Correctional Service Canada
Facilities Branch
Electronic Security Systems

ES/SPEC – 0950
December 23 2014

ELECTRONICS ENGINEERING SPECIFICATION

DOOR CONTROL AND MONITORING SYSTEM

FOR USE IN

FEDERAL CORRECTIONAL INSTITUTIONS

AUTHORITY

This Specification is approved by the Correctional Service Canada for the procurement and installation of a Security Management and Supervision System in Canadian federal correctional institutions.

Recommended corrections, additions or deletions should be addressed to the Design Authority at the following address:

Director, Electronic Security Systems
Correctional Service of Canada
340 Laurier Avenue West,
Ottawa, Ontario
K1A 0P9

Prepared by:

Electronic Systems and Installation Engineer
Electronic Security Systems

Approved by:

Director,
Electronic Security Systems

TABLE OF CONTENTS

ABBREVIATIONS

Abbreviation	Expansion
API	Application Programming Interface
ATP	Acceptance Test Procedure
BIFMA	Business & Industrial Furniture Manufacturers Association
CCDA	Command Control and Data Acquisition
CCTV	Closed Circuit Television
CD	Commissioner’s Directive
CER	Common Equipment Room
COTS	Commercial-Off-The- Shelf
CSA	Canadian Standards Association
CSC	Correctional Service Canada
DCMS	Door Control and Monitoring System
DES	Director Engineering Services
EIA	Electronic Industries Association
FAAS	Facility Alarm Annunciation System
FAR	False Alarm Rate
FDS	Fence Disturbance Detection System
FIU	FAAS Interface Unit
GFE	Government Furnished Equipment
MCCP	Main Communications and Control Post
MDS	Motion Detection System
NAR	Nuisance Alarm Rate
NTP	Network Time Protocol
PA	Public Address
Pd	Probability of Detection
PIDS	Perimeter Intrusion Detection System
PIU	Perimeter Intrusion Detection System Integration Unit
RFP	Request for Proposal
PPA	Portable Personal Alarm
PPAL	Portable Personal Alarm Locatable
SIO	Security Intelligence Officer
SOW	Statement of Work
STR	Statement of Technical Requirements
TCP/IP	Transport Control Protocol/Internet Protocol
TER	Telecommunications Equipment Room
UPS	Uninterruptible Power Supply
V&C	Visits and Correspondence
VIRS	Visits Intercept and Recording System
VMS	Video Management System

Table of Definitions

The following definitions are used in this specification:

#	Term	Example(s)	Description	Function
1	Administrative User Interface		Monitor and Software that supports task specific User Interaction for System Administrators, located in a secure area	Provides Administrative Personnel with the ability to map enrolled users to the functional domains that they are allowed to access and change
2	Application	Cell Call Management, PA Management	Software that is used to deliver Application Support functionality for a sub-system	Software that provides the Operator Interface and supporting logic that allows a sub-system (Control Domain) to be managed
3	CCTV Monitor	PIDS or Range CCTV Monitor	Computer Monitor Hardware	Displays CCTV images for Operator viewing
4	Client		Rack mounted computer located in a secure area away from a Control Post or Control Desk.	Runs software and supports one or more Application
5	Configuration Data	Site floor plans showing quantity of cameras, doors, cells etc. Camera locations. Number of User Interfaces required in a Post.	Site and System specific information typically supplied by CSC that defines how a sub-system Application is to be set-up for a site, location within a site, or post.	The configuration data provides the information that a sub-system application requires to tailor it to meet site, location within a site, or post user requirements.
6	Configuration User Interface		Monitor and Software that supports task specific User Interaction, located in a secure area	Allows suppliers or qualified personnel to add, delete and modify Application Configuration
7	Contract Authority		Public Works and Government Services Canada (PW&GSC) is responsible for all contractual matters associated with the system design and implementation.	
8	Contractor		The company selected as the successful bidder.	

9	Control Console	MCCP Console, Living Unit Control Post Console	Console, typically located in a Control Post. Serves as the physical support infrastructure for Operator User Interfaces	Contains User Interfaces or Control Panels used by staff to execute their management responsibilities and interact with the Domains over which they have Control
10	Control Desk	Living Unit Control Desk	Desk, typically located in a Control Post or Office. Serves as the physical support infrastructure for Operator User Interfaces	Equipped with User interfaces used by staff to execute their management responsibilities and interact with the Domains over which they have Control
11	Control Domain	Cell Call, Guard Tour, Public Address	A group of Physical and Virtual devices or objects, often supported by specialized hardware and software, that performs a set of related functions	Collect information, or activate capabilities in their operational domain
12	Control Panel	PACP, Fire Alarm	Hardware and Software device that provides an Operator Interface (I/O device), located in a Control Post	Allows Operators to manage one or more Domain
13	Control Post	Living Unit Control Post/MCCP	Room or area, typically located in a secure area in an institution	Room used by staff to execute their management responsibilities and interact with the Domains over which they have Control
14	Custom Equipment		Equipment designed and/or manufactured specifically for a specific contract.	
15	Design Authority		Director, Electronic Security Systems (DES) Correctional Service of Canada (CSC) is responsible for all technical aspects of the system design and implementation.	
16	Device	CCTV Camera, Managed Door, Call Origination Device	A specialized device, typically consisting of hardware and software	Provides data collection or activate functions associated with a specific system or sub-system
17	Enrolment User Interface		Monitor and Software that supports task specific User Interaction, located in a secure area	Allows Designated Personnel to enroll and delete Users from the Command, Control and Data Acquisition System.

18	Maintenance User Interface		Monitor and Software that supports task specific User Interaction, located in the CER or Maintenance Service Provider Office	Provides Maintenance Personnel with the ability to interact with one or more Systems to carry out their day to day tasks to troubleshoot and maintain Systems and Subsystems
19	Notification	Notification that a door is opened, or a door is closed, or a sensor is in alarm	A notification is a message that can be shown on a User Interface and/or logged in a database that represents a change in state or a command initiated by an operator.	
20	Off-the Shelf		Equipment currently on the market with available field reliability data, manuals, engineering drawings and parts price list.	
21	Operator User Interface	PIDS Display, Door Control and Monitoring System Display	Computer Monitor and Software that supports User Interaction (I/O device)	Provides an Operator with the ability to interact with one or more Systems to carry out their day to day tasks at a Control Console or Control Desk
22	Project Officer		A CSC employee or a contracted person designated by DES to be responsible for the implementation of the project.	
23	Reporting User Interface		Monitor and Software that supports task specific User Interaction, located in a secure area	Provides Management Personnel with the ability to access preconfigured reports and to create custom reports
24	Server	Network Video Recorder	Rack mounted computer that runs software and is located in an equipment room such as a CER or TER	Runs software that is used to deliver services that support Command and Control Applications to connect to sub-systems
25	State		The state of a device as reported to a sub-system or system	This is a logical representation of the state of a device that is being monitored or managed
26	Sub-system	Cell Call, Guard Tour	A group of Physical and Virtual devices or objects, often supported by specialized hardware and software, that perform a specific set of related functions	Collects information, or activates capabilities in their operational domain

