PART 1 - GENERAL

1.01 DESCRIPTION OF WORK

A. Refer to 280500 Part 1

1.02 RELATED DOCUMENTS

A. Refer to 280500 Part 1

1.03 RELATED DIVISION PROVISIONS

A. Refer to 280500 Part 1

1.04 REFERENCES

A. Refer to 280500 Part 1

1.05 SUMMARY

A. This Section includes access control devices to be connected to the Security Management System (SMS).
   1. Access Control:
      a. Regulating access through doors, gates, traffic-control bollards and others access controls as specified in drawing documents.
      b. Anti-passback where required.
      c. Surge and tamper protection.
      d. Secondary alarm annunciator.
      e. Card readers.
      f. Biometric identity verification equipment.
      g. Push-button switches.
      h. RS-232 ASCII interface.
      i. Reporting.

1.06 DEFINITIONS

A. Refer to 280500 Part 1

1.07 SUBMITTALS

A. Refer to 280500 Part 1

1.08 COORDINATION

A. Refer to 280500 Part 1

1.09 QUALITY ASSURANCE

A. Refer to 280500 Part 1

1.10 MAINTENANCE & SERVICE

A. Refer to 280500 Part 1

1.11 SYSTEM DESCRIPTION

A. The access control system shall be a networked system and utilize an IP network. The system shall be coordinate with 280500.

1.12 PERFORMANCE REQUIREMENTS

A. Refer to 280500 Part 1

1.13 DELIVERY HANDLING & STORAGE

A. Refer to 280500 Part 1

1.14 PROJECT CONDITIONS

A. Refer to 280500 Part 1

1.15 EQUIPMENT AND MATERIALS

A. Refer to 280500 Part 1

1.16 ELECTRICAL POWER

A. Refer to 280500 Part 1

1.17 ENVIRONMENTAL CONDITIONS

A. Refer to 280500 Part 1

1.18 LIGHTNING, POWER SURGES, & GROUNDING

A. Refer to 280500 Part 1

1.19 COMPONENT ENCLOSURES

A. Refer to 280500 Part 1

1.20 ELECTRONIC COMPONENTS

A. Refer to 280500 Part 1

1.21 SUBSTITUTE MATERIALS & EQUIPMENT

A. Refer to 280500 Part 1

1.22 LIKE ITEMS

A. Refer to 280500 Part 1

1.23 WARRANTY

A. Refer to 280500 Part 1

PART 2 - PRODUCTS

2.01 MANUFACTURERS

A. The S2 NetBox™/Enterprise™ Security Management System shall be implemented through network appliance architecture with a three-tiered modular hardware hierarchy and embedded three-tier software architecture.
   1. The network appliance shall be capable of running on an existing TCP/IP network and shall be accessible, configurable, and manageable from any network-connected PC with a browser.
   2. Browser access for configuration and administration of the system shall be possible from a PC on the same subnet, through routers and gateways from other subnets, and from the Internet. Control and management of the system shall therefore be geographically independent.
   3. Security of the data communicated over the network to and from the browser, Network Controller, and nodes is protected by encryption (SSL 128-bit) or authentication (SHA-1).
   4. The top hardware tier is the Network Controller. Embedded on the Network Controller are an operating system, a web server, security application software, and the database of personnel and system activity.
   5. The middle hardware tier is the Network Node. The Network Node shall make and manage access control decisions with data provided by the Network Controller, and it shall manage the communication between the Network Controller and Application blades connected to the system's inputs, outputs, and readers. This modular design makes 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 are automatically re-integrated.
   6. The bottom hardware tier is the Application Blades. Four unique Application blades shall be available:
      a. Access Control Blade: shall support two readers, four supervised inputs, and four relay outputs.
      b. Alarm Input Blade: shall support eight supervised inputs.
      c. Relay Output Blade: shall support eight relay outputs.
      d. Temperature Blade: shall support eight analog temperature sensor inputs.

B. The S2 system shall integrate, within a browser interface, access control, alarm monitoring, video monitoring, and temperature monitoring applications. These applications shall be embedded in a three-tier software architecture.
   1. The database tier shall use PostgreSQL. PostgreSQL is a full featured, high performance database management system that supports ODBC. This shall provide a small footprint, low administration, and high reliability relational database that is embedded without requiring the use of a separate PC server.
   2. The web server tier shall be based on an Apache™ embedded web server. This shall provide a graphically rich security management application through a standard web browser.

3. The web browser shall provide UL 1076 compliant browser-based monitoring and incorporate asynchronous Javascript™ and XML technology (AJAX) for a faster user experience.
4. The security application software tier contains the business logic. This application shall also be embedded on the network device and requires no additional memory or processing power.
5. This three tiered embedded software design runs within an embedded Linux Ubuntu operating system and shall require no client-side software other than a web browser.

C. All equipment and materials used shall be standard components, regularly manufactured,
and regularly utilized in the manufacturer's system.

D. All S2 systems and components shall have been thoroughly tested and proven in actual use.

E. All S2 systems and components shall be provided with an explicit manufacturer warranty of one year for software and two years for hardware.

2.02 OVERALL SYSTEM CAPABILITY

A. The S2 NetBox™/Enterprise™ Security Management System shall meet the requirements of business and government access control systems. The system shall monitor and control facility access, and shall perform alarm monitoring, camera and video monitoring, communications loss monitoring, and temperature monitoring. The system shall also maintain a database of system activity, personnel access control information, and system user passwords and user role permissions. The system shall be controlled from a web browser and require no software installation or client licenses. The system shall provide control and access to users on Local Area Networks (LAN), Wide Area Networks (WAN), wireless networks, and the Internet. The system shall provide email and/or text message alerts for all alarm conditions and threats.

B. Widget Desktop: The S2 system shall provide a widget-based user interface that enables users to create custom monitoring layouts by selecting and arranging widgets on a desktop.
1. Each widget shall provide easy access to a frequently used function—allowing users to, for example, view an activity log, a camera view, or real-time web content.
2. System administrators can save custom layouts for subsequent call up by users, who can then arrange the widgets as desired on their desktops. The administrator shall determine which widgets are available in a layout and the extent to which users can customize the layout.
3. The widgets that shall be available for layouts are: Activity Log, Camera View, Clock, Duty Log Entry, Events, Explorer, Floorplans, Intrusion Panel, Passback Grace, PhotoID History, Portal Status, Portal Unlock, Statistics Block, Status, and Threat Level.
4. In addition, when the alarm workflow feature is enabled for the system, an Alarm Workflow widget shall become available for layouts. This widget shall allow operators to monitor and resolve alarms within the alarm workflow implemented for the system.

C. System Partitioning: The system administrator shall have the ability to divide the S2 system into partitions, allowing subsets of the overall population and/or resources to be managed separately.
   1. From the default Master partition, one or more additional partitions can be created.
   2. Each partition shall contain some number of administrators, card holders with their credentials, and resources.
   3. When performing administrative functions, the administrator of a partition shall have the ability to affect only the cardholders and resources in that partition. However, resources can be shared across partitions through the mapping of access levels from one partition to another.
   4. System partitioning shall have a precision feature that allows administrators in one or more partitions to view and perform edit functions on person records that belong to another partition.

D. The S2 system shall provide the following Access Control capabilities:
   1. Login throttling, which can be enabled for the system to limit the number of login attempts from the same IP address in a given period of time.
   2. Integrated photo ID creation capability with video verification.
   3. User interface secured access under encrypted password control.
   4. System-wide timed anti-passback function.
   5. Regional anti-passback with mustering and roll call functions.
   6. Region occupancy counting and control.
   7. “First-in-unlock” rule enforcement.
   8. Multiple access levels and cards per person.
   9. 128-bit card support for Wiegand card readers.
   10. Detailed time specifications.
   11. Simultaneous support for multiple card data formats.
   12. Elevator control.
   13. Access privileges variable by threat level.
   14. Scheduled portal unlock by time and threat level.
   15. Card format decoder quickly discovers unknown card formats.
   16. Card enrollment by reader or keyboard.
   17. Compatibility with various input devices, including biometric readers.
   18. Activation/expiration date/time by person with one minute resolution.
   19. Access level disable for immediate lockdown.
   20. Use of Threat Levels to alter security system behavior globally.
   21. Duress PINs, which can be enabled for the system to allow a valid user to raise an alarm if compelled under duress to use his or her credentials (card and PIN) to allow access for another person.
   22. Multiple holiday schedules.
   23. Timed unlock schedules.
   24. Scheduled actions for arming inputs, activating outputs, and locking and unlocking portals.
   25. Optional two-man access restriction for portals, requiring two valid card reads from two separate cardholders for portal entry.
   26. Card enrollment reader support.
   27. Dual-reader portal support.
   28. Wiegand Reader support.

29. Magnetic-stripe reader support with cards using ABA Track 2 format for up to 200 bits.
30. Wiegand keypad PIN support for 4-digit or 6-digit PINs.
31. 8-bit and 4-bit burst keypad support for 4-digit or 6-digit PINs.
32. Integration with supported alarm panels.
33. DMP intrusion panel high-level TCP/IP integration.
34. Optional storage and recall of ID photos and personal/emergency data.
35. Up to 60,000 person records.

