SECTION 28 13 00
ACCESS CONTROL SOFTWARE AND DATABASE MANAGEMENT

PART 1 GENERAL

1.1 PULL FROM PART 1 & 3 DOC

PART 2 - PRODUCTS

2.1 ACCESS CONTROL SOFTWARE AND DATABASE

A. The product or product types listed below describing various features shall be supplied by a single manufacturer for access control.

B. **Software for access control shall be Hanwha Vision OnCAFE**

1. Software
   a. Manufacturer: Manufacturer: Hanwha Vision (https://www.hanwhavision.com/en, https://hanwhavisionamerica.com)
   b. Model: OnCAFE (with licenses as defined below)
2. General Description:
   a. Licensing and Credentials
      1) Licensing shall only be required per entry and no per reader licensing shall be accepted
      2) Licenses shall be offered in scaled packs, supporting multiple entries in a license pack. Licenses shall be available in quantities of 1, 4, 8, 16, 32, 64, and 128 entries, as published on manufacturer's standard price list.
      3) Entity licenses shall be offered in 1 year duration with the option to apply renewal licenses with no loss of duration or downtime in operation.
         a. License part numbers:
            i. CA-1Y-ENTRY
            ii. CA-1Y-ENTRY4
            iii. CA-1Y-ENTRY8
            iv. CA-1Y-ENTRY16
            v. CA-1Y-ENTRY32
            vi. CA-1Y-ENTRY64
            vii. CA-1Y-ENTRY128
      4) System shall support BLE and Wallet based licenses, via licensing, and shall support both license types at a given location, simultaneously, without issue.
         a. Mobile credential license part numbers:
            i. BLE mobile credentials (qty 20): CA-1Y-BLE20
            ii. BLE mobile credentials (qty 100): CA-1Y-BLE100
            iii. BLE mobile credentials (qty 500): CA-1Y-BLE500
            iv. Wallet-based (Apple or Google) credentials: CA-1Y-WC20

b. Operational Requirements
    1) Access Control System shall be deployed through a cloud-based access control portal hosted by the manufacturer.
        a. The Access Control System Software shall be hosted in an Amazon Web Services (AWS) environment.
        b. Browser access for configuration and administration of the system shall be possible from any client PC.
        c. Security of the data communicated over the network to and from the browser, ACS software, and field panels shall be protected by 256-bit-encrypted HTTPS protocol – TLS protocol encryption.
        d. Distributed Processing - The field panels shall make and manage access control decisions with data provided by the ACS, and it shall manage the communication between the ACS and the system's inputs, outputs, and readers. This modular design shall make it possible, even during network downtime, for the system to continue to manage access control and store system activity logs. When network connectivity is re-established, the system activity logs shall be automatically re-integrated.
    2) The ACS shall integrate with, within a browser interface, access control, alarm monitoring, and video monitoring.
    3) All systems and components shall have been thoroughly tested and proven in actual use.
c. Software Requirements
    1) The system shall support a Cloud Infrastructure enabling system operators and administrators to monitor and control multiple distributed ACS field panels simultaneously.
    2) The system software shall be cloud native and entirely reside in the cloud. No software shall be required to be installed on any on-premises client or server.
    3) The software solution shall support an uptime of 99.5%.
    4) The ACS shall provide the following Monitoring capabilities:
        a. A Dashboard where key system details may be monitored.
        b. System Alarms
        c. Offline Device Status
    5) The ACS shall support any web browser.
    6) Software upgrade process:
        a. Shall be done in real time with no interruption to user activities.
        b. System licensing may be expanded as needed to a running system with no interruptions to any system activities.
    7) Data Security:
        a. The ACS shall use 256-bit-encrypted HTTPS protocol, TLS (Transport Layer Security) 1.3 and above for communication to the servers.
        b. The software database shall be stored in the cloud within AWS using AES-256-bit encryption.
        c. The system shall support Two-Factor Authentication.

d. The ACS shall comply with the California Consumer Protection Act (CCPA).
e. Communication between the field panels and the card readers shall use either:
    i. OSDP v2
    ii. OSDP v2 Secure Channel
    iii. Wiegand interface

8) Database Backups shall be automated by the Host Software and function as follows:
    a. All data (user, configuration, and historical) shall backed up in real time and in full.
    b. Backups shall be automatically stored the manufacturer's cloud (AWS).
    c. There shall be no limit to the amount of data that can be backed up.