27	System	PIDS	A group of Physical and Virtual devices or objects, often supported by specialized hardware and software, including devices from sub-systems that perform a more general set of related functions	Collects information, or activates capabilities in their operational domain
28	Touch Screen User Interface	Door Control and Monitoring System User Interface	Typically an LCD Monitor with touch screen technology	Allows an Operator to view and interact with the Systems presented on the Monitor
29	Workstation		Rack mounted computer located in a secure area away from a Control Post or Control Desk	Runs software that is used to deliver Command and Control Capabilities

1 INTRODUCTION

The purpose of a Door Control and Monitoring System (DCMS) is to enable Operational Staff in any location that controls Access and Movement to manage and monitor security doors, barriers and access within their span of control where required and to control emergency evacuation and lockdown. Typical examples of such locations would include Living Unit Control Posts, Movement Control Posts, and Visits and Correspondence Offices. The primary purpose of the DCMS is to control and monitor doors from a control post.

2 AUDIENCE

The intended audience includes potential developers, suppliers or integrators of Door Control and Monitoring Systems intended for use within Correctional Service Canada’s Facilities.

3 SCOPE

This specification defines the essential technical and functional requirements for the procurement and installation of a Door Control and Monitoring System for Federal Correctional Institutions. These requirements will describe the Scope and Scale of the DCMS system and the functionality, hardware, software, connectivity and maintainability expected of such a system.

The specifications address the User Interface, The Door Control Application, the Command, Control and Data Acquisition Platform, the connectivity and the devices that will provide the interface with the motors and locking mechanisms use in Door Control Systems, typically PLCs or equivalent devices. The specification does not address the motors and locking mechanisms, which are deemed to be industry standard devices.

4 OVERVIEW – SYSTEM ARCHITECTURE

4.1 Applications and Services

CSC is adopting an approach to the design and deployment of the Command and Control Systems in Institutions that will leverage current object oriented software development methodologies and the re-use of intellectual property. The Operator User Interface will be presented in the form of applications that are served up on a browser or thin client over a secure Intranet. These applications must use the services available to them from an underlying Command, Control and Data Acquisition Platform including, as a minimum:

Virtualization,

Redundancy/Robustness

Clock Generation

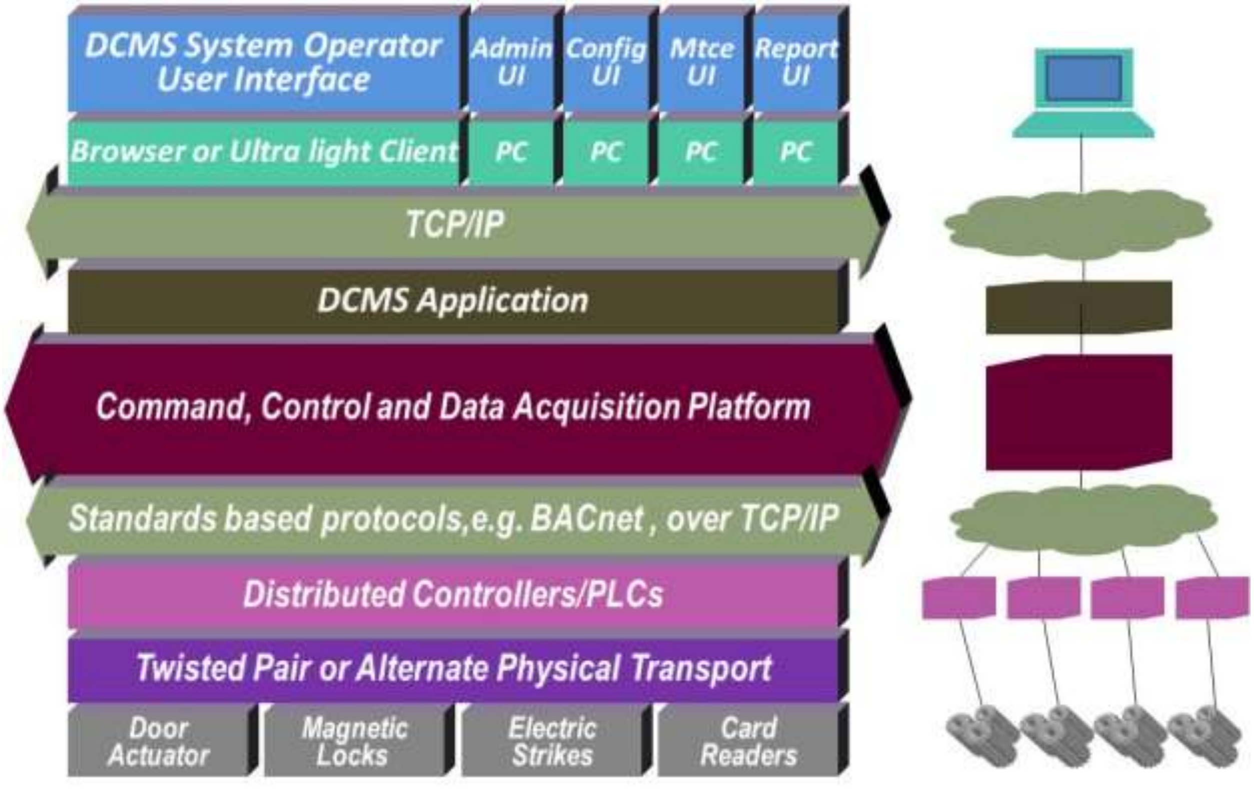
Support for Open APIs to lower level systems

Datalogging

Security and User Authentication

Interfaces to a common communications layer,

Diagnostics and Statistical Report Generation


DCMS System Operator User Interface
Admin UI
Config UI
Mtce UI
Report UI
Browser or Ultra light Client
PC
PC
PC
PC
TCP/IP
DCMS Application
Command, Control and Data Acquisition Platform
Standards based protocols,e.g. BACnet , over TCP/IP
Distributed Controllers/PLCs
Twisted Pair or Alternate Physical Transport
Door Actuator
Magnetic Locks
Electric Strikes
Card Readers

Door Control System Architecture

4.2 System configuration

The DCMS must be designed as a “generic” system that can be configured by the contractor or CSC to meet the specific needs of the Institution or the section of an Institution at which it will be installed. The configuration details will typically provided in a higher level document such as a Statement of Technical Requirements (STR). It must allow any or all of the functionality specified in this document to be configured and be flexible enough to meet the requirements defined in the STR.

