1. GENERAL

1.01 RELATED SECTIONS

.1 Section 08 74 00 – Access Control Hardware.

.2 Section 26 05 00 – Common Work Results for Electrical.

.3 Section 26 05 33.13 – Conduit for Electrical Systems.

.4 Section 27 05 00 – Common Work Results for Communications.

.5 Section 27 05 28 – Pathways for Communications Systems.

.6 Section 27 05 53 – Identification for Communications Systems.

1.02 REFERENCES

.1 Abbreviations:

.1 Electronic Access Control (EAC): control of people through entrances and exits of controlled area. Security utilizing hardware systems and specialized procedures to control and monitor movements within a controlled area.

.2 CPVX: Central Station Burglar Alarm Systems.

.3 CVSG: Mercantile Burglar Alarm Systems.

.4 CVWX: Proprietary Burglar Alarm Systems.

.5 DRS: Door Release System.

.6 PIN: Personal Identification Number.

.7 ICT – Information and Communications Technology

.8 CCTV – Closed Circuit Television

.9 PTZ – Pan, Tilt, Zoom Camera

.10 NVR – Network Video Recorder

.11 RTLS – Real-Time Locating System

.12 PWS – Patient Wandering System

.13 ATS – Asset Tracking System

.14 DGP – Data Gathering Point

.15 DC – Data Centre

.16 ACS – Access control System

.17 NTP – Network Time Protocol

.18 PoE – Power over Ethernet

.19 IP – Internet Protocol

.20 REX – Request to Exit Motion Detector

.21 RXP – Request to Exit Push Button

.22 LAN – Local Area Network

.23 4CIF – An image resolution of 740 x 480 pixels

.24 GUI – Graphical User Interface

.25 IPS – Images Per Second

.26 BTU - British Thermal Unit

.27 RU – Rack Unit

.28 UTP – Unshielded Twisted Pair

.29 RAM – Random Access Memory

.30 UPS – Uninterruptible Power Supply

.31 KVM – Keyboard, Video, Mouse console

.32 VMS – Video Management System

.33 DPU – Distributed Processing Unit

.34 SOC – Security Operations Centre

.35 SCS – Structured Cabling System

.2 Reference standards:

.1 Health Canada / Workplace Hazardous Materials Information System (WHMIS)

.1 Material Safety Data Sheets (MSDS).

.2 Underwriters' Laboratories (UL)

.1 UL 294-2009, Access Control System Units.

.2 UL 603-08, Power Supplies for Use with Burglar Alarm Systems.

.3 UL 681-1999, Installation and Classification of Burglar and Holdup Alarm Systems.

.4 UL 827-2008, Central-Station Alarm Services.

.5 CAN/ULC-S3-1-M88 Standard for Central and Monitoring Station Burglar Alarm systems.

.6 Underwriters Laboratories (UL) Cable Certification and Follow Up Program.

.3 National Fire Protection Association (NFPA)

.1 NFPA 70-2011, Article 517, National Electric Code.

.2 NFPA 101-2008, Life Safety Code.

.4 ANSI/TIA/EIA-568-B.1 and its addendum

.5 ANSI/TIA/EIA-568-B.3 and its addendum

.6 BICSI Telecommunications Distribution Methods Manual – Most current Edition

.7 BICSI Network Design Reference Manual – Most current Edition

.8 BICSI Information Transport Systems Installation Manual – Most current Edition

.9 American Society for Testing Materials (ASTM).

.10 Institute of Electrical and Electronic Engineers (IEEE).

.11 Applicable local Building Codes

.12 Manufacturer's specifications, latest issue.

1.03 SYSTEM DESCRIPTION

.1 The access control system shall consist of field and termination equipment necessary to provide a fully automated system to control and monitor authorized traffic in and out of controlled areas of the facility.

.2 The access control system shall be designed on a distributed processing architecture employing remote DGP's (Data Gathering Points) and operator workstations connected to a redundant central server solution.

.3 All doors and devices will be connected to centrally located DGP panels located in communications rooms. Connectivity from the DGP panels to the system front end will be based on Ethernet IP based protocols

.4 Provide card access to all locations provided in the specification drawings and schedules and door details

.5 The areas that shall be controlled and monitored through the access control system, ensuring compliance with the OBC include but are not limited to:

.1 All elevators

.2 Access controls on facility entrance points used by public and/or staff

.3 Access controls on transitions between spaces of differing security levels

.4 All perimeter doors designated as emergency exit only shall be monitored through the access control system.