9) Organization Details – The ACS shall define the customer instance at the Organization, Location, and Area levels.
    a. Organization level shall show a unique Organization ID (system generated and not user editable) and a Short Name (user defined)
    b. Locations shall be able to be viewed on a mapping instance without the user having to import any mapping details.
        i. Locations shall be auto-grouped and ungrouped, based on map view level, in order to optimize viewing and navigation.
    c. Organization Dashboard – The ACS shall include an Organization level dashboard including, but not limited to:
        i. Organization ID
        ii. Organization Short Name
        iii. Customer organization name
        iv. Organization Contact Details
            1. Address
            2. Phone Number
            3. Email Address
        v. Locations via mapping
        vi. Controller availability graph, with customizable view on duration and controller(s)
        vii. Total Entries (licensed and in use)
        viii. Mobile credentials (licensed and in use), delineated by type of BLE or Wallet
    d. Integrations – The ACS shall provide the ability to view and configure details of any available integrations including, but not limited to:
        i. Enable/Disable switch for integration
        ii. Current connection status
        iii. Details of integration
        iv. Configuration of integration

10) Identities – The ACS shall provide for the unified management of personnel via Identities, managing both physical access and logical access from the same software component.

a. All details for the Identity shall be visible from the Identity profile page including, but not limited to:
    i. View, Issue, Deactivate any/all credentials
    ii. Cardholder group(s) assigned
    iii. Access level(s) assigned
    iv. Recent activity
    v. Change log
    vi. Audit log of the identities' activity
b. Ability to deactivate individual credentials or the entire Identity, with full tracking of such action being taken and in place.
c. User Roles and Permissions - There shall be 'n' pre-programmed levels of User Roles, and a total of 'n' possible Custom User Roles that can be configured in the system with different permissions for each user:
    i. Preset User Roles
        1. Super Admin - System defined customer level role having access to resources of all the locations.
        2. Admin - System defined location admin role having access to all location resources.
        3. Operator – System defined user role with access to Badge Only user functions as well as system events, reports, and limited availability to entities.
        4. Cardholder Manager - System defined cardholder manager role having access to users and activity.
        5. Cardholder only - System defined user role having access to only access via credentials (no software login access).
    ii. Custom User Roles
        1. The system shall allow for the creation of Custom User Roles.
        2. Custom User Roles shall allow granular control of all resource permissions.
        3. Permissions shall include View-Only Access, or Full Access.
d. Passwords and Identity Management -
    i. Personnel data maintained in the system may also contain a username and password for logging on to the ACS platform as a system user. The system shall support the changing of administrator passwords.
    ii. Passwords shall require a minimum length of eight (8) characters, at least one uppercase letter, at least one lowercase letter, at least one number, and one special character.
    iii. Users shall be able to 'self-service' the password reset process without any requirement of an administrator.
e. Issuing and revoking cards (credentials):
    i. Physical credentials shall be assignable by the system user either by entering card data directly into the person record or by use of an 'auto-

enrollment' process, whereby the user can select a reader to receive the credential information. Access levels shall be assignable through the user interface by selection from the list.

ii. Physical credentials which have been deactivated shall show, in red text, to indicate that the credential remains issued to the identity but that it has been deactivated. Reactivation shall be possible via a 'single-click' interaction.