4.3 User Interface

The DCMS Operator User Interface and associated Door Control Application functionality is described in the “Standard for the Operator Graphical User Interface for a Door Control and Monitoring System”.

The DCMS system and the underlying application must be designed to allow it to configure and customize the CSC User Interface defined in the “Requirement for the Design of the Framework of Graphical User Interfaces” as one of a number of system configurable managed domains or sub-systems that can be presented to the operator on selection of the appropriate domain or sub-system icon. Typical examples of additional sub-systems that could be managed from the same User Interface on which the DCMS is presented could include power in Cells, lighting in the Living Units video camera control, Environmental Controls available to an Operator and cell call systems.

The DCMS must be designed such that it can be used in both medium and maximum security institutions.

5 APPLICABLE DOCUMENTS

5.1 Specifications, Standards and Statements of Work

The following documents of the issue in effect on the date of the Request for Proposal shall form a part of this specification to the extent specified herein.

ES/SOW-0101	Statement of Work for Installation of Electronic Systems
ES/SOW-0102	Statement of Work for Quality Control of Electronic Systems Installations
ES/SOW-0110	Statement of Work for Structured Cable Systems for Electronic Systems Installations
ES/SPEC-0102	Electronics Engineering Specification, Data Logger for use in Federal Correctional Institutions
ES/SPEC-0603	Electronics Engineering Specification, Facility Alarm Annunciation System Integration Unit for use in Federal Correctional Institutions
ES/STD-0300	Electronics Engineering Standard, Network Time Protocol Server
EIA-310	Electronic Industry Association Standard for Racks, Panels and Associated Equipment

6 REQUIREMENTS

6.1 General

The DCMS is a system allows Doors, Barriers and Gates to be managed and supervised by operators from one or more control locations using a Graphical User Interface. It consists of:

- Application Software, including the User Interfaces, that consists of executable code that runs on the Platform
- Platform Software,
- Platform Hardware,
- Network Connectivity, including cabling, switches and controllers as needed,
- Door control and supervision hardware, (supplied by others)

The DCMS supports the necessary inputs and outputs to monitor and control the devices connected to it, including door, barrier or gate motors and monitor the limit and status switches at each door, barrier or gate. A list of the Door Types to be supported, and their basic functionality, is provided in Appendix A of this document. The DCMS must support User Interfaces that can be presented on touch screen displays in selected locations. Typically each Operator Position is equipped with a pair of displays associated in a redundant configuration to allow for failure and busy periods. The DCMS must consist of the following elements:

The Door Control Application software must include:

- the logic required to manage the devices controlled and monitored by the DCMS based on object modelling concepts and operational sequences provided in *the Requirements for the Operator Graphical User Interface for a Door Control and Monitoring System* ES/STD-0903.
- the logic required to take advantage of the common services provided by the CCDA platform software and hardware, including data logging, network closk synchronization between systems and devices, event and fault reporting:
  - All actions in the DCMS initiated by the operator(s), devices or system diagnostic and monitoring tools must be logged including alarms, acknowledgements, cancellations, escalations, fault alarms, reboots, mask changes, and configuration changes,
  - All DCMS faults and alarms must be generated and stored in a format compatible with the "*Electronics Engineering Specification, Facility Alarm Annunciation System Integration Unit*" ES/SPEC-0603.
- the interfaces, software and logic required to communicate with the devices that are being managed and monitored,
- the ability to support the seamless integration of the behaviour of additional devices and systems that will be defined in future specifications, for example the addition of the user interface objects and the supporting application that would allow a Door Intercom system or a Cell & Unit Lighting Control capability and AC outlets and ventilation systems including fans and to be integrated into the Operator User

Interface to deliver a consistent user experience,

- the capability to deliver and, if needed, enable the development of the User Interfaces as defined in the paragraphs below.

User Interfaces that must include:

- An Operator User Interface on a Touch Screen Display that presents the Operator with the information needed to manage the functionality to be provided by the DCMS, including the visual and audible parameters that the operator will respond to and use to interact with the system. The touch screen display must provide a Framework that will include any graphic images and interactive controls required to manage the target system. A typical graphic map must incorporate the following display features as applicable to the area of presentation:
    - building structures including the devices being managed, including gates, doors, barriers, locks, lights, power etc.;
    - type, condition, priority and real time status of all devices being managed; and
    - emergency instruction and operator prompts, in graphic form wherever possible.
- The system graphics must reduce information clutter to a minimum with the appropriate use of icons, especially to display sensor location and state. Details of all icons, sizes, colours and actions will be provided in the supporting documentation.
- An Administrative User Interface on a display equipped with a keyboard and a pointing device that provides a designated Regional Representative with the ability to enable or disable system users from the pool of previously enrolled users and to assign them system privileges.
- A Report Development and Generation User Interface on a display equipped with a keyboard and a pointing device that provides designated Officers and Staff with the ability to access the system database and to run preconfigured reports from the database using a report generation menu or to develop and run custom reports using a general purpose reporting tool designed to generate reports from the datalogger database. The reporting tool must provide the ability to export the diagnostic data into various file formats (e.g. MS Excel, comma separated values, pdf.)
- If an existing, compatible ID card enrolment system and its User Interface is not available, an Enrolment User Interface on a display equipped with a keyboard and a pointing device that provides the designated Institutional Representative with the ability to enrol, modify or delete system users as represented by their RFID ID card.
- A Configuration User Interface on a display equipped with a keyboard and a pointing device that provides the Contractor or a designated representative with the ability to configure all of the variable parameters of the DCMS, including the creation of screen layouts, maps, positioning of devices etc.
- A Maintenance User Interface on a display equipped with a keyboard and a pointing device that provides the designated Maintenance Service Provider with the ability to access all maintenance and diagnostic services, tools and menus available in the SMSS. In addition, the Maintenance User Interface will allow access to all of the functionality associated with the other User Interfaces, except for the Administrative User Interface.

The Platform Software that must include:

- a Command, Control and Data Acquisition platform that meets the requirements identified in "*Standard for the Command and Control Platform including an Application Development and Service Delivery environment*" ES/STD-0813,
- a distributed processing environment such that the failure of any one hardware element will not disable the Platform and common services,
- a software driven application development and service delivery environment,
- an operating system,
- a structured and defined database or file that contains the complete configuration of the system as implemented for a specific location that can be exported for back up, restoration and training purposes,
- standards for security and access control, high availability, performance, reliability, redundancy and robustness,
- a centrally managed and accessible database for the storage, management and retrieval of events and alarms. A live or "active" copy of this database must be maintained in the Common Equipment Room.

