation date' checkbox for user groups that have permissions that should not begin until a later date. Provide a drop-down calendar tool to set the activation date
    f. Provide an 'Access has expiration date' checkbox for user groups that have permissions that should expire on a certain date. Provide a drop-down calendar tool to set the expiration date
    g. Provide an 'Allow access on restricted dates' checkbox for user groups that are allowed access on restricted dates
13. Assigning Users to a User Group
    a. Provide a means to assign users to user groups. When a user is assigned to a user group, they receive the permissions and rules of the user group in addition to their own rules and permissions
    b. Provide an Assign Users tab within the User Group Configuration screen. Each user in the database shall be displayed. Each user shall include a checkbox to assign the user to that particular group

B. Administrative Configuration Functions: Provide administrative-level tools to enhance and customize the functionality of the access control system software
1. Adding/Modifying/Deleting User Information Types
    a. Provide a User Information Type screen that shall allow the administrator to create new, modify existing, or delete existing information fields for users. Information types (i.e. – address, phone number, etc.) shall be defined by the administrator on this screen. The administrator shall be capable of assigning a display order for each information field. A minimum of 1000 administrator-definable user information types shall be available
    b. Once defined, these fields shall be displayed in the User Configuration screen. Provide an Additional Information tab within the User Configuration screen. All additional information specific to a particular user shall be displayed on this tab
2. Adding/Modifying/Deleting Restricted Dates
    a. Provide a Restricted Dates screen that shall allow the administrator to create new, modify existing, or delete existing restricted dates. Restricted Dates shall be used to control access on Holidays or other user-defined dates. Restricted dates shall be defined by the administrator on this screen. The administrator shall be capable of

assigning a name, as well as a date for the restricted date on this screen. A minimum of 1000 administrator-definable restricted dates shall be available

b. Once defined, access on restricted dates shall granted by going to the Assign Rules tab within the User Configuration screen, and checking the 'Allow access on restricted dates' checkbox

3. Reporting Features: The access system shall have the following reporting features
   a. User Profile Report: This report shall provide information in a document format on the user, such as full name, ID Number, and whether the account is activated or deactivated. This report shall also detail what group(s) the user belongs to, as well as what resources the user has permission to access. The rules for the user shall also be listed in the User Profile Report
   b. Resource Report: This report shall provide information in a document format on a particular resource. This report shall detail the specific resource chosen, as well as what group and user permissions are assigned to the resource
   c. Audit trail available historically or in real time, including standard reports that include, but not limited to:
      1) Invalid access attempts
      2) Time and attendance
      3) Door reader location
      4) Group of readers
      5) Individual cardholder
      6) Operator console activity
      7) History report for an alarm point(s) of state. An alarm point state shall be defined as: Normal, alarm, Trouble, Ajar
      8) History report for card state. A card state shall be defined as: Normal, Trace, Not Found, Anti-Pass violation, Time Zone Violation, Site Code violation or Expired card
   d. Ability to design custom reports

4. System Backup/Restore: The access system shall have the following administration features
   a. Database Backup: This tool shall provide a database management window, which shall allow the database files to be backed up to another directory or external media
   b. Database Restore: This tool shall provide a database management window, which shall allow the database files to be restored from another directory or external media
   c. Provide automatic backup procedure daily.
5. Badge Designer: The system shall have the following Badge Designer features
   a. Badge Designer Basics: This tool shall be used to create custom badge templates. A badge template can then be assigned to any number of users in order to print custom user badges. The badge designer shall be capable of creating templates for use with badges with similar requirements
   b. Badge Printing: This tool shall be used to allow for edge-to-edge card printing
6. Software shall have ability to partition control of the system by user ID.
   a. Allow multiple administrators with partition control.
   b. Allow a minimum of four administrators with ability to create security levels per operator.
   c. The cardholder database must be shareable across partitions.
   d. Must be able to create cardholders that are only accessible from a single partition.

e. Hardware components (locks, readers, controllers, etc.) must be able to be assigned to a particular partition or shared across multiple partitions.

7. The system shall automatically adjust the time of the system for Daylight Savings changes.
8. The system shall cause an alarm when controllers go off-line.

1.5 SUBMITTALS

A. Refer to Section 285000 for submittal requirements.

PART 2 - PRODUCTS

2.1 MANUFACTURERS

A. Identicard Premisys

2.2 FILE SERVER/CARD ACCESS CLIENT STATION COMPUTER

A. Provide a File Server with Card Enrollment equipment and Client stations as indicated on the drawings. This file server shall be permanently connected to PLC via Ethernet. File Server and Client Station computers shall include but not be limited to the following:
   1. Access Control Software shall operate on Windows 7 or better. Software shall include Administration, Event Monitoring, Status Windows, and support multiple application windows open simultaneously.
   2. The PC-based workstations shall consist of an Intel Core i5-4570 quad core, 3.2GHz turbo processor or better, 512K cache, 8GB 1600MHz DD3 Memory, 250GB hard drive, 2 USB ports, network card for Ethernet operation, CD-ROM drive, sound card, video accelerator, running Windows 8 pro. Provide UPS power for all workstations.
   3. Approved Manufacturers:
      a. HP
      b. Dell