11) Cardholder Groups – The ACS shall provide means of defining Cardholder Groups as a means of managing the Access Level(s) assigned to multiple Cardholders simultaneously.
    a. Cardholder Groups shall have unique names and an optional Description field to be able to describe the use the that specific Cardholder Group
12) Controller Configuration – The ACS shall provide visual feedback of the controller hardware configuration so as to reduce errors and prevent confusion
    a. Visual indication shall match the controller/board hardware type actually in use and shall not be generic
    b. Visually differentiate reader port configuration between OSDP and Wiegand
    c. Indicate controller details without the need for navigation to the device page, or another application, to view
        i. Model
        ii. MAC Address
        iii. IP Address
        iv. Utilization
            1. Doors/Elevators
            2. Readers
            3. Inputs
            4. Outputs
    d. Indicate both Cloud Connector and Device Firmware current versions in the software without need for navigation to the device page, or another application, to view and set auto-update selector, along with auto-update timing interval.
13) Intrusion Panels - The ACS shall integrate with intrusion panels, arming the panels, disarming the panels, and triggering events based upon intrusion panel status.
14) Alerts - The ACS shall be able to notify users of designated conditions, via browser, mobile, or by sending an email, with the alert details for the following conditions:
    a. Controller – Connected, Disconnected, Fire Alarm Input Activated.
    b. Door – Opened, Closed, Forced Open, Locked, Unlocked, Access Granted, Access Denied, Open Too Long
    c. Input Group – Triggered, Normal, Activated, Deactivated
    d. Output Group – Activated, Deactivated
    e. No default alerts shall be configured and alerting shall be completely user defined via Alarms and Automations.
15) Access Control:
    a. Card Formats:

i. The ACS shall support up to 8 system defined card formats for physical credentials
ii. The ACS shall support mobile credentials in Apple Wallet, Google Wallet, and via Bluetooth credential.
1. Mobile credential support shall be via Wavelynx mobile credentials

b. Administrators shall be able to specify unique activation and deactivation dates for each credential in the system.
c. Administrators shall be able to specify a single credential as disable or specify a specific Identity from being disabled.
i. Disabling an Identity shall revoke all software access and access credentials.
d. Deletion of Identities, Cardholder Groups, Access Levels, and Entities within the ACS shall require the user to enter the name of that which is being requested for deletion in order to serve as a means of verification of the action performed.
e. Access Levels: The ACS shall support unlimited access levels.
f. The ACS shall support mobile credentials.
i. The use of mobile credentials shall be controlled entirely within the ACS software. There shall be no need for separate data entry or credential management.
ii. Mobile credentials shall support Bluetooth Low Energy (BLE) or Near-Field Communication (NFC) on both Android and iOS devices.

16) Visitor Management:
a. The ACS Visitor Management feature shall support unlimited visitors and devices.
b. The system shall support visitor pre-registration.
c. The system shall be configured that visitors can have credentials assigned to them, but these are only valid once the visitor has been checked into the location. All visitor credentials shall no longer have valid access rights upon visitor check out.

17) Reports:
a. The ACS supports a variety of predefined reports regarding software and security hardware configuration, event history, and the administration of people within the system.
i. Predefined reports shall include:
1. Audit Report
2. Event Report
3. Alarm Report

b. All reports shall have immediate access to the entire historical database.
c. There shall be no need to restore blocks of historical data to run a report that parses said data.

d. System reports showing events or alarms shall include graphical representation of the content included, with real-time filtering.
e. All system reports shall show the data, according to the report configuration, in table format including any associated Event Videos.
f. Report shall be able to be exported in either a CSV or PDF format.

d. Video Management Integration
1) The ACS shall support the integration of third-party video management systems.
a. OnCloud
b. Wisenet WAVE

e. Apple Wallet Integration
1) The ACS shall support provisioning access cards into the Apple Wallet.
2) The user shall be able to provision up to two devices (one iPhone and one Apple Watch).
3) The ACS shall support Express Mode where users do not need to unlock their device to use the access card stored in Apple Wallet.

f. Google Wallet Integration
1) The ACS shall support provisioning access credentials into the Google Wallet

g. Artificial Intelligence
1) The system will have artificial intelligence built into the user portal capable of creating schedules upon request and be able to do so upon direction via natural language processing.
2) Outputs from the AI generation shall be visually displayed for the user to confirm prior to saving.
3) User shall be able to modify the output, without having to remove all generated output, in order to refine as needed.

END OF SECTION 28 13 00

PART 3 EXECUTION

3.1 PULL FROM PART 1 & 3 DOC