Platform Hardware that must include:

- all Common Server equipment (e.g., computers, power supplies, logic boards, interface units, network switches, etc.) which must be located in an Equipment Room supplied for that purpose. (This area will be identified in the Statement of Technical Requirements.)
  - all equipment deployed in the Equipment Room must be rack mounted in racks compliant with EIA-310.
  - to the maximum practical extent, off-the-shelf equipment must be selected for use in the DCSM. New designs must be restricted to common interface areas, control panels and consoles, or unique devices for which an off-the-shelf item does not exist.
- Touch Screen Displays which will be located in a remotely located Control Console. (Quantity and location to be defined in the Statement of Technical Requirements.) Consistent with the foregoing, only items of equipment such as touch screen displays, visual and audible anunciators, switches, actuators, etc. which the operator must access directly must be located in the control panels.

Platform Service Integration that must include:

- A Data Logger interface that meets the requirements identified in "*Electronics Engineering Specification, Data Logger for use in Federal Correctional Institutions*" ES/SPEC-0102RX, including the ability to communicate using the IP embeeded Starcom Protocol as defined in the "Senstar100 Starcom IP Implementation" attached as an appendix to this document,
- Interface to a Network time Server that meets the requirements identified in "*Electronics Engineering Standard, Network Time Protocol Server for use in Federal Correctional Institutions*" ES/STD-0500R1,

- A FAAS interface that meets the requirements identified in "*Facility Alarm Annunciation System Integration Unit for use in Federal Correctional Institutions*" ES/STD-0500R1,
- include an open SDK for the display interface generation. This is required in the event that the DCMS is deployed as a standalone system.
- provide an object model for all devices that are managed by the system, either as native TCP/IP devices or in the form of metadata that is exposed to the Platform. This will allow their core functionality, including both events and manageable parameters, to be normalised and exposed to higher level systems,
- Use Ethernet networking standards for communications between any and all TCP/IP managed devices and the CCDA platform";
- ensure a minimum of twelve (12) months of data is retained; and
- ensure data over twelve (12) months is deleted automatically.

Network Connectivity that must include:

- all necessary wiring and control equipment required to interface the DCMS to the MCCP Data Logger described in ES/SPEC-0005. In addition, communication must be provided over TCP/IP in the event that the DCMS needs to support an interface to the MCCP Data Logger.
- all necessary wiring and control equipment required to interface the DCMS to the FAAS in the MCCP as described in ES/SPEC-0005. In addition, messages must be provided over TCP/IP in the event that the DCMS needs to support an interface to the MCCP FAAS.
- all necessary wiring and control equipment required to connect the DCMS to the Door Control Hardware, including Programmable Logic Controllers (PLCs) or their functional equivalent.
- Connectivity between system elements must be over TCP/IP over Ethernet wherever possible.

Devices: Door Control and Supervision Hardware:

- The Door Control hardware, and cabling from the Door Actuators, Magnetic Locks, Electric Strikes, RFID Readers and associated Door Switches to the TER, will be provided by others.

Design, supply, installation, testing, documentation and training:

- The contractor must design, supply, install, test and provide documentation and training for any DCMS in accordance with the *"Statement of Work for Installation of Electronic Systems*", ES-SOW 0101.

6.1.1 System Capacity

The DCMS must support:

a) at least two thousand (2,000) cells per Touch Screen User Interface in a Control Post,
b) at least two thousand (2,000) cells per system,
c) at least thirty two (32) Touch Screen Operator User Interfaces per system
d) at least two (2) Administrative User Interfaces per system
e) at least four (4) Report Development and Generation User Interfaces per system
f) at least four (2) Enrolment User Interfaces per system
g) at least two (2) Configuration User Interfaces per system
h) at least two (2) Maintenance User Interfaces per system
i) at least 8,000 edge devices, including all of their manageable and monitored attributes

6.1.2 System Configuration

The DCMS must support:

a) The door types specified in Appendix A

b) Up to 64 Floor plans per Control Domain (this is typically one Control Post that is equipped with a cluster of two to four User Interfaces)

c) The ability to assign between one to four User Interfaces on Touch Screen Monitors to a Command Domain

d) The ability to define a ”home” floor plan for each User Interfaces on the Touch Screen Monitors (This is the plan to which the User Interface reverts on boot up)

e) A minimum of 16 configurable priorities that can be assigned to the state changes from each Edge Device

f) A minimum of 16 configurable Alert Sounds that can be assigned to the state changes from each Edge Device

g) The ability to assign up to 64 doors, gates or barriers to floor plans

h) The ability to assign up to 64 additional “touchable icons” representing other edge devices with up to four managed states and four monitored attributes to floor plans

i) The ability to assign doors gates or barriers to “baseline” Interlock Groups with no Interlock Override

j) The ability to assign up to 16 doors gates or barriers to “baseline” Interlock Groups with Interlock Override

k) The ability to assign up to 16 doors gates or barriers to “optional” Interlock Groups with Interlock Override

l) The ability to configure up to 64 groups of monitored edge devices that are logically related, e.g. door position switches

m) The ability to apply logical operators to the state changes reported by the edge devices and to apply timers to the state changes reported by the edge devices
n) The ability to trigger predefined alarm or event strings to a higher level system based on the logical states defined by these groups

6.1.3 System Performance

The DCMS must:

a) Provide 99.9% availability,
b) Deliver an MTBF of 3 years,
c) Provide redundant Application software and User Interfaces with seamless failover between the active instance of the Application Software and a back up instance of the Application Software,
d) Support a latency of no greater than one (1) second between a change of state at an edge device and an indication of that change of state on the Operator User Interface,
e) Support a latency of no greater than 1 second between the selection of a command on the Operator User Interface and the delivery of a signal to an edge device.

6.1.4 Period of Operation

The DCMS and all associated equipment must be rated and capable of operation 24 hours per day, seven days a week with an expected operational life of no less than 10 years.

A system failure will be deemed to have occurred when any required alarm or warning (visual or audible) is not produced or when any required control function cannot be performed.

Loss or restoration of primary power to the system must not produce spurious readings or outputs to the data logger. When power is returned after a power failure, the system must resume normal operation without operator action and must automatically start from a pre-defined and pre-configured start up condition.

6.2 System Requirements

6.2.1 Commercial-Off-The-Shelf Equipment

The DCMS must use commercial off-the-shelf Command Control and Data Acquistion software and hardware and proven designs to the maximum extent possible. All new software and hardware must meet the specified lifespan requirements. The goal is to allow integration of co-located systems on to shared displays and provide a consistent, common look and feel. The system design must provide open Ethernet TCP/IP APIs to the system controllers and the edge devices to allow integration with future systems. The API must be provided to allow the DCMS to be usable in an extensible, open architecture, security electronics framework, exposing the status of all managed objects to higher level systems and allowing the manageable attributes of all managed objects to be addressed by higher level systems through the API.