B. Provide at Access Control System station a 22" or larger LCD flat panel monitor with 1280 X 1024 resolution.
   1. Approved Manufacturers – Dell, Samsung, NEC, HP

2.3 MATERIALS

A. Central Equipment
   1. All components used in creating the access control system shall be of the same manufacturer and/or approved by the manufacturer for system compatibility. Used products shall not be acceptable. Equipment specified herein indicates the types of equipment and the minimum quality of equipment required. It shall be the SCSC's responsibility to assure the compatibility of all access control equipment, software, programming, cable, mounting methods, etc. that are used in providing a complete, fully-functional system.
   2. All central equipment power shall be provided from emergency circuits. Additional UPS or Battery Backup power shall be provided for all central equipment to provide error free operation.
   3. Intelligent Controller: Supports up minimum of 8 readers. Firmware for 10,000 cardholder records and 1,000 transactions. Shall support both proximity readers and keypads simultaneously for each door. Systems shall be capable of optionally supporting LAN or WAN communications using TCP/IP.

B. Proximity Reader
   1. Dimensions: 3.3” x 4.8” x .95”
   2. Power Supply: 5-12 VDC
   3. Current Requirements: Average – 50/75mA (12VDC)
   4. Operating Temperature: -40° to 150°F (-40° to 65°C)
   5. Operating humidity: 5-95% relative humidity, non-condensing
   6. Transmit and Excite Frequency: 125kHz and 13.56MHz
   7. The proximity reader shall be a HID Corp. model RP40 or approved equal

C. Proximity Reader/Keypad
   1. Dimensions: 3.3” x 4.8” x .95”
   2. Power Supply: 5-12 VDC
   3. Current Requirements: Average – 50/75mA (12VDC)
   4. Operating Temperature: -40° to 150°F (-40° to 65°C)
   5. Operating humidity: 5-95% relative humidity, non-condensing
   6. Transmit and Excite Frequency: 125kHz and 13.56MHz
   7. The unit shall include an integrated weatherized keypad.
   8. The proximity reader/keypad shall be a HID Corp. model RPK40 with keypad or approved equal

D. Access Control System Integration
   1. Proximity readers and other token readers shall interface to the security network via serial device servers.
   2. Provide serial device servers that meet the following specifications;
      a. LAN: 10/100/1000 megabit switched Ethernet, RJ 45 Ethernet with built-in 1.5 KV magnetic isolation
      b. Serial Interface: RS-422 Signals: Tx+, Tx-, Rx+, Rx-, GND; 8 or 16 ports as required.
      c. Serial Line Protection: 15 KV ESD for all signals
      d. Power Line Protection: 1 KV Burst (EFT), EN61000-4-4; 0.5KV Surge, EN61000-4-5
      e. Built-in HMI, buzzer, real time clock, watch dog timer
      f. Serial Communication Parameters:
         1) Parity: None, Even, Odd, Space, Mark
         2) Data bits: 5, 6, 7, 8
         3) Stop bits: 1, 1.5, 2
         4) Flow control: RTS/CTS, XON/XOFF
         5) Speed: 50 bps to 230.4 kbps software features
         6) Protocols: ICMP, IP, UDP, DHCP, BootP, Telnet, DNS, SNMP, HTTP, SMTP, SNTP;
         7) Utilities: Real COM/TTY drivers, Linux real TTY driver; Configuration: Web browser, Telnet console, or Windows utility
      g. Power Requirements: Power input: 100 to 240VAC, 47 to 63HZ, or 12-48 VDC; Power consumption: 212 mA for 100V, 130mA for 240V
      h. Mechanical Specifications: Material: SECC sheet metal (1mm)
      i. Environmental Specifications: Operating Temperature: 32 to 131°F (0 to 55°C), 50- 95% RH; Storage Temperature: -4 to 167°F (-20 to 75°), 5 to 95% RH
      j. Regulatory Approvals: EMC: FCC Class A, CE Class A; Safety: UL, CUL, TÜV

k. Standard 19-inch rack-mountable

3. Provide quantity of serial device servers to interface to all proximity readers, proximity/keypad readers and other token readers as shown on the plans.

E. Door Position Switches (ADDENDUM 04)

1. Description: Balanced-magnetic switch, complying with UL 634, installed on frame with integral overcurrent device to limit current to 80% of switch capacity. Bias magnet and minimum of two encapsulated reed switches shall resist compromise from introduction of foreign magnetic fields.

2. Flush-Mounted Switches: Unobtrusive and flush with surface of door and frame.

3. Securitron DPS series, Schlage 679-95 series, GE 1076D series or approved equal.

4. Match device color to door frame when possible. Coordinate color selection with owner.

PART 3 - EXECUTION

3.1 INSPECTION:

A. Check location, “roughing in”, and field dimensions prior to beginning work.

B. Do not begin installation until all unsatisfactory conditions have been corrected.

C. Verify field measurements are as shown on Drawings and as instructed by manufacturer.

D. Verify that required utilities are available, in proper location, and ready for use.

3.2 INSTALLATION/APPLICATION OF ALL SECURITY PRODUCTS:

A. Field testing and inspection will be performed under the provisions of Section 285000.

B. Replace equipment, components, & wiring as required to achieve a fully functional system

END OF SECTION 285300