Part 1 General

1.1 Introduction

.1 This Architecture and Engineering specification provides detailed information on Johnson Controls' P200 Integrated Security Management System (Pegasys)

.2 The City of Winnipeg currently operates a centralized P2000 server, and as such, no server is required for this project.

1.2 Work Included

.1 The work includes furnishing all labour, materials, tools, equipment, and documentation required for a complete and working Integrated Security Management System as specified in this section. This scope of work shall cover the requirements for the access control, alarm monitoring and integrated systems.

1.3 References

.1 Design and operation of the system shall conform to the following referenced codes, regulations and standards as applicable:

.1 CSA C22.1-2006 – Canadian Electrical Code, Part 1.

.2 NFPA 70

1.4 General Product Description

.1 The Security Management System (SMS) shall be capable of integrating multiple building functions including access control, alarm management, intrusion detection, video imaging and badging, database partitioning, interfacing to closed circuit television monitors (CCTV) and digital video recording (DVR) matrix switches, and interfacing with intercom equipment. It shall also be capable of controlling multiple banks of elevators, as well as allowing cardholder information and queries from external system databases (MIS interface).

.2 CCTV and DVR interface is a future requirement for the system.

.3 The system shall be modular in nature, and will permit expansion in both capacity and functionality through the addition of controllers, card readers, workstations, or by increasing the number of cards and sensors.

.4 The system shall incorporate the necessary hardware, software, and firmware to collect, transmit, and process alarm, tamper and trouble conditions, access requests, and advisories back to the City of Winnipeg central monitoring facility. The system shall control the flow of authorized personnel traffic through the secured areas of the facility.

1.5 Submittals

.1 Contractor shall submit all items in accordance with the requirements of the Submittals sections and shall include, but not be limited to, the following:

.1 Model numbers from all furnished job components.

.2 Manufacturers catalog data sheets for all components.

.3 Input power requirements for all SMS components.

.4 Complete engineered drawings indicating:

.1 Manufacturer model numbers and specifications.

.2 Dimensions, layouts and installation details.

.3 Point-to-point wiring diagrams for all SMS devices.

.4 Termination details for all SMS devices.

.5 Single-line system architecture drawings representing the entire SMS.

.6 Interfaces with all sub-systems.

.5 Owner Acceptance Form with a check box associated with each card reader and input point. A check mark in the box will indicate that each point has been correctly installed and that communication between the controller and the server has been established. This form shall be completed prior to Owner acceptance of the system.

.6 Six (6) sets of the Manufacturer's User and Installation Manuals.

.7 Course outlines for each of the end user training programs. The course outlines shall include the course duration, and a brief description of the subject matter.

1.6 Delivery, Storage, and Handling

.1 SMS components shall be shipped to the job site in original manufacturer's shipping containers.

.2 All shipping and handling costs shall be paid for by the Contractor at no additional cost to the Owner.

.3 All equipment stored on the job site shall be secured in a locked storage area as designated by the General Contractor or Owner.

1.7 Testing and Commissioning

.1 The Contractor shall be responsible for testing and commissioning the installation in accordance with all applicable documents in the Contract set.

.1 Testing shall be comprehensive and sufficient to demonstrate compliance with each requirement.

.2 A proposed test plan shall be submitted to the Owner's representative for approval before commencement of final test.

.3 Final tests shall be conducted in the presence of the Owner's representative.

Part 2 Products

2.1 Manufacturers

.1 Pegasys P2000 Integrated Security Management System by Johnson Controls L.P.

2.2 Operational Requirements

.1 System Capabilities:

.1 General

.1 The SMS shall operate in client-server architecture. Any SMS software and firmware required for the system shall be fully tested and compatible with the existing City of Winnipeg SMS application system.

.2 Database Management

.1 The system shall create and maintain a master database of all cardholder records and system activity for all connected points.

.3 Audit Trail

.1 The SMS shall maintain an audit trail file of operator activity, and provide the ability to generate a report by operator, time and date, and type of activity. The system shall allow the operator to direct the audit trail report to screen, printer or file.

.4 Remote Monitoring and Configuration

.1 The system shall transmit all information back to the City of Winnipeg central monitoring facility and shall be configurable from this facility.

.5 Input Point Monitoring

.1 The SMS shall collect and process status information from all monitored points.

.6 Input Point Supervision

.1 The SMS shall electrically supervise all 2-state and 4-state input points.