6.2.2 Technical Acceptability

The CSC operational environment is unique for its diversity of locations, climate exposures and the physically restrictive construction techniques of penal institutions. Maintaining national security, the safety of staff and offenders alike is CSC's commitment to the government and public. Electronic security systems operating in this unique environment must maintain very high standards of dependability and reliability.

The CSC Technical Services Branch, Engineering Services Division has established technical specifications and equipment standards for specific electronic security systems which are based on very specific and restrictive operational performance criteria as detailed in its Electronic Engineering Standard. Technical acceptability of these systems means that the equipment complies with the pertinent CSC specifications and standards.

6.2.3 System Definition Deliverables and Parameters

The Contractor must:

- include an open integrated development environment (IDE) for designing graphical user interfaces,
- include a runtime environment where a device automation objectfor each type of device that is managed by the DCMS regardless of whether the device is a native addressable TCP/IP device or a device that is represented by metadata. This will allow the device functionality, including both events and manageable parameters, to be accessed, normalised and exposed to the DCMS application or other applications that may eventually run on the platform,
- provide a copy of the database structure and schema,
- provide a published or standard protocol for communications between all TCP/IP managed devices and the platform, preferably based on existing network standards such as SNMP;
- ensure a minimum of twelve (12) months of data is retained; and
- ensure data over twelve (12) months is deleted automatically.

6.2.4 Human Factors

The GUI for the DCMS must conform to accepted principles of good human factors design.

6.2.5 Existing Equipment

In most installations, control and annunciation elements of the DCMS will share console space with other electrical/electronic equipment such as intercoms, cell call systems, lighting controls, etc. and will be operated by the same staff member. In such cases it is important that effort be made to coordinate the functional and operational design of the DCMS according to accepted human engineering principles to ensure a uniform appearance and commonality of a layout to assist the operator in the performance of their duties.

6.2.6 System Components

The DCMS must consist of the following elements or devices in the quantities given in the Statement of Technical Requirements (STR):

a) Distributed Door Controllers
   i. must connect using Ethernet/IP (either directly or from an I/O end device such as the Request to Exit switch),
   ii. if connected to an I/O device, be equipped with supervised wiring to detect short circuits and open circuits,
   iii. must be powered directly by Power over Ethernet (PoE) or from the I/O end device;

b) Magnetic Locks – Provided by Others/GFE
c) Magnetic Strikes – Provided by Others/GFE
d) Touch Screen <u>Operator User Interface</u>
   i. deployed according to the STR, may be presented on the same Operator User Interface as other sub systems or control domains,
   ii. a graphical touch screen display,
   iii. 22” screen size with an aspect ratio of 16:9
   iv. full highth-definition (FHD) display (1080 resolution), and
   v. an RFID reader for application access control
e) Administrative User Interface
f) Report Development and Generation User Interface
g) Enrolment User Interface
h) Configuration User Interface
i) Maintenance User Interface
j) Support for connectivity to a hard wired “kill switch” input to turn off power to Operator Interfaces and to provide an alarm output to the Facility Alarm Annunciation System Integration Unit for use in Federal Correctional Institutions in compliance with the Starcom over IP Protocol provided as an Appendix.
k) include an open SDK for the display interface generation.
l) The configuration for the displays defined in sections e) through j) above is as follows
   i. deployed according to the STR,
   ii. a graphical display,

iii. minimum 22" screen size with an aspect ratio of 16:9.
iv. full highth-definition (FHD) display (1080 resolution),
v. an RFID reader for application access control, and;
vi. two (2) USB 2.0 (or better) ports (to be used for a keyboard and mouse, a USB keyboard and a USB mouse are part of this system);

m) Common equipment (network hardware, switches, routers, servers, historical data archiver/data logger in the CER, etc.);
n) Interconnecting wiring, cables, etc.; and
o) Conduit, ducts, outlet boxes, etc.

6.2.7 Wires, Cables, Conduits, Ducts

The contractor must supply all necessary terminations, cross connection cabinets, conduits, wire and cabling and any other items that may be required for the satisfactory completion of the specified system. All installation workmanship must be performed in accordance with ES/SOW-0102 and ES/SOW-0110 Statements of Work and all applicable national, provincial, and local electrical codes.

A wiring diagram must be supplied in the Installation section of the Maintenance Manual to detail where module connections terminate and how wires are routed and terminated.

Conduits, cables, ducts, trays, etc. may be either GFE or must be supplied and installed by the contractor depending on the particular institution. The determination will be made by the Design Authority and will be identified in the RFP.

Connectors provided on the ends of any cable must mate with the corresponding connector on the equipment. Adapters from one type of connector to another are not acceptable.

6.2.8 Common Equipment

Where feasible and practical all common equipment (e.g., servers, power supplies, logic boards, amplifiers, etc.) must be located in the Terminal Equipment Room or Space supplied for that purpose. This area will be identified in the STR. Consistent with the foregoing, only items of equipment such as Touch Screen User Interfaces, other visual and audible annunciators, switches, actuators, etc. which the operator must access directly must be located in the control panels.

All equipment deployed in Terminal Equipment Room must be rack mounted in racks compliant with EIA-310.

To the maximum practical extent, off-the-shelf equipment must be selected for use in the DCMS. New designs must be restricted to common interface areas, control panels and consoles, or unique devices for which an off-the-shelf item does not exist.

6.2.9 Interface to Data Logger

If the DCMS is a free standing system as opposed to an application running on a common Command, Control and Data Acquisition Platform, the contractor must supply and install all necessary wiring and control equipment required to interface the ICCS to the MCCP Data Logger described in ES/SPEC-0005, including the ability to communicate using the IP embedded Starcom Protocol as defined in the “Senstar100 Starcom IP Implementation” attached as an appendix to this document.

If the DCMS is an application running on the Command, Control and Data Acquisition Platform, the Application must communicate with the Data logger that is part of the Common Services. All actions in the DCMS must be logged including alarms, acknowledgements, cancellations, alarm escalations, escalations from group alarms, fault alarms, reboots, mask changes, shutdowns and configuration changes.

6.2.10 Interface to MCCP/FAAS

If the DCMS is a free standing system as opposed to an application running on a common Command, Control and Data Acquisition Platform, the contractor must supply and install all necessary wiring and control equipment required to connect the DCMS to the FAAS in the MCCP as described in ES/SPEC-0005 over the Security IP Network. The message formats must be as described in ES/STD-0102.

If the DCMS is an application running on the Command, Control and Data Acquisition Platform, the Application must communicate with the FAAS Application that runs on Platform. All DCMS faults and alarms must be relayed in near real-time to the FAAS in the formats defined in the “Senstar100 Starcom IP Implementation” attached as an appendix to this document as an Appendix to this document.