.5 All Automatic Door Operators shall only function in conjunction with a valid access card.

.6 Monitoring Locations

.1 System monitoring shall be centrally monitored through the Owner's network.

.2 Primary monitoring within the LTC shall be at the 2nd floor RHA workstation. This location shall be able to acknowledge alarms.

.3 System monitoring shall also be provided via web browser accessible from any workstation on the network. Access shall require a valid user ID and password.

.4 The system shall be capable of operating even in the event that the system management server is unavailable.

.5 Following a power failure and the restoration of main or backup power, the ACS shall revert automatically to normal service status without the need for operator intervention. The system shall restart in the same state as existed before the power interruption with no loss of functionality or transaction data.

.6 In the event that communication between the DGP and access control server is unavailable, the functionality of the DPG shall be preserved such that door functionality at every door is unaffected.

.7 This will apply for all card records that were recorded in the access control system database prior to the loss of communication between the DGP and access control system server.

.8 The ACS shall provide continuous unattended access control and alarm monitoring at specified locations while meeting the technical, operational and feature requirements of this specification.

.9 The ACS shall grant or deny access within one (1) second of an access attempt. Alarms shall be fully displayed on Client Workstations within one second of origination.

.10 Under no circumstances shall a false acceptance be allowed.

.11 The Access Control system shall support a minimum of five thousand (5,000) cards and an unlimited amount of facility codes.

.12 The system shall be capable of responding to card only, card and pin/key pad.

.7 The Access Control System (ACS) shall include but not be limited to the following elements:

.1 Supply and install field devices as per identified on the drawings, but not limited to:

.1 Card Readers

.2 Keypads/Pin Pads

.3 Door Control Units / Data Gathering Panels

.4 Door Position Switches

.5 Access Cards

.6 Tamper Alarms

.7 Local Audio Alarms

.8 Request to Exit Motion Detectors

.9 Request to Exit Push Buttons

.10 Key Switches

.11 Interface to door hardware (Power Transfer Switches/Crash Bars, strikes, maglocks, door operators, etc.) including monitoring circuit for “lock status” and or “bond sensors”

.8 Common Portal Functions

.1 The below functions are general to all doors where applicable, and unless otherwise stated within the respective portal sub-sections.

.1 Valid Access Trigger – The following are valid triggers which shut the door alarms, and allow proper access through the respective portal.

.1 Valid Access Card Swiped

.2 Valid Pinpad input

.3 Request to Exit Motion Detector or Pushbutton

.4 Remote Access Granted

.2 Loss of Power Operation

.1 Non maglock doors shall be arranged to remain locked on loss of power to the sensor.

.2 Where required by building code, doors with Mag-Locks shall release their Mag-Locks when loss of power occurs.

.3 When power is restored Mag-locks shall not be re-energized unless the master Mag-Lock override key-switch is actuated.

.3 Intercom

.1 An Intercom icon will be displayed in the SOC Control room upon alarm, if an intercom station is installed at alarm location.

.4 Invalid Card Reader Swipe

.1 Upon presentation of an invalid access card, the card reader shall provide an audio/visual indication of the invalid access attempt.

.5 Door Forced Open Alarm

.1 In the event that the Door Position Switch or Lock Status Switch activate without a Valid Access Trigger, generate a “Door Forced Open” alarm at the SOC Control room, and activate the local annunciator.

.2 Local annunciator, shall remain active until door is closed and a valid access card is swiped. Alarm can also be reset by the operator in the SOC Control room.

.3 Door Held Open Alarm - Door not closed during shunt time will activate "Door Held Open" indication in the SOC Control room and activate local annunciator. The system should have the ability to keep the local annunciator active until door is closed and a valid card is swiped. Alarm can also be reset by the operator in the SOC Control room.

.4 Delayed Egress – Panic bar activated

.1 The security system shall be configured with fifteen (15) second delayed egress functionality.

.2 Upon panic bar activation, immediately activate the local annunciator, and a three second timer shall start. If the panic bar is released within the first three seconds, de-activate the local annunciator.

.3 After the first three seconds of continuous activation of the panic bar, a 12 second time shall start to unlock the door.

.4 After the first three seconds of continuous activation of the panic bar, an alarm shall be generated. Alarm shall be indicated as "Door in Delayed Egress Mode", which warns the operator that the door shall unlock at the end of a 12 second delay.

.5 Upon door unlock, the lock status sensor shall indicate a "Door Unsecure" alarm.