.7 Web Access Option

.1 The Web Access feature shall enable users to perform various security management tasks from any web-ready PC or compatible PDA device. This feature shall support different permission levels for each user, and requests can be approved and/or validated prior to being implemented to prevent unauthorized operations or changes to the SMS. Rules shall be established to determine how requests are submitted. If requests require approval, pre-defined approvers shall approve or reject requests. If validation shall be required, a user with the proper permission shall

confirm the validity of the request before it can be fully processed. Web Access features shall include:

- Visitor requests
- Contract requests
- Cardholder management
- Customizable user interface
- Request approval and validation
- Badge activities
- Guard services
- Emergency access disable

.8 Future CCTV Capability

.1 The system shall have the capability to operate the cameras and monitors forming part of the CCTV system as part of a future expansion. The system shall then provide the controls to define and run the following:

- Alarms, macros, and tours
- Sequences from the monitors
- Pan, tilt, zoom focus, iris, wiper, washer and light controls for any given camera
- Patterns, presets, and auxiliaries

The CCTV capability will provide for a single-seat integrated security solution when used with the SMS and shall support at a minimum the following CCTV protocols.

- General ASCII protocol
- American Dynamics switch: AD1024
- BetaTech switch: Ademco VideoBlox Switch
- Geutebruck - GST Interface: CPX 24/8; CPX 48/8; VX 3 (Vicros III); KS 48 (Vicros II); and KS 40 switches.
- Panasonic SX850 switch, other models may be supported if they are compatible with SX850 Protocol Version 1.4 01.24/00.
- Pelco 9760, CM 6700 and CM 6800 switches.
- Philips Burle (Bosch) LTC 8100; LTC 8200; LTC 8300; LTC 8500; LTC 8600; LTC 8800 and LTC 8900 series switches.
- Ultrak MaxPro-1000 switch.
- Vicon VPS1300; VPS1344; VPS1422 and VPS1466 switches.

.9 Future DVR Integration Capability

.1 The systems shall have the capability to provide seamless integration of the SMS with compatible Digital Video Recording (DVR) systems as part of a future expansion. The integration shall then allow authorized

users to manage camera functions, including frame rate and resolution, from a single workstation, as well as to tie an event generated on the system to live or recorded audio visual (AV) recording. Audio and video may be accessed via a real time list, real time graphical map, or alarm monitor screen.

.2 Users shall be able to search, retrieve, and download real time or archived AV recording from any surveillance camera, from any place, at any time. Query options shall include time/date, alarm events, camera ID and DVR ID. The playback interface shall have fast forward, rewind, go to first frame, go to last frame, pause and stop controls. The AV integration shall allow for Pan, tilt, zoom control, including presets.

.3 The system shall support at a minimum the following DVR protocols:

- Nice protocol, version 8.0 (with alarm forwarding and message filtering)
- Loronix protocol, versions 4.4 and 4.5
- Verint SmartSight
- Johnson Controls Digital Vision Network DVN 5000 series and DVN 3000 series.

.10 Future Metasys® System Extended Architecture Capability

.1 The Metasys System Extended Architecture capability shall allow the SMS to interface using web-based technology to the Johnson Controls Metasys Building Management System as part of a future expansion. It shall allow the Metasys workstations to view and acknowledge certain SMS alarms, send access control commands, print reports, and to create interlock events.

.2 The option shall require no special hardware subset, but rather be a simple upgrade, via software.

2.3 Software Requirements

.1 Provide additional 5 client licenses to add-on to the existing server.

2.4 Hardware Requirements

1. Controllers shall be Johnson Controls, Inc. CK721 v2.4+

.1 The controller shall be a fully stand-alone processor capable of making all access control decisions without the involvement of the server computer based on a set of parameters passed to the controller from the server.

.2 The controller shall support up to sixteen (16) card readers in addition to either 256 input points or 128 input and 128 output points. It shall further support up to 12 facility codes per reader, 40 unique holidays, 32 access group and time zone pairs.

.3 Memory Requirements:

.4 Standard number of cards: 15,000 expandable to 200,000.

.5 Minimum number of historical transactions: 5,000 expandable to 50,000 at full card capacity.

.6 The controller shall require no firmware changes and shall use flash memory modules to provide non-volatile storage of both data and operational code.

.7 Each controller shall be provided with built-in hardware to support hard-wired communications between the controller(s) and readers of up to 4000 feet.

.8 Communications between the controller(s) and the server shall be via Ethernet TC/IP at 10Mbps.

.9 An alarm summary relay shall be built-in to the CK7xx controller motherboard. If so programmed, the alarm relay shall be activated whenever a connected alarm point transfers to the alarm state and whenever soft alarms become active.

.10 A SPDT tamper switch shall be attached to the inner surface of the controller enclosure. The tamper switch shall change state whenever the enclosure door is opened to signal the SMS of the condition. The tamper switch input shall be user programmable to be suppressed, to be recognized as an input point, to be processed by the alarm queue at the server computer, to printout at an optional printer connected directly to the controller, and to activate the alarm summary relay described above.

.11 The controller shall include a battery module to back-up the controller's applications programs and database for 30 days after the failure of the primary AC power service. The controller database, the time clock, the transaction history, and all operator entered parameters shall be backed-up by the battery.

.12 If required elsewhere in the drawings or Specification, the controller(s) shall be furnished with an UPS battery configuration instead of a standard AC linear power supply configuration. The battery shall power the controller upon failure of the primary AC service for a minimum of one hour.

.13 While on UPS service, the controller shall continue to process event activity, card transactions, and record history transactions.

.14 The controller shall provide built-in LED to indicate whether the controller is properly communicating with the server computer.

.2 Alarm monitoring and Output Control terminal boards. Intelligent alarm monitoring and output control terminal boards shall be Johnson Controls, Inc. plug-in modules to CK7xx series controller with at least the following functionality:

.1 Sixteen two-state alarm input points.

.2 Eight four-state supervised alarm input points.

.3 Eight two-state alarm input points and eight SPDT output relays.

.4 Eight four-state supervised alarm input points and eight SPDT output relays.

2.5 Cards and Card Readers

.1 General

.1 All readers shall be configured with the reader electronics mounted separately, on the "secure" side of the door such that only the reader head and pilot lights are mounted in the reader housing on the "entry" side of the door.

.2 Proximity Technology

.1 Standard range Proximity reader (contact to 20 in.)

.1 The reader shall be integrated and contain all reader electronics inside a single polycarbonate enclosure.

.2 The reader shall operate when mounted on a variety of surfaces, including metal. Maximum read range degradation when mounted on a metal surface shall be 50-percent.

.3 The reader shall contain an integral color LED and audio tone to indicate if the card has been successfully read.

.4 The reader shall be 8" x 8" x 2" maximum.

.5 Read range shall be dependent on model selected.

.6 The reader shall be rated for normal operation from -5 to 150°F.

.7 The proximity card shall be encased in sealed plastic with a surface suitable to receive an adhesive backed photo ID or shall be capable of direct printing.

.2 Mullion Style Proximity Readers

.1 The reader shall be integrated and contain all reader electronics inside a single polycarbonate enclosure.

.2 The reader shall operate when mounted on a variety of surfaces including metal. Maximum read range degradation when mounted on a metal surface shall be 50-percent.

.3 The reader shall contain an integral color LED and audio tone to indicate if the card has been successfully read.

.4 The reader shall be 1.7" x 6" maximum.

.5 Read range shall be up to 5".

.6 The reader shall be rated for normal operation from -5 to 150°F.

.7 The proximity card shall be encased in high impact sealed plastic with a surface suitable to receive an adhesive backed photo ID.

.3 Proximity Family Smart Card Readers

.1 All electronics shall be integrated and contained inside a single polycarbonate enclosure.

.2 Reader shall operate when mounted on a variety of surfaces including metal. Maximum read range on metal shall be degraded to a point as specified by model selected.

.3 The reader shall contain an integral color LED and audio tone to indicate a successful read.

.4 Reader size shall be no greater than 6” x 6” x 3”.

.5 Technology of read shall be Johnson Controls specific, 26 or 34-bit with site code, user level and badge number output in 2 wire Wiegand (D1/D0).

.6 Readers shall be personalized according to the controller type the data is sent.

.7 Readers shall comply with ISO 14443 A or B as specified by smart card use.

.8 Smart cards shall be dual use (insert or non-contact) containing at least an 8K microprocessor.