Emergency Shutdown:

Each Control Post that is equipped with the Door Control Application’s Operator User Interface must provide the ability to quickly engage an Emergency Shutdown of the Control Post and all associated workstations. When the Operator User Interface is undergoing an emergency shutdown the application must send an alarm notification message to the FAAS indicating that emergency shutdown event, After an emergency shutdown, the Operator User Interface will not be accessible in the Control Post until it has been re enables externally.

Also, the Control Posts with Operator User Interfaces (both active and inactive) must also have the capability to be shut down by a command received from the MCCP to perform an emergency shutdown.

Forced Entry Alarm Escalation:

When the pre configured elapsed time associated with a forced entry alarm expires and is detected by the DCMS, the system must send an alarm notification to the FAAS so that the appropriate security protocols can be followed to ensure the safety of the Institution and the inmates.

Door Group Alarm Escalation (interlocked or Sally Port Configuration):

The DCMS must wend an alarm notification to the FAAS when a door position switch for doors configured in a group was triggered after a preconfigured lapse of time.

Transfer of Control:

The DCMS must support the ability to transfer control from one workstation to another based on preconfigured settings. Authentication for this action is required by means of a password or RFID card swipe.

6.3 Design Requirements

6.3.1 Physical Configuration

The DCMS must be designed to ensure that the system servers are located in secure, environmentally controlled environments identified in the STR and that User Interfaces are as "thin" as possible and require minimal computing power to deliver them.

The DCMS Operator User Interfaces must be delivered on browsers or thin clients such that all that is required in a Control Console is a Touch Screen User Interface. The Touch Screen User Interface must be connected to the system server over a TCP/IP network.

All other DMCS User Interfaces can be delivered either on a browser, a thin client or a workstation connected to the Command, Control and Data Acquisition Platform by means of a TCP/IP network.

Connectivity between the Servers running the Command, Control and Data Acquisition Platform and the Distributed Controllers that are located in secure environments close to the Devices being managed must be over a TCP/IP network.

Wherever physically possible, the DCMS must be implemented using a space-diversity approach to system planning to ensure that loss of one interconnection routing does not impair the operational capability of the complete ICCS system.

6.3.2 Network Connectivity

The Contractor must supply a system in which the connectivity between the system components uses TCP/IP except for connectivity between the Distributed Controllers, or equivalent, and Door and Lock Hardware.

A design objective is to use TCP/IP over Ethernet to connect the system elements with PoE being used to power edge devices where this is technically feasible. Acceptable protocols include:

- Ethernet/IP

The Contractor can propose alternate means of connectivity as long as the interface to the Command, Control and Data Acquisition Platform uses a CSC approved protocol and supports connectivity to a TCP/IP network.

6.3.3 Wiring Supervision

All signal wiring other than TCP/IP cables must be supervised in all system modes. An alarm must occur if any system wiring is cut or shorted to other wires or if the system devices are tampered with by unauthorized persons or environmental conditions. Ethernet elements must be monitored with regular communication checks at least every minute.

6.3.4 Sabotage, Tampering and Survivability

Elements of the DCMS must operate in areas exposed to inmate access and must have high resistance to damage, destruction, or conversion to other uses (including weapons). All interconnecting service must be secure against tampering, improper interception, or interference. In particular, the Request to Exit switch must not provide a suspension point nor must it have more than the thickness of the face plate proud of the wall.

6.3.5 Application Software Design

The behaviour and appearance of the DCMS application software for the Operator User Interface is defined in detail in the "*Requirements for the Operator Graphical User Interface for a Security Management System*", and must be developed using the software design best practices, as identified in paragraph 6.3.6 below.

The behaviour and appearance of the application software that supports the features and functionality of the other DCMS User Interfaces is defined at a high level as part of this specification. It must also be developed according to software design best practices, as identified below.

6.3.6 Software Design Best Practices

Software design best practices must be used in developing any custom software application required to implement the DCMS. Typical software best practices are defined as:

- Selection of the appropriate development process which incorporates an Object-Oriented design and integration approach,
- Selection and usage of the appropriate development tools intended for this functional domain,
- The use of source-control management software,

- Application of sound estimating techniques,
- Preparation of project plans with multiple and achievable development milestones,
- Project Leadership in the management and delivery of software per established project plan milestones.
- Development of modular, portable, extensible and reusable code that is portable and can be reconfigured to meet similar requirements at the same or other locations,
- Provide tools to support the configuration of the system in an easy and intuitive manner,
- Application of periodic testing practices with multiple customer acceptance of testing results,
- Development of detailed software documentation and user manuals for the various user interfaces,

The Contractor must provide details of its proposed software development process and how it intends to meet the software best practices provided above for the development of custom application functionality for the DCMS application.

6.4 Operational Requirements

6.5 General

All applications must be implemented as browser based or thin client applications running on workstations at one (1) or more locations as specified **in the STR. The Operator User Interfaces will be located in the Control Post or Posts specified in the STR.**

All applications except for the Operator User Interface, which is defined explicitly, shall:

- Provide an on-screen legend, possibly implemented as a pop up window to explain icons, colours and usage;
- Accept input to toggle between French and English versions; and
- Provide the ability to modify the French and English messages

6.5.1 Operator User Interface

The Operational requirements for the Operator User Interface are provided in the ““*Requirements for the Operator Graphical User Interface for a Security Management System*”. This document provides sample operations sequence for the typical operator actions required to manage the range of Doors, Barriers, Gates and Alarms that are associated with an DCMS in an Institutional environment.

The Design Requirements for the development of the Operator Graphical User Interface are provided in “Icons for the graphical user interfaces for use in federal correctional institutions”. This document defines the essential design and functional requirements for the Icons to be used for the Graphical User Interface that is to be incorporated into the design of all User Interfaces for all control posts for Federal Correctional Institutions.

6.5.2 Administrative User Interface

An Administrative User Interface, located in the CER, on a Display equipped with a keyboard and a pointing device that provides the Regional Technical Authority with the ability to enable or disable system users from the pool of previously enrolled users and to assign them system privileges.

The Administrative Application must provide administration capabilities including:

a) be displayed on the Configuration User Interface;
b) require an Admin enabled RFID card, or username and password, to access the system;
c) accept an RFID card input to log the user out of the system or from the User Interface;
d) automatically log the current user out of the system or from the User Interface after five (5) minutes of inactivity;
e) allow generation and printing of reports as follows:
   i. list by user type as specified by the authorized RFID cards and names sorted by last name, and
   ii. list added and/or removed authorized RFID cards and names, with authorizing RFID card number and, sorted by date range sorted by date and time;
f) add/remove authorized RFID cards with names for Operator, Configurer, Reporter, Maintainer, and Admin privileges.
g) accept input from a USB keyboard and mouse.

6.5.3 Diagnostics and Statistics Report User Interface

The DCMS must provide a User Interface that enables the creation and generation of reports that is installed at one (1) or more location that specified in the STR, on a Monitor equipped with a keyboard and a pointing device. The reporting tool that provides designated Officers and Staff with the ability to access the system database and to run preconfigured reports from historical data stored in the database. The diagnostic and Statistics report Application must provide reporting capabilities including:

a) accept input from a USB keyboard and mouse.