.6 Upon door opening, the Door Position Switch shall indicate a "Door Forced Open".

.7 The door shall remain unlocked until the key switch is activated. The door can only be re-secured by activation of the local key switch.

.8 Where applicable, the door shall be interlocked (through software at the panel

level) with all other downstream doors in the egress path, such that the total egress delay does not exceed 15 seconds.

.5 Fire Alarm Release Operation

.1 Fire Alarm Release – Doors with magnetic locks that are required to be used exiting or for egress to exit are required to be released when the fire alarm is activated.

.2 This interface shall be a hardware relay provided by the Fire Alarm System and zoned from the Fire Alarm System. This shall release the door lock immediately and generate a single alarm indicating that the doors are in "Fire Unlock Mode", which warns the operator that all the fire egress doors are unlocked

.3 While the door is in Fire Unlock mode, inhibit the alarms from the Lock Status Monitor. If the door is opened, generate a "Door Forced Open" alarm for each respective door.

.4 Upon fire alarm restore, the Mag-locks need to be re-energized. This is done by operating a switch available only to authorized personnel.

.9 Telecom Rooms

.1 Provide cable troughs, conduit, and emergency power circuits for DGP configurations. Cable troughs shall be grounded to earth ground.

.2 All Equipment mounted in each DGP configuration shall be mounted on fire rated plywood.

.3 Access Control equipment, cable troughs, conduit, and emergency power circuits, and CCTV power supplies shall be wall mounted as per manufacturer's specifications.

.4 Provide emergency electrical panel Power Monitoring devices for each communications room and connect into the Access Control System for monitoring.

.5 It shall be the responsibility of the contractor to keep Security Equipment clean and free of dust at all times during the installation.

.10 Network

.1 Ensure all IP addressing schemes used on the network are coordinated and reviewed by the facility and the Owner's IT services configuring the network.

.2 The ACS will reside on a ACS VLAN on the Owner's Network, the contractor shall coordinate with Owner's IT services for connection to the existing ACS network.

.11 Interface with Other Systems

.1 Elevators

.1 The system shall provide for floor by floor control. The elevator on a valid card read shall unlock all floors pertain to the cardholders access rights. Once a single floor is chosen, all other floors shall once again lock, and the elevator shall be directed to the floor chosen. The system shall capture information as to the floor that was chosen by the card holder.

.2 All work, equipment, and supplies relating to the installation of Card Access or modification of the elevators to support card access in building elevators shall be performed by the Elevator manufacturer.

.3 Coordinate with elevator provider to ensure the functionality of the elevator fireman's override key switch such that on activation the security system shall relinquish all control over the elevator call buttons and the elevator shall function normally.

.4 Coordinate with elevator provider to ensure the functionality of the Fire Alarm system override such that on activation of a fire alarm the security system shall relinquish all control over the elevator call buttons and the elevator shall function normally.

.5 Connect all relevant equipment to the Access Control system, restrict access of card holders to each elevator floor.

.6 Coordinate the installation testing and commissioning of all required elevator security equipment with the elevator

company in relation to security system components and devices.

.12 Power

.1 120 VAC power (on centralized UPS/generator back-up) shall be provided to all security system devices.

.2 Connect to the 120 VAC power and for providing CSA listed power supplies and transformers to distribute low voltage power to system components.

.3 All power supplies shall be hard wired into source 120VAC power. Plug in transformers are not acceptable.

.4 Provide lockable, hinged covered, terminal cabinets for all power supplies, transformers, and power distribution terminal strips. Provide all conduit and wiring from the 120 VAC facilities to the terminal cabinets.

.5 Provide protection against surges, spikes, noise, and other line problems for all system equipment and their components. In addition to generator support, all power sources shall be equipped with uninterrupted power supply capable of supporting all attached equipment for a period of 60 minutes.

.6 All equipment and system components which are powered by more than 48 volts AC or DC shall be ULC listed for safety. This includes equipment or system components classified as non-power limited.

.7 All system power supplies shall be monitored, by the Access Control System, for line failure on a dedicated monitoring input point. Therefore, when an AC line fails, a unique alarm condition will be caused.

1.04 ACTION AND INFORMATIONAL SUBMITTALS

.1 Submit in accordance with Section 01 33 00.

.2 Product Data:

.1 Submit manufacturer's instructions, printed product literature and data sheets for access controls and equipment and include product characteristics, performance criteria, physical size, finish and limitations.

.2 Submit copy of product WHMIS MSDS.

.3 Submit:

.1 Functional description of equipment.

.2 Technical data for all devices.

.3 Device location plans and cable lists.

.4 Devices mounting location detail drawings.

.5 Typical devices connection detail drawings.

.3 Shop Drawings:

.1 Submit drawings stamped and signed by professional engineer registered or licensed in Province of Ontario, Canada.

.2 Shop drawings to indicate project layout, including details.

.1 Shop drawings to indicate, mounting heights and locations, wiring diagrams.

.2 Submit zone layout drawing indicating number and location of zones and areas covered.

.3 Submit wiring diagrams.

.4 Submit complete equipment list.

.5 Manufacturer specification sheet for each new piece of equipment. Each sheet should clearly identify the particular model number of the hardware being provided.

.6 Software configuration parameters.

.4 Test and Evaluation Reports:

.1 Submit certified test reports from approved independent testing laboratories indicating compliance with specifications for specified performance characteristics and physical properties.

.5 Manufacturer's Instructions: submit manufacturer's installation instructions.

.6 Manufacturer's Field Reports: submit manufacturer's written reports within 3 days of review, verifying compliance of Work, as described in PART 3 - FIELD QUALITY CONTROL.

.7 Integration Document for each interface to be implemented or configured.

.8 Testing and commissioning plan

1.05 CLOSEOUT SUBMITTALS

.1 Submit in accordance with Section 01 78 00.

.2 Operation and Maintenance Data: submit operation and maintenance data for access controls and equipment for incorporation into manual.

.1 Include:

.1 System configuration and equipment physical layout.

.2 Functional description of equipment.

.3 Instructions of operation of equipment.

.4 Illustrations and diagrams to supplement procedures.

.5 Operation instructions provided by manufacturer.

.6 Cleaning instructions.

1.06 DELIVERY, STORAGE, AND HANDLING

.1 Deliver, store and handle materials in accordance with Section 01 61 00 and with manufacturer's written instructions.

.2 Delivery and Acceptance Requirements: deliver materials to site in original factory packaging, labelled with manufacturer's name and address.

.3 Storage and Handling Requirements:

.1 Store materials indoors and in accordance with manufacturer's recommendations in clean, dry, well-ventilated area.

.2 Store and protect access controls and equipment from nicks, scratches, and blemishes.

.3 Replace defective or damaged materials with new.

.4 Project Warranty: refer to CCDC 5B 2010 for project warranty provisions.

.5 Extended warranty period must include warranty against meeting specified performance requirements, for specified time period.

.6 Manufacturer's Warranty: submit, for Owner's acceptance, manufacturer's standard warranty document executed by authorized company official.

2. PRODUCTS

2.01 MATERIALS

.1 General Requirements

.1 Contractor is fully responsible for the ultimate design and implementation of the system topology (physical and logical) best suited for the project.

.2 The Devices provided for Mulock house will match those provided for the other areas of Mulock Park.

.2 Field Devices

.1 Door Position Switches (supplied and installed by Division 08)

.1 Door position switches shall be supplied and installed to monitor door status of all security points;

.2 Door position switches shall be concealed discrete devices unless otherwise noted and shall not be integral to other devices such as strikes, maglocks, etc. Where exposed mounting is necessary devices shall be mounted so as to limit easy access to unauthorized personnel.

.3 Acceptable devices are as follows:

.1 Concealed - Interlogix 1078/1076 series or approved equivalent.

.2 Surface - Interlogix 1085T series or approved equivalent. (may be used where approved only)

.3 Overhead – Interlogix 25200 series Armored Cable or approved equivalent. (on overhead doors)

.4 Frame mounted magnetic door contacts, hinge mounted plunger type switches, are not acceptable with the exception of overhead shutters and doors.

.2 Tamper Alarms

.1 All security equipment cabinets (including CCTV, ACS power supply cabinets) shall be equipped with sensors, which detect and remotely annunciate their opening.

.2 All communication and alarm device cabling at the door and between the DGP and the door shall be supervised to detect and remotely annunciate "open", "high

impedance", "low impedance", and "short" conditions. The end of line supervision device shall be installed as close as possible to the security device.

.3 Request to Exit Motion Detector (supplied and installed by Division 08)

.1 Request to Exit Motion Detectors shall be the T.REX series or as manufactured by Tyco approved equivalent.

.2 Request to Exit Motion Detectors shall be supplied and installed on all security doors that require free egress. The REX will mask the alarm when a person is using the door for egress from the secure side of the door. REX shall shunt the door contact alarm only.