E. The S2 system shall provide the following Monitoring capabilities:
1. Common alarm panel integration for disarm on access, and arm on egress.
2. Integrated alarm monitoring and event management with alarm panels.
3. Support for the direct viewing of IP cameras.
4. Integrated real-time IP, DVR, and NVR systems with stored video replay for events.
5. Provides alarms on video loss, video motion detection, and video restore events.
6. Virtual inputs for video loss and building-occupancy-limits-exceeded.
7. Provides alarms on communication loss and temperature variation.
8. Support for the creation of custom sets of alarm event actions.
9. Provides the ability to record video and link to video for alarm events.
10. Available video control and playback through the S2 System user interface.
11. Provides the ability to assign threat levels to various alarms according to severity.
12. Provides the ability to select up to 20 levels of priority for event actions.
13. Provides the ability to enter a duty log comment into the Activity Log, or to append a unique or preset comment to a particular log entry while viewing the Activity Log.
14. Support for the display of Activity Log entries that include both the time the event occurred on the node and the time it was reported to the controller.
15. Support for electronic supervision of alarm inputs.
16. Support for the use of output relays for enabling circuits under alarm event control.
17. A monitoring desktop that integrates video, system activity logs, floorplans, ID photos, and alarm notifications.
18. Support for the creation of unlimited customized monitoring layouts through the use of widgets.
19. Graphic floorplans with active icons of security system resources.
20. System user permissions to grant whole or partial access to system resources, commands, and personal data.
21. Secure access to the user interface under encrypted password control.
22. Delivery of alerts via browsers, email, and text messages.

F. The S2 system shall provide the following Video Management capabilities:
1. Real-time video monitoring displays, including unlimited cameras simultaneously.
2. Playback of event-related video.

3. Video switching and video widget pop-ups based on access activity or event activation.
4. Integrated alarm inputs from the video management system.
5. Digital playback of video events.
6. Linking of video and events based on triggers provided by the S2 system or video system.
7. Support for multiple DVR and NVR systems.
8. Multiple pre-programmed supported cameras.
9. Recall of photo ID and real-time image for comparison.
10. Monitoring and control through a web browser interface.
11. System user permissions to grant whole or partial access to system cameras and video resources.

G. The S2 system shall provide the following Security Database capabilities:
1. Maintain data of system activity, personnel access control information, system user passwords and custom user role permissions for whole or partial access to system resources and data.
2. Partitions: It shall be possible to partition the system to create independent, virtual security management systems for multiple populations.
3. Support for the sharing of access levels and user privileges across partitions in a system.
4. Built-in Open Database Connectivity (ODBC) compliant database for personal data.
5. LDAP integration for single-user logon authentication.
6. Unlimited person records.
7. Network-secure API for external application integration.
8. Extensive and easy to use custom report generator.
9. User-defined data fields in personnel records.
10. Record recall by vehicle tag, name, or card.
11. ODBC compliant Database.
12. An API for adding to, deleting from, and modifying the database.
13. Storage of system user passwords and permissions.
14. Storage and recall of ID photos and emergency personal information.
15. Pre-defined reports on system configuration, system activity history, and people.
16. An Audit Trail report that shows changes made to the security database over a specified period of time.
    a. For each transaction listed in the report results, information is available on when the transaction occurred, who made the changes, the fields that were modified, and the original and new values.
    b. Search criteria can be applied to filter the report results, either by the person whose record was changed or by the area of the system configuration that was modified.
17. A Credential Audit report that shows all existing access cards by their current status settings. The report also shows for each card the name of the person to whom it was issued and the card number.

18. A Duty Log report shows duty log comments residing in the current security database, including archives.
    a. For each duty log comment included in the report results, information is available on when the comment was entered, who entered it, the date and time of the logged event associated with the comment, the name of the logged event, and the specific comment text.
    b. Search criteria can be applied to filter the report results, either by Operator (the user who entered the duty log comment) or by Event type.
19. English-based query language for instant custom reports.
20. Custom report writer interface that allows the interactive creation of custom reports. Reports may be saved for later reuse. No third party software (such as Crystal Reports) shall be necessary.
21. Periodic backup to on-board flash ROM and optional network attached storage (NAS), including FTP servers.
22. Periodic archive creation for historical custom reporting and improved on-board database performance.
23. Email and text messaging (SMS) alert notifications.

2.03 HARDWARE REQUIREMENTS

A. The S2 NetBox™/Enterprise™ Security Management System shall employ a modular hardware concept that enables simple system expansion and utilizes a three-tiered hardware hierarchy:
    1. At the top tier is the Network Controller, which shall contain the database engine, web server, application software, and configuration data. It is at this level that System Users, through a browser interface, shall interact with the S2 system, set configurations, monitor activities, run reports, and manage alarms.
    2. At the second tier is the Network Node, an intelligent device with native TCP/IP support, which shall make and manage access control decisions.
    3. At the third tier are the application extension blades. Each of these blades shall connect to and manage a set of inputs, outputs, readers, cameras, or temperature monitoring points.
    4. The network device shall run on existing building TCP/IP networks and shall be configurable for access from separate subnets, through gateways and routers, and from the Internet.
    5. A MicroNode shall also be available that combines an Access Control blade and a Network Node.

B. The Network Controller shall contain the operating system, database engine, web server, application software, and configuration data. The Network Controller shall be available in four configurations to support small to medium, large, and ultra-large systems. Those systems shall be identified as: a solid-state NetBox Plus Network Controller, a solid-state NetBox Extreme Network Controller, an Enterprise Select Network Controller, and an Enterprise Ultra Network Controller.

C. A solid-state NetBox Plus™ Network Controller shall consist of a blade-style, circuit card that also combines a Network Node on the card. The Network Controller portion

of the card shall contain a processor, flash memory, and a network switch. The Network Controller shall be supplied with 12V DC at a minimum of 3 amps. Internal battery backup shall supply sufficient power to provide for an orderly shutdown of the system in case of loss of external power. External battery backup shall be used to provide uninterrupted operation in the event of external power loss. The Network Node portion shall contain a serial port for communication with the Application blades and a network interface port. A solid-state Network Controller shall have the following capabilities:

1. Nodes/MicroNodes 32
2. Access control portals 32
3. Access cards..... 60,000
4. Access levels 512
5. Card formats..... 32
6. Alarm input points 500
7. Control point outputs 500
8. Temperature monitor points..... 500
9. Elevators 20
10. Floors 100
11. IP, DVR, and NVR cameras ..... Limited only by license
12. Online event history log..... up to 10 million records
13. Ethernet ports 2
14. Time specifications 512
15. Time spec groups 64
16. Time specs per group 8
17. Threat Levels 8
18. Threat Level Groups 32
19. Holidays 30
20. Access levels per person 16
21. Cards per person 100
22. Report Groups..... 50
23. Camera Groups 50
24. Concurrent system users 2

D. The S2 NetBox™ Extreme Network Controller shall be available in wall-mount or 2RU rack-mount enclosure. It shall contain a motherboard with an Intel® Atom™ processor and solid-state disk drive. An Ethernet connector shall be provided for network connection. The NetBox Extreme Network Controller shall have the following capabilities:

1. Nodes/MicroNodes 64
2. Access control portals 256
3. Access cards.....150,000
4. Access levels.....512 per partition
5. Concurrent system users 10
6. Alarm input points 2000
7. Control point outputs 2000
8. Temperature monitor points:.....500
9. IP, DVR, and NVR cameras: .....Limited only by license
10. Online event history log:.....up to 40 Million records
11. Ethernet switch ports: 1

12. Time specifications .....512 per partition
13. Time spec groups .....64 per partition
14. Time specs per group .....8 per partition
15. Threat Levels .....8 per partition
16. Threat Level Groups .....32 per partition
17. Holidays .....30 per partition
18. Access levels per person 16
19. Cards per person 100
20. Report Groups 50
21. Camera Groups 50

E. The S2 Enterprise Select Network Controller shall consist of a 1U rack-mounted Controller with additional processing power and memory, disk drive, serial port and network connections. The S2 Enterprise Ultra Network Controller shall consist of a 2U rack-mounted controller with additional processing power and memory, RAID-1 disk drive array, serial port and network connections. The Enterprise Select and Enterprise Ultra Network Controllers shall have the following capabilities:

1. Nodes/MicroNodes .....128 (512 for Ultra)
2. Access control readers .....1792 (7168 for Ultra)
3. Access cards.....unlimited
4. Access levels.....512 per partition
5. Concurrent system users .....25 (35 for Ultra)
6. Alarm input points .....2000 (4000 for Ultra)
7. Control point outputs .....2000 (4000 for Ultra)
8. Temperature monitor points:.....500
9. IP, DVR, and NVR cameras: .....Limited only by license
10. Online event history log:.....up to 400,000,000 records
11. Ethernet switch ports: 1
12. Time specifications .....512 per partition
13. Time spec groups .....64 per partition
14. Time specs .....8 per group
15. Threat Levels .....8 per partition
16. Threat Level Groups .....32 per partition
17. Holidays .....30 per partition
18. Access Levels per person.....16
19. Credentials per person.....100
20. Report Groups.....50
21. Camera Groups 50

F. Enterprise Platform Attributes

		Enterprise Select:	Enterprise Ultra:
1. Physical			
	a. Dimensions (w, h, d)	19”x 1.7”x 19.6 (1U) ...	19”x3.46”x18.9 (2U)
	b. Weight:	7.28 Kg (16 lbs)	13.57 Kg (30 lbs)
	c. Power:.....	300W, 100–240VAC ...	300W, 100–240VAC
	d. Heat Output:	1024 BTU.....	1024 BTU
2. Platform		Enterprise Select:	Enterprise Ultra:
	a. Processor:	Intel Quad Core 2 2.6 GHz	Intel Quad Core 2 3.0 GHz
	b. RAM:.....	2G DDR2	4G DDR2

c. Storage:.....32G SLC SSD.....2 – 32G SLC SSD
d. DVD-R/W: .....Yes .....Yes
e. Ethernet Port:.....1 (10, 100, 1,000).....1 (10, 100, 1,000)
f. MTBF:.....52,560 hrs.....52,560 hrs

3. Environmental
   a. Operating Temperature .....0^0C - 40^0C (32^0F - 104^0F)
   b. Storage Temperature .....–20^0C - 60^0C (–4^0F - 140^0F)
   c. Relative Humidity .....10 to 85% at 40^0 (104^0F) non-condensing
4. Certifications
   a. Electrical.....CE, UL60950-1, FCC
   b. Environmental .....RoHS
5. Application Features Enterprise Select: Enterprise Ultra:
   a. Capacity Rating .....30.....96
   b. Portals (Nodes) supported .....1,792 (128).....7,168 (512)
   c. Inputs (Outputs) supported.....2,000 (2,000).....2,000 (2,000)
   d. Online Historical Transactions.....160,000,000.....160,000,000
   e. Simultaneous Users .....25.....35

G. The Network Node shall make and manage access control decisions with data provided by the Network Controller, and it shall manage the communication between the Controller and Application blades connected to the system's inputs, outputs, and readers. The Node shall be supplied with 12V DC at a minimum of 3 amps. The Node blade shall supply all Application blades in the node with power. The Network Node shall be available in three configurations: a combined Network Controller/Network Node blade; a standalone Network Node blade, and a MicroNode with included Access Control blade. Each Network Node shall support up to seven Application blades except for the MicroNodes. Communications between the node and Network Controller shall be encrypted and authenticated (SHA-1). Each Network Node shall have the following capabilities:

1. Application blades 7
2. Access control readers 14
3. Access Levels.....512
4. Portals 14
5. Portal Groups 64
6. Readers.....14
7. Reader Groups 128
8. Supervised Inputs.....56
9. Input Groups 64
10. Relay Outputs.....56
11. Output Groups.....64
12. Temperature Monitor Inputs.....56
13. Elevators 14
14. Floors 52
15. Floor Groups 64
16. Credential storage 20,000
17. Activity Log records 27,000

H. The Application blades shall interface with the Network Controller through the Network Node. The Application blades shall be blade-style circuit cards. There shall be four types of Application blades:
   1. Access Control blade: shall support 2 readers (input devices such as keypads, RFID devices or Biometric readers), 4 supervised inputs and 4 relay outputs.
   2. Supervised Input blade: shall support 8 supervised inputs. Supervised input connectors are 2-pin. The system shall support a wide variety of input supervision types including normally-open circuit and normally-closed circuits, and zero, one or two resistor configurations.
   3. Relay Output blade: shall support 8 relay outputs. Relay output connectors are 3-pin. Both normally-open circuit and normally-closed circuit output devices are supported. The relay outputs shall support any output devices that operate on the following maximum electrical ratings: 30 Volts DC or AC, 2.5 Amps inductive or 5.0 Amps non-inductive.
   4. Temperature blade: shall support 8 analog temperature sensor inputs. Temperature range shall be 32° to 158° F (0° to 70° C). Temperature precision within that range shall be ±1.0° F (±0.5° C).

I. The MicroNode shall combine a Network Node and an Application blade capability in one enclosure. The Access Control blade portion of the MicroNode shall support two readers, one temperature input, four supervised inputs and four relay outputs. A MicroNode shall utilize 12VDC power at 3 Amps or Power over Ethernet (PoE) at the 802.3AF standard and be capable of supplying direct power to 2 readers, 2 motion REXs, and 2 door strikes.

2.04 HARDWARE PACKAGING REQUIREMENTS

A. The S2 NetBox™/Enterprise™ Security Management System shall have various hardware enclosures and configurations available to support different installation requirements. Enclosures shall be available for wall or rack mounting. The wall-mount enclosures shall have a lock requiring a key, and a cabinet door tamper switch.

B. The S2 Wall-Mount enclosure supports one solid-state Network Controller/Node blade or a standalone Network Node blade and seven Application blades. The dimensions are: 17" (432 mm) H x 15" (381 mm) W x 6.75" (171.5 mm) D.

C. The S2 4U Rack-Mount enclosure supports one solid-state Network Controller/Node blade or a standalone Network Node blade and seven Application blades. The dimensions are: 19" (483 mm) W x 7" (178 mm) H (4U) x 15" (381 mm) D.

D. The S2 NetBox Extreme Network Controller wall-mount units shall be housed in an enclosure with dimensions of: 12" (304.8 mm) W x 14" (355.6 mm) H x 3.5" (88.9 mm) D. The rack-mount unit dimensions shall be 2U rack x 12" (304.8 mm) D.

E. S2 Enterprise Select Network Controllers shall be housed in a 1U rack-mount enclosure with dimensions of 19" (483 mm) W (including the mounting brackets) x 1.75" (0.7 mm) H x 16.75" (425 mm) D.

F. S2 Enterprise Ultra Network Controllers shall be housed in a 2U rack-mount enclosure with dimensions of 19" (483 mm) W (including the mounting brackets) x 3.5" (1.4 mm) H x 16.75" (425 mm) D.

G. The S2 MicroNode enclosure shall support a solid-state Node, its Access Control blade, and one temperature point.
   1. It shall be a wall-mount enclosure with dimensions of 7" (178 mm) H x 7" (178 mm) W x 3.5" (89 mm) D.
   2. It shall be possible to power the MicroNode with a 12VDC power source at no less than 2 Amps, or with PoE that conforms to the IEEE 802.3af standard. This provides nominal 48VDC at a maximum of 400mA.

H. The solid-state NetBox Controllers shall be powered by either 100-240V AC at 50-60 Hz, or by 12VDC at 3 amps. Power must come from a separate circuit with an isolated earth ground. If AC power is supplied it must be connected to the internal power supply. If DC power is supplied the internal power supply shall be bypassed. It shall be possible to backup power supplied to the S2 system with an Uninterruptible Power Supply (UPS). It shall also be possible to place within the wall-mount enclosure an SLA battery backup sufficient for an orderly shutdown in case of external power loss.

I. Enterprise and Enterprise Ultra controllers shall be powered by 100-240V AC at 50-60 Hz. Power must come from a separate circuit with an isolated earth ground and it must be connected to the internal power supply. It shall be possible to backup power supplied to the rack-mounted Enterprise and Enterprise Ultra controllers with an Uninterruptible Power Supply (UPS).

2.05 S2 NETWORK CONTROLLER, NODE, AND APPLICATION BLADE SPECIFICATIONS

A. S2 Solid-state Network Controller: All Application blades shall receive 12VDC power via the ribbon cable bus directly from the Node on the controller. The solid-state NetBox Plus Controllers shall be powered by either 100-240V AC at 50-60 Hz, or by 12VDC at 3 amps.
   1. Network Nodes Supported.....32
   2. Processor.....OMAP3503 ARM Cortex-A8 Core – 600 MHz
   3. RAM .....256 MB
   4. ROM .....32 KB
   5. Memory.....4 GB SD Card (Transcend Class 10)
   6. Operating Temperature.....32°to 122° F (0° to 50° C)

B. S2 NetBox Extreme Network Controller
   1. Network Nodes Supported.....64
   2. Processor.....Intel® Atom™ 1.6 GHz
   3. RAM .....1 GB
   4. Solid-State Disk Drive.....8 GB, 64 GB optional.
   5. Ethernet Ports.....1
   6. Operating Temperature.....32° to 95° F (0° to 35° C)
   7. Relative Humidity.....95% at 40° non-condensing
   8. Power Supply.....10 W, 85 to 260 VAC
   9. MTBF.....117,000 hrs
   10. Weight.....Wall-mount: 7.0 lbs. (3.2 kg)
       Rack-mount: 7.5 lbs. (3.4 kg)
   11. Heat Output.....82 BTU
   12. Storage .....8 GB SSD, optional 64 GB SSD
   13. Storage Temperature.....–20° C - 70° C

14. Electrical Certification.....CE, FCC Part 15
15. Environmental Certification...RoHS, WEEE
16. Capacity Rating.....10 eps

C. S2 Enterprise Select Controller
1. Network Nodes Supported 128
2. Processor.....Intel® Core 2 Quad 2.6 GHz
3. RAM 2G DDR2
4. Solid State Drive.....80 GB SATA
5. Ethernet Ports.....1
6. Operating Temperature.....0° to 40°C (32° to 104°F)
7. Storage Temperature.....–20°C - 60°C (–4° to 140°F)
8. Relative Humidity.....10 to 85% at 40°C (104°F) non-condensing
9. Power Supply.....300 W, 100 to 240VAC
10. MTBF.....52,560 hrs (calculated)
11. Weight.....16 lbs. (7.28 Kg)

D. S2 Enterprise Ultra Network Controller
1. Network Nodes Supported.....256
2. Processor.....Intel® Core 2 Quad 3.2 GHz
3. RAM .....4 GB DDR2
4. Solid State Drive.....2 x 80 GB SATA in RAID-1 configuration
5. CDRW/DVD-R.....Internal
6. Ethernet Ports.....1
7. Operating Temperature.....0° to 40°C (32° to 104°F)
8. Storage Temperature.....–20°C - 60°C (–4° to 140°F)
9. Relative Humidity.....10 to 85% at 40°C (104°F) non-condensing
10. Power Supply.....300 W, 100 to 240VAC
11. MTBF.....52,560 hrs (calculated)
12. Weight.....30 lbs. (13.57 kg)

E. S2 MicroNode: Each MicroNode shall function as a node and as an access control blade. In addition each MicroNode shall support one temperature input. The MicroNode may be supplied with 12VDC at 3 amps. With a 12VDC 3A power supply the total power available for all external output is 1100mA (13 watts). Alternatively, it shall also be possible to power the MicroNode by PoE that conforms to the IEEE 802.3af standard. This provides nominal 48 VDC at a maximum of 400mA. With PoE as the power source the total power available for all external 12V output is 500mA (6 watts).
1. 7-pin reader connectors.....2
2. Maximum reader wire length.....500 feet (152 m) (18 AWG twisted, shielded)
3. 2-pin supervised input connectors 4
4. Maximum input wire length.....2000 feet (610 m) (22 AWG twisted, shielded)
5. 3-pin relay output connectors.....4
6. Maximum output wire length.....Determined by the peripheral device
7. 2-pin analog temperature inputs.....1
8. Maximum temperature wire length....1000 feet (305 m) (18 AWG twisted, shielded)

F. S2 Access Control blade: The access control blade shall receive power via the ribbon cable bus directly from the Node Blade. The access blade shall supply up to 400 milliamps of power to one reader or 200 milliamps of power to each of two readers.
   1. 7-pin reader connectors 2
   2. Maximum reader wire length.....500 feet (152 m) (18 AWG twisted, shielded)
   3. Power available to readers .....400 milliamps
   4. 2-pin supervised input connectors 4
   5. Maximum input wire length.....2000 feet (610 m) (22 AWG twisted, shielded)
   6. 3-pin relay output connectors.....4
   7. Maximum output wire length.....Determined by the peripheral device

G. S2 Input blade: The input blade shall receive power via the ribbon cable bus directly from the Node Blade. It shall support a wide variety of input supervision types including normally-open circuit and normally-closed circuits, and zero, one or two resistor configurations.
   1. 2-pin supervised input connectors 8
   2. Maximum input wire length.....2000 feet (610 m) (22 AWG twisted, shielded)

H. S2 Output blade: The output blade shall receive power via the ribbon cable bus directly from the Node Blade. Both normally-open circuit and normally-closed circuit output devices shall be supported. The relay outputs shall support any output devices that operate on the following maximum electrical ratings: 30 Volts DC or AC, 2.5 Amps inductive or 5.0 Amps non-inductive.
   1. 3-pin relay output connectors.....8
   2. Maximum output wire length.....2000 feet (610 m) (22 AWG twisted, shielded)

I. S2 Temperature blade: The temperature blade shall receive power via the ribbon cable bus directly from the Node Blade.
   1. 2-pin analog temperature inputs 8
   2. Maximum temperature wire length....1000 feet (305 m) (18 AWG twisted, shielded)

2.06 SOFTWARE REQUIREMENTS

A. Operating System and Application Software:
   1. The embedded operating system for the solid-state S2 Network Controller shall be the Linux Ubuntu operating system. The disk-based S2 Enterprise and S2 Enterprise Ultra Network Controllers shall use Linux Ubuntu 10.04 LTS (long term support) as the operating platform. The operating system kernel shall be open-source and no operating system training or certification shall be necessary.
   2. The S2 system application software shall be embedded in the system. The database shall be an embedded PostgreSQL relational database requiring a small footprint and provides high reliability. The web server shall be based on an embedded Apache™ web server enabling users to access and operate the system using a standard web browser.

B. S2 Software Licensing:
   1. Software licensing shall be based upon the number of readers, cameras, and select features for one Network Controller. Software license upgrades shall be available if system reader and camera capacity must be raised.

The S2 user license shall be valid in perpetuity and shall include one year of software updates from the date of shipment from the factory.

2. Licensing shall be controlled by a Product Key and an Activation Key. The Product Key contains the licensed system features and limits. To upgrade your system license to enable more cameras or more doors you will need a new Product Key. The Activation Key contains the warranty expiration date. The keys are locked to the system license number. The system license number shall be viewable on-screen on the Support : About page

C. S2 Software Upgrades: Software upgrades shall be possible from a browser on any network-connected PC, by uploading a software update to the Controller. Controllers shall automatically upgrade all connected nodes. No client software installation shall be necessary.

D. Online Help and Documentation: The S2 system shall be provided with complete embedded documentation. The online documentation shall include:

1. Context-sensitive online Help. (The Help displayed is specifically relevant to the current screen.) The online Help system shall provide explanations and procedures for all monitoring, administrative, and system configuration and maintenance functions. The Help system shall have linked table of contents, a linked index, and frequently asked questions pages. Each topic shall also have links to related topics. Each Help topic shall be printable.
2. Technical Support Notes: These documents shall be in PDF format, shall be printable, and shall be linked to from the Help system table of contents, index, and related topics.
3. Installation Guides: These documents shall be in PDF format, shall be printable, and shall be linked to from the Help system table of contents, index, and related topics.
4. Video Integration Guides: These documents shall be in PDF format, shall be printable, and shall be linked to from the Help system table of contents, index, and related topics.
5. System Administration Guide: This document shall be in PDF format, shall be printable, and shall be linked to from the Help system table of contents, index, and related topics

E. S2 Support Collaboration: It shall be possible, by the use of a network Support Collaboration Tool, for a technical support specialist to connect to the S2 system and assist on-site technicians from remote network-connected locations. It shall only be possible for an on-site system administrator or technician to initiate this connection. There shall be no way to initiate this connection from outside the secure network.

F. Language Support: The S2 system shall be provided with multiple language support. The ability to switch from one language to another shall be accomplished through the user interface. Translation of the user interface, online help and documentation into other languages shall be available. The languages supported shall include:

1. English
2. Spanish
3. Portuguese

4. French
5. Italian
6. Thai
7. Chinese
8. Japanese

G. Date Formats: The S2 system shall support global date formats as follows:
1. mm/dd/yyyy
2. dd/mm/yyyy
3. yyyy/mm/dd

H. Floorplans: The S2 system shall provide graphic floorplan capability including graphic display of links to other floorplans, alarms, system resources such as portals, IP video cameras, inputs, outputs, and temperature monitoring points.
1. The Network Administrator holding at least a 'Setup' user role shall be able to graphically configure device icons onto the floorplan images, and to upload additional floorplan images. JPEG images shall be supported, and the maximum size for a floorplan image shall be 256K.
2. It shall be possible to create floorplan groups for the purpose of assigning or withholding assignment of these groups to system user permissions known as Custom User Roles. If a floorplan group is assigned to a particular system user then the floorplans in that group shall be viewable by that system user.

I. Personnel Data: The S2 system shall maintain person data relating to access control, system user privileges, photo identification, system activity, and contact information.
1. All person data in the system shall be integrated onto one tabbed page for viewing, editing, and deletion by system users.
2. A system user holding at least an 'Administer' user role shall be able to create, delete, and modify person records, including access levels.

J. Data Import and Export: A Data Management Tool shall be provided that supports, via an API, the import and export of personnel data. This tool shall make possible the pre-populating, and ongoing populating, of cardholders into the S2 system database. Data that shall be importable and exportable shall include:
1. LASTNAME
2. FIRSTNAME
3. MIDDLENAME
4. ACTDATE (activation date)
5. EXPDATE (expiration date)
6. NOTES
7. TEXT1...TEXT20 (user defined fields 1 through 20)
8. ACCESSLEVEL1...ACCESSLEVEL32
9. PERSONID
10. PIN
11. ENCODEDNUM1...ENCODEDNUM10
12. HOTSTAMPNUM1...HOTSTAMPNUM10
13. CARDFORMAT1...CARDFORMAT10
14. BADGELAYOUT
15. JPEG ID PHOTO

16. CONTACT PHONE
17. CONTACT EMAIL
18. CONTACT SMS EMAIL
19. CONTACT LOCATION
20. OTHER CONTACT NAME
21. OTHER CONTACT TELEPHONE
22. OTHER CONTACT TELEPHONE2
23. VEHICLE 1 COLOR
24. VEHICLE 1 MAKE
25. VEHICLE 1 MODEL
26. VEHICLE 1 STATE
27. VEHICLE 1 LICENSE#
28. VEHICLE 1 TAG#
29. VEHICLE 2 COLOR
30. VEHICLE 2 MAKE
31. VEHICLE 2 MODEL
32. VEHICLE 2 STATE
33. VEHICLE 2 LICENSE#
34. VEHICLE 2 TAG#
35. LASTMOD

K. Data Security:
1. Communication between the S2 Network Controller and the browser shall be secured using SSL. In addition, administrative access to the security management application and the personnel data shall be password protected and controlled by roles-based authorizations.
2. Communication between the S2 Network Controller and the S2 Network Nodes shall be encrypted and authentication/tamper detection shall be done using the SHA-1 algorithm.
3. Communication between the S2 Network Controller and other systems (when using the API) shall be secured using SSL and authentication/tamper detection shall be done using the SHA-1 algorithm.

L. Data Backups: It shall be possible to configure regular automatic database backups.
1. It shall be possible to back up a solid-state NetBox Plus Network Controller and NetBox Extreme Network Controller to an on-board compact flash.
2. It shall be possible to back up an Enterprise Select Network Controller and Enterprise Ultra Network Controller to a built-in hard drive.
3. It shall also be possible to save backups from any controller to separate network attached storage (NAS) and file transfer protocol (FTP) servers.
4. It shall also be possible to setup regular automatic creation of database archive files.

M. On-board Data Management: Each night the S2 system shall truncate a sufficient number of the oldest records held on-board to reduce the database to its set limit, if required. This shall create the needed storage space for additional system activity records. Truncation will be performed on a First-in, First-out (FIFO) basis.

N. Partitions: It shall be possible to create multiple partitions for the management of multiple security systems or multiple populations.
   1. It shall be possible to limit access to the data and resources of one partition to those with permissions for that partition.
   2. It shall be possible for each partition to have its own population, resources, rules, events, video management, log data, reports and network resources.
   3. It shall be possible to grant Monitor, Administer, and Setup privileges for multiple partitions to the same user. It shall also be possible to create custom user roles for each partition.
   4. A node can reside in only one partition. It shall be possible to create partitions without nodes.

O. User Roles and Permissions: There shall be four pre-programmed levels of User Roles, and a total of 16 possible Custom User Roles that can be configured in the system with different permissions for each user:
   1. Master Partition Monitor: These users may use the functions in the Monitor menu only within the Master (default) partition. Monitor functions shall include viewing the activity log, cameras, and floorplans.
   2. Master Partition Administer: These users may use the functions of both the Administration and Monitor menus only within the Master (default) partition. Administrative functions shall include adding and editing person information in the enrollment database, issuing and revoking cards, generating reports, and performing database backups.
   3. Master Partition Setup: These users may use the functions of the Setup, Administration, and Monitor menus only within the Master (default) partition. Setup functions shall include defining access control, alarm event behavior, camera settings, floorplan images and configurations, holiday and time specifications. Setup functions shall also include: designation of network resources such as time and DNS servers, email and network storage settings; performance of system maintenance such as database backup and restore, software updates and file cleanups; designation of time zone, daily backup schedule and enrollment readers.
   4. Full System Setup: These users may use the functions of all menus in all partitions.
   5. Custom User Roles: In addition to the roles above the system shall also support the creation of detailed user permissions regarding which cameras, floorplans, elevators, events, access levels, portals, reports, and personal data fields the system user may see, edit, delete, or control.

P. Alarm Panels: The S2 system shall be capable of integrating with alarm panels, arming the panels, disarming the panels, and triggering events based upon alarm panel status.

Q. DMP Intrusion Panels: The S2 system shall be capable of integrating with Digital Monitoring Products (DMP) XR500 Command Processor Panels.
   1. Security administrators can use events on a DMP panel, such as a zone going into an alarm state, to trigger events in the S2 system. They can also use events in the S2 system to control operations on the DMP panel, such as the arming or disarming of an area.

2. Monitors can use the Intrusion Panel widget to view configuration and status information for a DMP panel. They can also arm and disarm areas, bypass and reset zones, and activate and deactivate outputs associated with the panel.

R. Alarm Events: The S2 system shall be capable of managing alarm events.
   1. It shall be possible to delay an input's change to the Alarm state by a specified number of seconds. The range of delay options shall be .5 seconds or 1-120 seconds.
   2. It shall be possible to associate specific actions with each alarm event. These actions may include, but are not limited to:
      a. Lock and Unlock portals.
      b. Activate and Deactivate relay outputs.
      c. Arm and Disarm input groups.
      d. Pulse outputs or output groups.
      e. Arm and Disarm alarm panels.
      f. Send emails and SMS messages.
      g. Move cameras to preset positions.
      h. Switch to a video monitor.
      i. Record video.
      j. Momentarily unlock portals.
      k. Display ID photos.
      l. Change the system threat level.
      m. Make entries in the activity log.
      n. Play a digital sound file.
      o. Display alarms in different colors.
      p. Set a priority for an alarm (one of 20 levels, with 1 being the highest).
      q. Require a duty log entry.
      r. Clear alarm automatically or require an acknowledgement.
   3. A system user holding at least a "Setup" user role shall be able to create, delete, and modify alarm system inputs, input groups, outputs, output groups, alarm panels, and events.
   4. It shall be possible to trigger events based on system activity such as:
      a. Video motion detection.
      b. Camera failure and camera restore events.
      c. Valid or Invalid card reads.
      d. Portals held or forced open.
      e. Valid card reads with a specified access level.
      f. Inputs entering an alarm state.
      g. High and low temperature events.
      h. Alarm panel arming failures.
      i. Alarm panel zone faults.
      j. Tailgating and passback violations.
      k. Occupancy limit violations.
      l. Zone empty violations.
      m. Node power failure, communication failure, timeout, and tamper events.

S. Activity Monitoring:
   1. The S2 system shall support a Monitoring Desktop that integrates video, system activity logs, floorplans, ID photos, and alarm notifications.
   2. Activity Log viewing includes one-click navigation to person records.
   3. The system shall support a Widget Desktop that allows the creation of custom monitoring layouts. Within a custom layout, widgets display live video, system activity logs, alarm notifications, ID photos, floorplans, duty log entries, portal status displays, and DMP intrusion panels.
   4. Many widgets support multiple partition viewing and filtering. For example, the Activity Log widget can display data from multiple partitions and data filtered by event type or reader group, and/or based on the text content of the event.
   5. It shall also be possible to view cameras, activity logs, and floorplans on separate monitoring pages within the application.

T. Network-based Camera and Video Surveillance: The system shall provide live IP video surveillance capability. The number of supported cameras shall be limited only by license. The system's video capabilities shall include video monitor switching based on access activity. The system shall provide monitoring, configuration, and administration of IP video. Cameras can be separately monitored or monitored in groups.
   1. Presets: The system shall support the creation, deletion, and editing of camera preset positions in the system. It shall also be possible to save changes in preset positions directly to a camera website.
   2. Views: The system shall support the creation, deletion, and editing of multiple camera views, specifically Quad views (four cameras). The application shall provide a drop down pick list for selecting current views or naming of new views.

U. Access Control:
   1. The S2 system shall be able to make access control decisions, define a variety of access levels and time specifications, write system activity into a log file, maintain a personnel enrollment database, receive signals from input devices such as door switch monitors, card readers and motion detectors, energize devices such as door locks and alarms via outputs.
   2. Time Specifications: The system shall be capable of storing up to 512 time specifications. Each time specification must be assigned a unique alphanumeric name of up to 64 characters. The definition of a time specification shall require the assignment of both a start time and an end time. Each day of the week shall be individually assignable for inclusion in time specifications. Up to three holiday groups shall be assignable for inclusion in time specifications. If no holidays are assigned to a time specification then no holiday access shall be allowed.
      a. Time specifications shall be assignable to access levels, output groups, portal groups, input groups, and alarm events.
      b. Time specifications shall function appropriately per node for the time zone specified for that node.
   3. Card Formats: The system shall support the use of readers that use the Wiegand Reader Interface. The system shall default to the Wiegand 26 bit format unless a different bit length format is created in the system. The

system shall support but not require the use of the card facility code. The system shall also support the use of the Magnetic Stripe ABA track 2 card data formats.

a. It shall be possible to create new card formats, designate start bits and bit lengths for facility codes and card ID numbers, as well as designate parity bits. The system shall support up to 32 different card formats. The system shall support card formats up to 128 bits.
b. It shall be possible to reverse the read order of the bits in the facility code and/or card ID portions of a card format.
c. It shall be possible to view and change the default parity bit definitions for a card format.

4. Access Levels: The system shall be capable of storing up to 512 access levels in each partition. Each access level must be assigned a unique alphanumeric name of up to 64 characters. The definition of an access level shall require the assignment of a reader or reader group, and a time specification. It shall be possible to also assign an elevator floor group to an access level.
5. First-in Unlock Rule: The system shall support the use of a First-in unlock rule. It shall be possible to use this rule to control the unlock behavior of portal groups with assigned unlock time specs.
   a. The First-in unlock rule shall require a card read of a specified access level. The portals in the group shall unlock only when the rule is satisfied and the unlock time spec is valid.
   b. There can be up to 64 First-in unlock rules in the system at a time.
6. Double Card Presentation: The system shall support the use of a Double Card Presentation mode. This mode shall allow the presentation of a card twice in quick succession at a designated reader. Such a “double read” shall change the locked portal to an unlocked state until a subsequent relock event or user-designated timeout occurs. The double card presentation mode shall be enabled on an individual portal basis and shall also require a designation on the access level assigned to the cardholder. The mode shall adhere to time spec and threat level restrictions.
7. Keypad timed unlock: It shall be possible to enable a timed unlock feature for a portal that has a combination reader/keypad device. Once this feature is enabled, any cardholder with valid access to the portal shall be able to specify how long the portal will remain unlocked.
   a. A cardholder presents his or her card and then enters the associated PIN, followed by the number sign (#) and the number of minutes (1-99) the portal should remain unlocked.
   b. The portal will remain unlocked for the specified number of minutes, unless it is closed before the timer expires. If the portal remains open after the timer has expired, a [Door Held Open] alarm will be activated.
   c. If reader/keypad devices are located on both sides of the portal, cardholders will be able to use either device to initiate a timed unlock.
8. Holidays: The system shall be capable of storing up to 30 holidays per partition. Each holiday must be assigned a unique alphanumeric name of

up to 64 characters. The definition of a holiday shall require a start date and an end date. Holidays shall have the ability to span several days using only one holiday slot. Holiday definitions shall support the designation of a start time and an end time. If no start time is designated then the system shall default to 00:00 (start-of-day). If no end time is designated then the system shall default to 24:00 (end-of-day). Holidays shall require the use of 24-hour time format, e.g. 17:00 is 5:00PM.

9. Portals: A portal is any access point and each portal supports up to two access reader devices. The System User, holding at least a "Setup" user role, shall be able to view current portal definitions, change portal definitions, delete portals, and create new portals. Creating a portal defines the access and alarm behavior of the access point. This can include:
    a. Card readers and keypads.
    b. Output for locking.
    c. Input for monitoring the door switch.
    d. Input for a Request-to-Exit function.
    e. Local alarm outputs and system alarm events.
10. Portal Groups: It shall be possible to create groups of portals and to assign an unlock time specification to the entire group. All the portals in the group shall remain unlocked during the time specified.
    a. It shall be possible to use portal groups for the purpose of assigning or withholding assignment of these groups to system user permissions known as Custom User Roles. If a portal group is assigned to a particular system user then the portals in that group shall be viewable and unlockable by that system user.
11. Portal Alarm Conditions: Portals shall have four alarm conditions. The four alarm conditions are as follows:
    a. Forced: When a portal is opened and there has been no card read, nor request to exit.
    b. Held: When a portal is held open past the expiration of the shunt timer.
    c. Invalid: When the portal reader reads a card for which there is no entry in the database.
    d. Valid: When the portal reader reads a card for which there is a valid entry in the database.
12. Two-man entry restriction: It shall be possible to require two valid card reads by different cardholders within a specified number of seconds for entry to a specific portal.
13. Anti-passback: The system shall support both regional and timed anti-passback access control. For anti-passback functions, it shall be possible to configure regions, assign readers to those regions, and specify events for response to tailgate, passback, and occupancy limit violations. It shall also be possible to designate parent regions for hierarchical anti-passback.
    a. Grace: It shall be possible for a system Monitor or Administrator to Grace card holders from passback and tailgate violations.
    b. It shall also be possible to set a specific time for all cardholders to be Graced daily.

c. The system shall be able to automatically place the cardholder in a predefined region upon the selection of the grace option

14. Mustering: To aid in evacuation management it shall be possible to designate a region or regions for mustering. It shall be possible to quickly get an occupancy count and occupant list for any region.
15. Scheduled Actions: It shall be possible to specify system actions to occur at scheduled times. When scheduling an action, it shall be possible to specify whether the time specifications for the scheduled action will be based on the time zone set for the local Network Node or the time zone set for the Network Controller. Scheduled actions can include:
    a. Arming and disarming inputs.
    b. Activating and deactivating outputs.
    c. Locking and unlocking portals.
16. Floorplans: The system shall be capable of displaying active graphic floorplans and configuring each floorplan with icons representing system resources: cameras, portals, temperature points, and alarms. A network administrator holding at least a 'Setup' user role shall be able to upload floorplan images and graphically configure device icons onto the floorplan images. Viewing floorplans will require the Macromedia Flash Player 9.0 plug-in for the browser.
    a. It shall be possible to create floorplan groups for the purpose of assigning or withholding assignment of these groups to system user permissions known as Custom User Roles. If a floorplan group is assigned to a particular system user then the floorplans in that group shall be viewable by that system user.
17. Elevator Control: The system shall be capable of controlling elevator access to floors. The system shall be capable of controlling up to 52 floor buttons per node. It shall be possible to create, change, or delete floor groups to assign a free access time specification to a floor group. The floors in this group will be freely accessible during the times defined by the chosen time specification.
    a. It shall be possible to create elevator groups for the purpose of assigning or withholding assignment of these groups to system user permissions known as Custom User Roles. If an elevator group is assigned to a particular system user then the elevators in that group shall be viewable by that system user.
18. An S2 system user holding a "Setup" user role shall be able to create, delete, and edit access control specifications.

V. Threat Levels:
1. It shall be possible to configure up to eight threat levels. It shall be possible to alter security system behavior through the use of threat levels. Groups of threat levels may be created and assigned to portal groups, access levels, input groups, output groups, floor groups, and event actions. The behavior of groups, access levels, and event actions with assigned threat level groups shall change based upon the current system threat level.
2. The S2 system shall support 32 threat level groups.

3. It shall also be possible to change the system threat level in response to an alarm event.
4. The current system threat level shall display in the title bar of the security application interface and on floorplans.

W. Location-based threat levels: The system administrator shall have the ability to define locations. This allows for threat levels to be assigned to individual locations.
1. Within each parent location, sub-locations can be created, and additional sub-locations can be created within each of these, and so on. This creates a location hierarchy.
2. Portals can be assigned, and threat levels applied, to any location within the hierarchy.

X. Reports:
1. The S2 system shall be capable of producing a variety of predefined reports regarding software and security hardware configuration, event history, and the administration of people within the system. In addition, an easy to use query language shall be included to create ad hoc reports. The query language shall be documented in the online help system. Alternatively, it shall be possible to specify a query by use of point-and-click.
2. It shall also be possible to produce reports directly from the Network Controller based on data in archive files on FTP servers, network attached storage, or the controller-attached compact flash.
3. The S2 system shall support a graphic interface for interactively building custom reports from either historical or personnel data. These reports shall be savable for later reuse. Parameters can be inserted into reports to prompt for data input at report runtime. Report results can be printed, output to a PDF file or put into a spreadsheet.
4. It shall also be possible to group reports for assignment to custom user roles. Any reports not grouped and assigned to a custom user role shall not be viewable by that system user.
5. Report generation shall not affect the real-time operation of the system.
6. The specific reports provided shall include the following:
    a. Configuration Reports
        1) As Built: A graphical report that displays an image of each Application blade in a node and the specific resources (inputs, outputs, readers, etc.) configured for that blade. The network settings for the node shall also be included.
        2) Cameras: Displays all camera configuration information including control address, IP port, and camera type.
        3) Camera Presets: Displays configured presets for each camera in the system.
        4) Elevators: Displays elevator configuration information including Node, Reader, and Floor to output mappings.
        5) Floor Groups: Displays all configured floor groups for use in elevator control.
        6) Holidays: Displays holiday specification information.

7) Portals: Displays portal definition information including reader, DSM input, REX input, alarm outputs, and events.
8) Portal Groups: Displays a list of all defined portal groups.
9) Reader Groups: Displays defined groups of readers.
10) Resources: Displays all configured system resources including readers, inputs, outputs, elevators, and temperature points.
11) Threat Level Groups: Displays all configured threat level groups and the threat levels assigned to them.
12) Threat Levels: Displays all configured threat levels including the description and color assignment.

b. History Reports
1) Access History: Displays access history based on an entered query. The system user can specify the query using either the keyboard or point-and-click selection.
2) Custom Report: This provides the capability to create custom reports of historical data. A graphic interface provides the user with the ability to interactively create and save reports for later use. Parameters can be inserted into reports to prompt for data input at report runtime. Report results can be printed, output to a PDF file or put into a spreadsheet.
3) General Event History: Displays time, type of activity, and activity details for a variety of event types. The system user can select the specific event types for the report.
4) Portal Access Count: Display how many times users have used a portal.
5) Audit Trail: Displays an audit trail of system changes and the name of the system user that made the changes. It shall be possible to specify the dates and times covered in the report.
6) Duty Log: Displays duty log comments residing in the current security database, including archives.

c. People Reports
1) Access Levels: Displays all access levels entered into the system including time specification, reader/reader group, and floor group.
2) Current Users: Displays a list of all security system users currently logged in to the security system website.
3) Custom Report: This provides the capability to create custom reports of personnel data. A graphic interface provides the user with the ability to interactively create and save reports for later use. Parameters can be inserted into reports to prompt for data input at report runtime. Report results can be printed, output to a PDF file or put into a spreadsheet
4) Occupancy: Displays a list of defined regions with the number of people currently occupying each region and the maximum number of occupants allowed, if a maximum has been specified.
5) Photo ID Gallery: Displays all the photo ID pictures in the system and the person's name.

6) Photo ID Requests: Displays all outstanding badge print requests and lists ID, name, badge layout, activation date, request date.
7) Portal Access: Lists people with access for a selected portal.
8) Roll Call: Allows you to select a defined Region from the drop-down and see a list of people currently in that region.
9) Roster: Displays every person entered into the system and it lists name, ID photo, expiration date, username, and access level.
10) Time Specifications: Displays all defined time specifications currently in the system.

Y. Administration: The S2 system shall provide for the performance of system administration tasks from any network-connected computer with a browser. Most of the administrative, maintenance, and configuration utilities and functions shall require a S2 system user with at least a "Setup" user role. Information from the network administrator shall, in many cases, also be required. These administrative tasks shall include but not be limited to:

1. Generating reports:
   a. The system shall be capable of producing a variety of predefined reports regarding software and security hardware configuration, event history, and the administration of people within the system.
   b. Alternatively, the system shall support a graphic interface for interactively building custom reports from either historical or personnel data. These reports shall be savable for later reuse. Parameters can be inserted into reports to prompt for data input at report runtime. Report results can be printed, output to a pdf file or put into a spreadsheet.
   c. It shall also be possible to group reports for assignment to custom user roles. Any reports not grouped and assigned to a custom user role shall not be viewable by that system user.
   d. A system user holding "Administrator" permissions shall be able to view and create reports.
2. Database backups:
   a. The system shall create database, or full system data backups, each night at 00:15 hours. These backups shall be stored in ROM and compact flash onboard the solid-state Network Controller, and written to the drive on the disk-based controller.
   b. Backups shall also be written to network attached storage (NAS) or an FTP server if such storage has been configured in the system.
   c. It shall also be possible for the system users to create such database backups at any time. Any database backups onboard the Network Controller may also be downloaded to off board storage by the system user at any time.
3. System restore:
   a. The system shall be able to restore its database, or the full system data, from a backup. Restoration of the system shall only be possible from a backup copy onboard the Network Controller. It shall,

therefore, be possible to upload a copy of a database backup from any network attached storage.

b. It shall be possible to review backups by date and description and select the desired backup for upload to the Network Controller or restoration as the current system database.

4. Software updates:
   a. Software updates, upgrades and patches shall be provided from time to time. The system shall be able to update its software from these .tgz files. Update of the application software shall only be possible from an update file onboard the Network Controller. It shall, therefore, be possible to upload a copy of the software update from any network attached storage or from any PC drive or desktop.
   b. Software updates may involve the Network Controller only or may include updates for the node(s) also. The monitoring of the security system may be unavailable for several minutes during this process.
5. File cleanup: A utility shall be provided to assist in file cleanup. This utility will display for review and deletion all floorplan jpeg files, photo IDs, database backups, badge layouts, and software updates.
6. File upload: The system shall support uploads of files for use in and with the system. Files which shall be uploadable include:
   a. Floorplans in jpg format
   b. Badge layouts
   c. ID photos in jpg format
   d. Database backups
   e. Software license files
   f. software updates
   g. Threat level icons in jpg format
   h. Sound files (.wav) for use in event alerts
7. Setting system time, time zones, and time servers:
   a. The system shall support the setting of time zones by selection off of a drop down pick list. Time zones shall be separately settable for the controller and for each node or MicroNode in the system. An extensive list of world-wide time zones shall be provided. Adjustments for daylight saving time (summer time) shall be automatic.
   b. The system shall support the use of network time servers. Up to three time servers can be designated. Use of a network time server ensures that the Network Controller and its nodes will be regularly synchronized with the exact time used by all other network resources.
   c. It shall also be possible to manually set the system date and time.
8. Changing passwords:
   a. Person data maintained in the system may also contain a user name and password for logging on to the security application website as a system user. The system shall support the changing of administrator passwords. It shall be required to enter the password twice for verification purposes. Passwords may contain neither double-quote (“) nor single-quote (‘) characters.

b. It shall also be possible to integrate an LDAP server for single-user logon authentication. This will reference the LDAP-stored password for use by the system.

9. Issuing and revoking cards (credentials):
   a. Access cards shall be assignable by the system user either by entering card data directly into the person record or by use of an enrollment reader. Access levels shall be assignable through the user interface by selection from a drop-down list.
   b. Access cards shall be revocable at any time. A system user holding at least the Administer user role may perform this action. Revoked cards shall stop functioning immediately.
   c. A system user holding at least the Administrator role may also disable an access card by changing its Active status to Clear, Damaged, Disabled, Forgotten, Lost, Not Returned, Not Validated, Returned, Stolen, or Suspended. The card will not function with any of these status settings. Running a Credential Audit report shall allow existing cards to be viewed by their current status settings.
   d. A maximum number of active cards per person can be enabled for the system. Once a person has reached the system limit, a new card can be added for that person only if one of his or her active cards is revoked or disabled.
10. Enrolling new people: All person data entered into the system shall be held in the system database and shall be available only to system users holding at least the Administer user role. Person data can be added, deleted, and edited by such system users.
11. Creating Photo IDs: The system shall include an integrated photo ID function. It shall be possible:
   a. To design badge layouts,
   b. To upload badge layouts for badge printing,
   c. To capture ID photo images, print badges, and delete uploaded badge layouts.
   d. For the system user to manage all photo ID functions entirely from within the browser
12. Configuring network resources:
   a. DNS: The system shall support setting IP addresses for up to two domain name servers.
   b. Email settings: The system shall support the use of email notifications of alarm events. The system user must setup the email server IP address or DNS name and the email address of the Network Controller. A network administrator must setup the network mail server to relay email for the IP address of the Network Controller.
   c. File transfer protocol (FTP): The system shall support the use of an FTP Server for backups. Once configured, backups are automatically saved to the FTP server each night.
   d. NAS: The system shall support the use of network attached storage devices for backups. The network administrator must create a domain user account for the Network Controller and a password.

The system user must configure the network attached storage in the system including the domain name, server IP address, share name, and the directory where the Network Controller may store data.

e. Time Servers: The system shall support the use of network time servers. Up to three time servers can be designated. Use of a network time server ensures that the Network Controller and its nodes will be regularly synchronized with the exact time used by all other network resources.

f. A system user holding "Setup" permissions shall be able to configure network resources.

13. LDAP: It shall be possible to configure an Active Directory Server with the S2 system.
    a. This shall provide single user-login capability.
    b. Password rules and authentication will be governed by the LDAP server.

2.07 VIDEO MANAGEMENT INTEGRATION

A. General: The S2 NetBox™/Enterprise™ Security Management System shall support the integration of Digital Video Recorders (DVR) supporting analog video cameras and Network Video Recorders (NVR). This integration shall allow the viewing of live streaming video in the browser interface and recorded video playback. Viewing live streaming video shall require the Java™ 2 Runtime Environment version 1.4.2 or version 5.0.
   1. Events in the alarm subsystem can initiate video recording. Video motion detection, camera up and camera down messages from the VMS can initiate alarms.
   2. It shall be possible to monitor DVR and NVR cameras in the same views as IP cameras. VMS events shall be logged in the system activity log. It shall be possible to view recorded video of events from the Activity Log.

B. Integrated DVR/NVR Systems:
   1. Dedicated Micros – Generation 2 and Generation 3 DVR DS2 or DV-IP
   2. exacq – exacqVision
   3. JVC – VR900
   4. Milestone Systems – XProtect Enterprise, XProtect Professional, XProtect Corporate
   5. OnSSI – NetDVMS, NetDVR
   6. Panasonic Digital Disk Recorder – WJ-HD309a, WJ-HD316a
   7. Salient Systems CompleteView NVR
   8. Samsung iPOLiS NVR
   9. Vicon – ViconNet

C. OVID: Open Video Interface API:
   1. This specification defines an API to implement the integration of video surveillance systems with the S2 system.
   2. The OVID API shall allow users to monitor and control one or more video servers along with their associated video cameras, to augment the physical

security devices (door locks, card readers, etc.) controlled by the S2 system.

3. The integrated system shall be controlled through a web browser user interface which presents an integrated view of both the S2 system and the video surveillance system.

2.08 MERCURY HARDWARE INTEGRATION

A. The S2 system shall support the integration of access control hardware from Mercury Security Corp.

B. The following Mercury hardware components shall work with the S2 Controller:
   1. Supported Mercury Panels:
      a. EP2500: Intelligent Controller: 32 MB RAM, Ethernet
      b. EP1502: Intelligent Dual Reader Controller: 16 MB RAM, Ethernet, 2 readers (magnetic stripe or Wiegand) 8 inputs, 4 relays
      c. EP1501: Intelligent Single Door Controller: PoE, single door, 2 readers, 2 inputs, 2 outputs
   2. Supported Mercury Interface Boards (SIOs):
      a. MR-50 Reader Interface Module: 1 reader (magnetic stripe or Wiegand), 2 inputs, 2 relays
      b. MR-52 Reader Interface Module: 2 readers (magnetic stripe or Wiegand), 8 inputs, 6 relays
      c. MR-16in Input Monitor Module: 16 inputs (zones), 2 relays
      d. MR-16out: Relay Output Control Module: 16 relays

2.09 API INTEGRATOIN

A. An application programming interface (API) is provided for the S2 NetBox™/Enterprise™ Security Management system. The API provides programmatic access to the network-connected components managed by the S2 system.
   1. Communication between the S2 system and another application takes place through the TCP/IP networking protocol. The API is invoked by POSTing an HTTP message to the web server on the S2 Network Controller.
   2. The S2 database includes a table of “people” whose records act as container objects for attributes attached to people in real life. People are mapped to access levels, which specify access privileges—and to access cards, whose credentials are used for access control.
   3. Access levels are created in the system using the normal web user interface for the S2 system. People and credentials may be entered into the system either through the web user interface or through the API.
   4. The API supports commands for:
      a. Adding, modifying, removing, and retrieving data about a person, and retrieving information about one or more people based on various search criteria.
      b. Adding, modifying, and removing credentials, and retrieving a list of the names of defined card formats.

c. Adding, modifying, and deleting access levels, and retrieving a list of the valid access levels in the system.
d. Pinging the S2 system to determine its health, and retrieving the current version of the API from the server.
e. Retrieving a history of access activity, either for all users or for a particular access card.
f. Adding, modifying, and removing threat levels and threat level groups, and setting the threat level in the system.
g. Retrieving a list of portals and associated card readers defined for the S2 system.
h. Adding, modifying, deleting, and retrieving time specifications and time specification groups.
i. Adding, modifying, and deleting holidays, and returning a list of holiday keys or a specific holiday.
j. Adding, modifying, deleting readers and reader groups, and returning a list of reader group keys or information for a specific reader group.
k. Adding, modifying, and deleting portals and portal groups, and retrieving information about a specific portal group.
l. Requesting events from the Activity Log that occurred within a specified time period. These events are returned from the API in the CSV Export report format.

2.10 CARD READERS

A. Card readers shall be HID RP 15 multi class mullion mount reader or approved equal.

2.11 DOOR LOCK POWER SUPPLIES:

A. The Contractor shall provide a dual power supply for each DGP. Each power supply shall provide 24 VDC power to all electric locks and 12DC for DGP power. Each door's electric lock circuit shall be fused independently at the power supply enclosure (on DIN Rail terminal). Shorting or a single door lock circuit shall not affect other doors connected to a common door lock power supply. One (1) power supply shall be provided for each DGP. The door power supply shall include rechargeable standby power to provide a minimum of eight (8) hours of stand-by power at peak usage for door locks and DGP 12VDC. The power supplies shall be connected to the emergency generator circuit. The contractor shall provide separate low battery and AC power fail for the DGP and door power supplies.
   1. All locks shall be fail secure. All door lock hardware shall provide for free egress from the protected area by activating the door handle or push bar. Door locks and hardware are provided by Division 8, with connection to this hardware by Security Contractor (Division 280500).
   2. The power supplies shall meet the requirements of the data gathering panel manufacturer. All data gathering panels shall be supplied with rechargeable batteries. The rechargeable batteries shall be sized to provide a minimum of eight (8) hours of standby power for each power supply within the cabinet. Refer to Power Supply Specification.

2.12 LINE SUPERVISION

A. Communications between the host computer and the data gathering panels shall be protected against compromise. The system shall detect substitution of resistance or electrical potential, substitution of like equipment, and introduction of synthesized signals. Protective circuits (alarm inputs) shall be protected between the data gathering panel and the sensing devices (door contacts, motion detectors, etc.). Each circuit shall be supervised by end or line resistors located at the sensing device. The contractor must receive written approval from SI to locate the resistor elsewhere unless the drawings require this. The system shall detect resistance changes and report alarm and trouble signals at designated values defined by the system manufacturer. The system shall register a minimum of four (4) states: normal, alarm, trouble open (cut), and trouble closed (shorted). Trouble signals shall be displayed to the operator in a format readily identifiable by the operator as a supervisory condition.

2.13 CONTROL POINT FUNCTIONS

A. The system shall support at least 5,000 control point outputs which may be used to control external equipment and lighting. The system shall allow manual operation of non high security control points from the security console video display terminal, based on software established operator privilege levels, as well as automatic operation of control points by time and day. The system shall support named groupings of control points, which may be used to operate large numbers on control points with single commands. The system shall be capable of restricting or limiting control functions associated with any video alarm terminal as program feature or by line port.

2.14 PHOTO ID SYSTEM

A. The photo ID system shall include:
   1. Fargo DTC 4500 Card Printer/Encoder
   2. Card Design Software
   3. USB Digital Web Camera
   4. Full Color ribbons (printing)
   5. 300 cards
   6. 2.0 USB cable

B. The card printer/encoder shall be Fargo DTC4500 Photo ID System or approved equal.

2.15 PROXIMITY CARDS

A. General: The Contractor shall provide 500 iClass Proximity cards. The cards shall be compatible with existing Owner cards and readers in other facilities. The cards shall be PVC material credit card sized having maximum dimensions of 54 x 85.8 mm (3.38 x 2.13 in) and shall be a maximum 0.97 mm (0.038 in) thick.

B. Printing: Cards shall be capable of being printed in a dye-sublimation printer on the card front. Rear of card shall be printed in black ink using graphics provided by the Owner.

PART 3 - EXECUTION

3.01 GENERAL

A. The Contractor shall install all system components and appurtenances in accordance with the manufacturers' instructions, ANSI C2, and shall furnish all necessary interconnections, services, and adjustments required for a complete and operable system as specified. Control signals, communications, and data transmission lines grounding shall be installed as necessary to preclude ground noise, and surges from affecting system operation. Equipment, materials, installation, workmanship, inspection, and testing shall be in accordance with manufacturers' recommendations and as modified herein.

B. Consult the manufacturers' installation manuals for all wiring diagrams, schematics, physical equipment sizes, etc., before beginning system installation. Refer to the Riser/Connection diagram for all schematic system installation/termination/wiring data.

C. All equipment shall be attached to walls and ceiling/floor assemblies and shall be held firmly in place (e.g., sensors shall not be supported solely by suspended ceilings). Fasteners and supports shall be adequate to support the required load.

3.02 CURRENT SITE CONDITIONS

A. The Contractor shall visit the site and verify that site conditions are in agreement with the design package. The Contractor shall report all changes to the site or conditions which will affect performance of the system to the Owner in a report as defined in paragraph Group II Technical Data Package. The Contractor shall not take any corrective action without written permission from the Owner.

3.03 EXAMINATION

A. Examine pathway elements intended for cables. Check raceways, cable trays, and other elements for compliance with space allocations, installation tolerances, hazards to cable installation, and other conditions affecting installation.

B. Examine roughing-in for LAN and control cable conduit systems to PCs, Controllers, card readers, and other cable-connected devices to verify actual locations of conduit and back boxes before device installation.

C. Proceed with installation only after unsatisfactory conditions have been corrected.

3.04 PREPARATION

A. Comply with recommendations in SIA CP-01.

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

C. Obtain detailed Project planning forms from manufacturer of access-control system; develop custom forms to suit Project. Fill in all data available from Project plans and specifications and publish as Project planning documents for review and approval. All forms shall be completed in accordance with specified timelines outlines in Group Technical Data Packages in Section 280500.

1. Record setup data for control station and workstations.
2. For each Location, record setup of Controller features and access requirements.
3. Access Lists.
4. Propose start and stop times for time zones and holidays, and match up access levels for doors.
5. Set up groups, facility codes, linking, and list inputs and outputs for each Controller.
6. Assign action message names and compose messages.
7. Set up alarms. Establish interlocks between alarms, intruder detection, and video surveillance features.
8. Prepare and install alarm graphic maps.
9. Develop user-defined fields.
10. Develop screen layout formats.
11. Propose setups for guard tours and key control.
12. Discuss badge layout options; design badges.
13. Complete system diagnostics and operation verification.
14. Prepare a specific plan for system testing, startup, and demonstration (see the Testing section for requirements).
15. Develop acceptance test concept and, on approval, develop specifics of the test.
16. Develop cable and asset management system details; input data from construction documents. Include system schematics and Visio Technical Drawings.
17. Develop data gathering panel matrices that conform to Section 280500.

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

E. All Programming and access lists are submitted, reviewed, and accomplished before any devices are terminated and/or tested.

END OF SECTION 28 13 00