6.5.4 Enrollment User Interface

If an existing, compatible RFID card enrollment system and its User Interface is not available, an Enrollment User Interface on a Display, at one (1) or more locations specified in the STR, equipped with a keyboard and a pointing device that provides the appropriate Institutional Representative with the ability to enroll or delete system users as represented by their RFID ID card.

The Enrollment Application will provide the following capabilities:

a) be displayed on the Configuration Monitor;
b) accept an RFID card input to log the user out of the system or from the User Interface;
c) automatically log the current user out of the system or from the User Interface after five (5) minutes of inactivity;
d) add/remove authorized RFID cards with names for User, Reporter, and Configurer privileges– this will either share/extend an existing RFID card database or require creation of one that will be used by this and other future applications.
e) Change User's details, including, but not limited to:
   i. Name
   ii. ID number
   iii. Photograph
   iv. Authorization Level
f) accept input from a USB keyboard and mouse.

6.5.5 Configuration User Interface

A Configuration User Interface on a Display, at one (1) or more locations specified in the STR, equipped with a keyboard and a pointing device that provides the Contractor or a designated representative with the ability to configure all of the variable parameters of the SMSS, including the creation of screen layouts, maps, positioning of devices etc.

The Configuration Application will provide the following capabilities:

a) be displayed on the Configuration Monitor;
b) accept an RFID card input to log the user out of the system or from the User Interface;
c) automatically log the current user out of the system or from the User Interface after five (5) minutes of inactivity
d) create/edit descriptive information for each device up to 30 characters;
e) assign doors to cells;]
f) assign cells to ranges;
g) assign ranges to units;
h) configure interlock tables;
i) have the acknowledge timeout set to 1 minute, fixed;
j) have the service timeout set to 5 minutes, fixed;
k) have the door mask timeout set to 1 hour, fixed;
l) allow generation and printing of reports that support the following commands, alarms, events or state changes where the commands or state changes are invoked by the operator and the events and state changes are initiated by the device:
   i. Door Secured
   ii. Barrier closed
   iii. Door Unsecured
   iv. Barrier open

v. Device Selected
vi. Open/Unlock command by touchscreen
vii. Maintain Open/Unlock by touchscreen
viii. Door Close by touchscreen
ix. Cancel Maintained Unlock by touchscreen
x. Interlock Override by touchscreen
xi. Door held open alarms
xii. Communication/System Fault Alarm
xiii. Selection of Mask/Double Lock
xiv. Removal of Mask/Double Lock
xv. Selection of Local Enable/Inmate Pass
xvi. Removal Local Enable/Inmate Pass
xvii. Operation of environmental controls/lighting by device
xviii. Intercom calls initiated and answered
xix. Unit DCMS Shut-down
xx. Unit DCMS Enabled:

m) allow editing of English and French user text messages;
n) allow archiving Single Detail Reports to external, USB connected storage in a text format; and
o) accept input from a USB keyboard and mouse.

6.5.6 Maintenance User Interface

A Maintenance User Interface on a Display, at a location or locations specified in the STR, equipped with a keyboard and a pointing device that provides the designated Maintenance Service Provider with the ability to access all maintenance and diagnostic services, tools and menus available in the DCMS. In addition, the Maintenance User Interface will allow access to all of the functionality associated with the other User Interfaces, except for the Administrative User Interface.

The Maintenance Application must provide maintenance capabilities including:

a) be displayed on the Configuration Monitor;
b) all selection of Report, Configuration or Maintenance application.
c) accept an RFID card input to log the user out of the system or from the User Interface;
d) automatically log the current user out of the system or from the User Interface after five (5) minutes of inactivity;
e) report on the status of the I/O of each device;
f) allow generation and printing of a fault/tamper list for a user selectable time interval;
g) Door Control maintenance mask/unmask any Door in the facility – not subject to mask timeout; and
h) accept input from a USB keyboard and mouse.

6.5.7 User Access and Scope of Control

Application access must be limited according to the following RFID privilege levels:

		Applications					
		Status	Monitoring	Reporting	Configuration	Maintenance	Admin
Privilege	User	Yes	N/A	No	No	No	No
	Reporter	Yes	N/A	Yes	No	No	No
	Configurer	No	N/A	Yes	Yes	No	No
	Maintainer	Yes	N/A	Yes	Yes	Yes	No
	Admin	No	N/A	No	No	No	Yes

An RFID card must have at most one privilege assigned. The Reporter privilege will likely be assigned to Correctional Managers. The Monitoring Application is integrated only into the MCCP and does not use any card authorization.

6.5.8 Interface to Data Logger

The DCMS must have the ability to provide an output to the Data Logger described in ES/STD-0102, to provide a record of all DCMS events including the state changes described in section 6.4.5.l and:

a) System failures and restorations;
b) Door alarms with unit, range and cell;
c) all tamper/fault alarms with unit, cell and any available details;
d) Entry and Exit from Evacuation Mode
e) Change of State of any managed Edge Device
f) Key switch for TER/CER located in a secure area outside the Control Post, excluding the T&E/TER room.

All of these activities must be logged in plain-language (or approved abbreviation thereof) without the need for a cross-reference table. The events must also include date and time to the nearest second.

6.5.9 Interface to FAAS

The DCMS reports events, alarms and faults to the MCCP. The alarms are integrated into the existing FAAS application at the MCCP.

The FAAS shall:

a) display alarms for:
    i. Kill switch Activation and deactivation via the Key Switch ,
    ii. Entry and Exit of Evacuation Mode,

6.6 Environmental Requirements

All DCMS hardware must operate within the following indoor environmental conditions:

a) Temperature: 0□□C to +50□□C; and
b) Humidity: 0 to 90% relative, non-condensing.

6.7 Power Requirements

All DCMS control hardware must use VAC power within the following limits:

a) Voltage: 120 VAC ±10%;
b) Frequency: 60 Hz ±1.5%;
c) Transients: up to 5 times nominal voltage for up to 100 msec durations. Changes in the input power or any fluctuations within the above limits must not cause damage to the unit;
d) Power: power consumption must not exceed 100 watts per display; and
e) Power backup: all components of the system must be supported by UPSs for a minimum of 1 hour.

6.8 Installation Requirements

The DCMS must be installed at the site in accordance with the ES/SOW-0101, Statement of Work and the ES/SOW-0102, Statement of Work.

6.9 Documentation Requirements

All final DCMS documentation must be provided in accordance with the ES/SOW-0101, Statement of Work.

6.10 Support Requirements

The DCMS maintenance support must be provided in accordance with the ES/SOW-0101, Statement of Work.