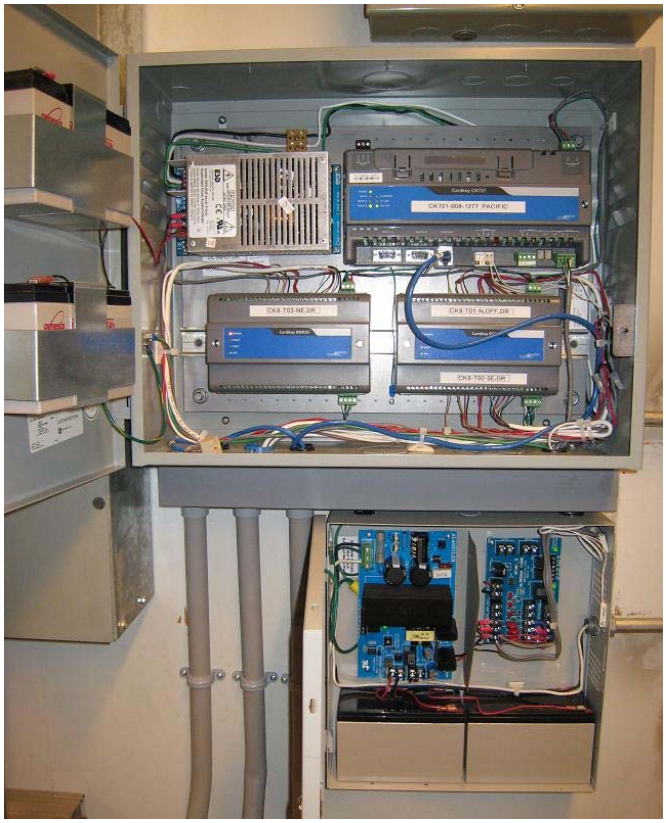
2.6 Enclosures and Power Supplies

.1 Johnson Controls cabinets PAN-ENC2436WDP or PAN-ENC3648WDP shall be used to accommodate the hardware modules instead of standard Pegasys S300-DIN-L enclosures in order to save room. One power supply S300-DIN-L-PS shall be used to power up every three modules.

.2 Separate Altronix AL600ULACMCB power supplies shall be used to drive the power for the locking hardware.

.3 Tamper switches shall be installed in every Pegasys related hardware enclosure (i.e. power supply, controllers, DSC, etc.) and connected to the dedicated panel tamper input on CK721 network controllers

.4 Both Altronix and JC power supplies shall have backup batteries.



2.7 Cable Types

.1

Description	Cable type
Cardkey RS-485 (internal bus wiring)	18 AWG, 4 conductor, shielded
Card reader	22 AWG, 6 conductor, shielded
Door strike	18 AWG, 2 conductor, shielded
Auxiliary Access (request to exit motion sensor)	22 AWG, 4 conductor, shielded
Door contact	22 AWG, 4 conductor, shielded

2.8 Miscellaneous Hardware

.1 Recessed magnetic door contacts Honeywell 951 WH are to be used wherever possible.

.2 Kantech T.REX-LT is to be used as REX PIR.

.3 Von Duprin locking hardware shall be used at Cindy Klassen site.

.4 Indala wall switch FP2521A and slim FP2511A Wiegand 26 bit forward readers are to be installed.

Part 3 Execution

3.1 Installation

.1 All consoles, terminals, and controllers shall be factory wired before shipment to the job site.

.2 Cabinet doors shall open a minimum of 170 degrees to avoid blocking personnel movement. Each door shall be equipped with a cylinder lock, a tamper switch and a piano-type hinge with welded tamperproof pins.

.3 Provisions shall be made for field wiring to enter the cabinet via standard knockouts at the top, bottom and sides of controller cabinets.

.4 Each wire shall be identified at both ends with the wire designation corresponding to the wire numbers shown on the wiring diagrams.

.5 All exposed wiring within the cabinets, consoles, and terminals shall be formed neatly with wires grouped in bundles using non-metallic, flame-resistant wiring cleats or wire ties.

.6 All ferrous metal work shall be painted, in accordance with the manufacturer's standards.

.7 All low-level input cables, such as system data and reader cables must be shielded types. The cables run in grounded conduit or at least two feet from AC power, fluorescent lights, or other high energy sources.

3.2 Terminations

.1 Electrical contractor to provide all raceways and pull wires ready for field terminations to be made.

.2 Review with City of Winnipeg for installation practices. Follow City's installation practices.

.3 Provide wire markers on all cables.

.4 All field and cabinet terminations by electrical contractor.

.5 Fork tongue terminals shall be used for connecting wires to port terminals.

.6 Inductive load protection shall be installed at both field device and power supply sides according to CK721 installation instructions.

.7 Wires and modules inside the controller's enclosures shall be labeled. Wires shall be secured inside the enclosure using Ty-raps and adhesive backed mounting brackets. Enough cable slack should be left for servicing the hardware modules.

.8 All I/O field devices should be connected as four-state and DEOL resistors should be installed inside REX PIR case and inside the door frame for the door contacts. If installation of DEOL resistors is impossible in a door frame, City's technicians will determine the location for the resistors fittings.

.9 The Contractor shall terminate and calibrate field I/O devices.

END OF SECTION