.3 Activation of the REX shall not unlock the door.

.4 The REX must have an accurate and adjustable detection zone capable of both vertical and horizontal adjustments.

.4 Card Readers

.1 Card readers shall be a Keyscan access card reader or an approved equivalent.

.2 Card readers shall read the encoded data from the credential and transmit the data to the host panel. The card reader shall also present audio and visual feedback to the user that a card read operation is either "valid" or "invalid".

.3 Visual feed back shall be through the use of LCD displays at doors with Pin pads or other advanced user interaction.

.4 Card readers shall be capable of being flush or surface mounted, and will typically be wall mounted.

.5 DATA GATHERING PANELS (DOOR CONTROLLERS)

.1 Data gathering panels shall be manufactured by Dormakaba and shall be an 8-reader CA8500 model or an approved equivalent.

.2 All security DGP's shall be mounted on fire retardant plywood provided by the electrical contractor.

.3 Security contractor shall be responsible for providing all hardware, licenses, wiring, connections, terminations, power supplies, configuration, programming, testing and

commissioning for a fully operational access control and alarm monitoring system.

2.02 ACCESS CONTROL AND ALARM MONITORING SYSTEM

.1 The Access Control and Alarm Monitoring System shall be the key central component for managing physical security access control, alarm monitoring, and visitor management as specified herein.

.2 Manufacturer

.1 Keyscan Aurora Control Software.

.2 The Access Control and Alarm Monitoring System shall be capable of processing an unlimited number of credential readers, scalable from single site to multiple sites.

.3 Security Contractor shall be responsible for providing all servers, DGP's, licenses, programming, wiring, terminations, configuration, testing, and verification required to provide for a fully operational access control and alarm monitoring system for Mulock House.

.4 This will be integrated into the Mulock Park System

3. EXECUTION

3.01 GENERAL

.1 Programming.

.1 Include as part of solution all associated costs to program the system and ensure all configuration and naming conventions are reviewed by the Consultant.

.2 Include as part of their solution all associated cost related to database programming, and user enrolment.

.3 Attend pre-installation meetings as required with facilities to identify the specifics of the system programming.

.4 Be responsible to document all decided on software configuration parameters and submit for approval.

.5 Once approved, contractor shall implement and test all system programming required.

.6 Include for all approved software configuration parameters in final revisions shop drawings.

.7 Building door numbers are not yet final and will change prior to final system programming. Be responsible to ensure final programming configuration and system documentation match this newest set to be provided by the Architect.

3.02 EXAMINATION

.1 Verification of Conditions: verify conditions of substrates previously installed under other Sections or Contracts are acceptable for access control system installation in accordance with manufacturer's written instructions.

.1 Visually inspect substrate in presence of Consultant.

.2 Inform Consultant of unacceptable conditions immediately upon discovery.

.3 Proceed with installation only after unacceptable conditions have been remedied and after receipt of written approval to proceed from the Owner.

3.03 INSTALLATION: ACCESS CONTROL SYSTEM

.1 USA: UL 1641 in lieu of CAN/ULC-S310.

.2 Install Access Control System units and components in accordance with CAN/ULC-S310.

.3 Conduits and back boxes for devices in walls and doors will be provided by Electrical Trade as noted in Section 27 05 28.61. Provide all control boxes/equipment and conduit work to tie in to rough-ins.

.4 Provide tamperproof attachments for each activation unit cover plate to receptacle back box.

.5 Enclose in conduit or flexible protective armor external cables for associated junction box to remaining system locations, from junction box to above ceiling mounted cable ducts or master conduit routes.

.6 Securely fasten all components to wall, ceiling, or other substrate or structure.

3.04 SITE TEST AND INSPECTION

.1 Perform verification inspections and test in presence of facility representatives.

.1 Provide all necessary tools, ladders, and equipment.

.2 Ensure appropriate subcontractors manufacturer's representatives are present for verification.

.2 Performance testing:

.1 Test procedure: perform test on a "go-no-go" basis.

.1 Make only operator adjustments required to show proof of performance.

.2 Test to demonstrate and verify that installed system complies with installation and technical requirements of this specification under operating conditions.

.3 Test results to be evaluated by the Consultant as either acceptable or unacceptable using following procedures.

.2 Documentation review:

.1 This review will determine if information provided is sufficient to meet requirements of this specification.

.2 Provide for review all System manuals, as installed drawings, pretest forms, antenna radiation patterns, equipment cabinet pictorials, antenna pictorial, antenna mount pictorial, video and audio equipment details.

.3 Mechanical inspection:

.1 Consultant and Contractor to tour areas to ensure that Systems and Subsystems are installed in place for proof of performance testing.

.2 Take system inventory at this time. Verify following items before beginning proof of performance tests:

.1 Electrical power circuits designated for system equipment are properly labeled, wired, phased, protected and grounded.

.2 Conductor ends are protected by heat shrink wrap; audio spade lugs, barrier strips and punch blocks are used.

.3 Dust, debris, solder splatter, etc. are cleaned and removed from site.

.4 Equipment is properly labelled.

.5 Equipment identified in system's equipment lists are in-place and properly installed.

.6 Each System ground method are installed in accordance with manufacturer's instructions and this specification.

.3 Subsystem functional test:

.1 Conduct operational testing after review of documentation and mechanical inspection completed. Proceed as follows.

.1 Perform operational test of each Subsystem to verify that all equipment is properly connected, interfaced and is functionally operational to meet requirements of this specification.

.2 Control units:

.1 Take S/N readings from control unit's input and output in manual (and/or automatic) mode. Check output of DC/Data converter for S/N. Evaluate entire signal quality at baseband connector output of control unit and remote equipment.

.3 Distribution (or interface) system:

.1 Check each door utilizing a volt/ohm (or signal level) meter to confirm each function and to ensure that system meets all performance requirements.

.2 Test each interconnection point (i.e.: door unit, junction box "cross connection", control unit, etc.) to ensure compliance with this specification.

.4 Total system test:

.1 Proceed with testing when system and subsystems are functionally tested and accepted. Total system tests to verify that requirements have been met for DC (and/or audio), sub carrier, and control signals in accordance with this specification.

.5 Safety:

.1 Demonstrate with documentation that access control system meets safety requirements specified in UL 294.

.4 Visual verification: objective is to assess quality of installation and assembly and overall appearance to ensure compliance with Contract Documents. Visual inspection to include:

.1 Sturdiness of equipment fastening.

.2 Non-existence of installation related damages.

.3 Compliance of device locations with reviewed shop drawings.

.4 Compatibility of equipment installation with physical environment.

.5 Inclusion of all accessories.

.6 Device and cabling identification.

.7 Application and location of ULC approval decals.

.5 Technical verification: purpose to ensure that all systems and devices are properly installed and free of defects and damage. Technical verification includes:

.1 Validate sensitivity of readers and applicability and application of cards.

.2 Connecting joints and equipment fastening.

.3 Compliance with manufacturer's specification, product literature and installation instructions.

.6 Operational verification: purpose to ensure that devices and systems' performance meet or exceed established functional requirements. Operational verification includes:

.1 Operation of each device individually and within its environment.

.2 Operation of each device in relation with programmable schedule and or/specific functions.

3.05 FIELD QUALITY CONTROL

.1 Manufacturer Services:

.1 Manufacturer of products, supplied under this Section, to review Work involved in the handling, installation/application, protection, and cleaning, of its products and submit written reports, in acceptable format, to verify compliance of Work with Contract.

.2 Manufacturer's Field Services:

.1 Obtain written reports from manufacturer verifying compliance of Work, in handling, installing, applying, protecting, and cleaning of product.

.2 Submit manufacturer's field services consisting of product use recommendations and periodic site visits for inspection of product installation in accordance with manufacturer's instructions.

.3 Ensure manufacturer's representative is present before and during critical periods of installation and testing.

.4 Schedule site visits to review Work at stages listed:

.1 After delivery and storage of products, and when preparatory Work on which Work of this Section depends is complete, but before installation begins.

.2 Twice during progress of Work at 25% and 60% complete.

.3 Upon completion of Work, after cleaning is carried out.

3.06 CLEANING

.1 Progress Cleaning: clean in accordance with Section 01 74 00.

.1 Leave Work area clean at end of each day.

.2 Final Cleaning: upon completion remove surplus materials, rubbish, tools, and equipment in accordance with Section 01 74 00.

.1 Remove protective coverings from accessories and components.

.2 Clean housings and system components, free from marks, packing tape, and finger prints, in accordance with manufacturer's written cleaning recommendations.

.3 Clean components free from dirt and fingerprints.

.4 Remove recycling containers and bins from site and dispose of materials at appropriate facility.

3.07 PROTECTION

.1 Protect installed products and components from damage during construction.

.2 Repair damage to adjacent materials caused by access controls and equipment installation.

End of Section