6.11 Training Requirements

Operator training and maintenance training on the DCMS must be in accordance with the ES/SOW- 0101, Statement of Work.

7 QUALITY ASSURANCE

The DCMS Quality Assurance program must be provided as detailed in the ES/SOW-0101, Statement of Work.

All on-site installation work, test plans and system acceptance testing must be conducted in accordance with the ES/SOW-0101, Statement of Work.

8 DELIVERY

Delivery requirements for the DCMS documents, drawings, plans, manuals, etc. (where applicable) must be in accordance with the ES/SOW-0101, Statement of Work.

Delivery requirements of the DCMS equipment must be in accordance with the ES/SOW-0102, Statement of Work.

9 INTERFERENCE

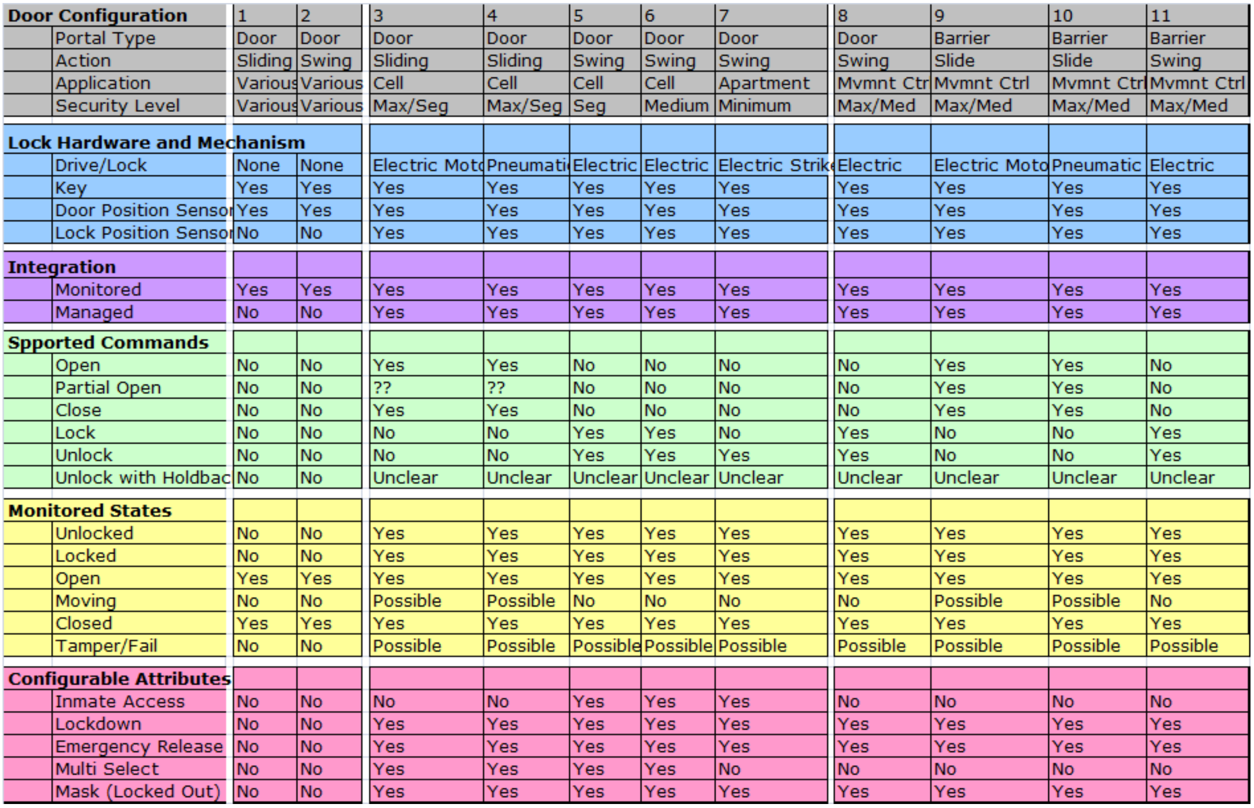
Performance of the DCMS must not be affected by the use of standard electronic equipment used at the institution. Distance limits of standard electronic equipment are as follows:

a) 5 watt CB transceivers at 1 metre or more;
b) 6 watt VHF and UHF transceivers at 1 metre or more;
c) 25 mW 420-430 MHz Personal Portable Transmitters at 1 metre or more;
d) Other radio frequency transmitting, receiving and distribution equipment at 5 metres or more; and
e) Personal computer and/or computer work stations at 5 metres or more.

10 SAFETY

All DCMS electrically powered elements must meet the applicable CSA standards.

Appendix A



Door Configuration		1	2	3	4	5	6	7	8	9	10	11
	Portal Type	Door	Door	Door	Door	Door	Door	Door	Door	Barrier	Barrier	Barrier
	Action	Sliding	Swing	Sliding	Sliding	Swing	Swing	Swing	Swing	Slide	Slide	Swing
	Application	Various	Various	Cell	Cell	Cell	Cell	Apartment	Mvmnt Ctr	Mvmnt Ctrl	Mvmnt Ctrl	Mvmnt Ctrl
	Security Level	Various	Various	Max/Seg	Max/Seg	Seg	Medium	Minimum	Max/Med	Max/Med	Max/Med	Max/Med
Lock Hardware and Mechanism												
	Drive/Lock	None	None	Electric Moto	Pneumati	Electric	Electric	Electric Strik	Electric	Electric Moto	Pneumatic	Electric
	Key	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
	Door Position Senso	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
	Lock Position Senso	No	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Integration												
	Monitored	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
	Managed	No	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Spported Commands												
	Open	No	No	Yes	Yes	No	No	No	No	Yes	Yes	No
	Partial Open	No	No	??	??	No	No	No	No	Yes	Yes	No
	Close	No	No	Yes	Yes	No	No	No	No	Yes	Yes	No
	Lock	No	No	No	No	Yes	Yes	No	Yes	No	No	Yes
	Unlock	No	No	No	No	Yes	Yes	Yes	Yes	No	No	Yes
	Unlock with Holdbac	No	No	Unclear	Unclear	Unclear	Unclear	Unclear	Unclear	Unclear	Unclear	Unclear
Monitored States												
	Unlocked	No	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
	Locked	No	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
	Open	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
	Moving	No	No	Possible	Possible	No	No	No	No	Possible	Possible	No
	Closed	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
	Tamper/Fail	No	No	Possible	Possible	Possible	Possible	Possible	Possible	Possible	Possible	Possible
Configurable Attributes												
	Inmate Access	No	No	No	No	Yes	Yes	Yes	No	No	No	No
	Lockdown	No	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
	Emergency Release	No	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
	Multi Select	No	No	Yes	Yes	Yes	Yes	No	No	No	No	No
	Mask (Locked Out)	No	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes