CORRECTIONAL SERVICES CANADA
TECHNICAL SERVICES BRANCH
ELECTRONIC SECURITY SYSTEMS

ES/ SPEC -0404
Revision 3
2013 April 18

ELECTRONIC ENGINEERING SPECIFICATION

MOTION DETECTION SYSTEM

FOR USE IN FEDERAL CORRECTIONAL INSTITUTIONS

AUTHORITY

This Specification is approved by the Correctional Service of Canada for the procurement and installation of Motion Detection Systems (MDS) 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

Approved by:

Director, Electronic Security Systems

TABLE OF REVISIONS

Revision	Paragraph	Comment
3	All	Initial update from Revision 2 (EM) and review with Tech Services stakeholders.

TABLE OF CONTENTS

TABLE OF ABBREVIATIONS

Abbreviation	Expansion
API	Application Programming Interface
ATP	Acceptance Test Procedure
CD	Commissioner's Directive
CER	Common Equipment Room
COTS	Commercial-Off-The- Shelf
CCDA	Communications, Control and Data Acquisition platform
CSA	Canadian Standards Association
CSC	Correctional Service Canada
DES	Director Engineering Services
EIA	Electronic Industries Association
FAAS	Facility Alarm Annunciation Sub-System
FAR	False Alarm Rate
FDDS	Fence Disturbance Detection Sub-System
GFE	Government Furnished Equipment
MCCP	Main Communications and Control Post
MDS	Motion Detection Sub-System
NAR	Nuisance Alarm Rate
NTP	Network Time Protocol
PIDS	Perimeter Intrusion Detection Sub-System
PIU	Perimeter Intrusion Detection System Integration Unit
Pd	Probability of Detection
RFP	Request for Proposal
SOW	Statement of Work
STR	Statement of Technical Requirements
TCP/IP	Transport Control Protocol/Internet Protocol
UPS	Uninterruptible Power Supply

TABLE OF DEFINITIONS

Term	Definition
Design Authority	Director, Engineering Services (DES) - Correctional Service of Canada (CSC) is responsible for all technical aspects of the system design and implementation.
Contract Authority	Public Works and Government Services Canada (PW&GSC) is responsible for all contractual matters associated with the system design and implementation.
Contractor	The company selected as the successful bidder.
Project Officer	A CSC employee or a contracted person designated by DES to be responsible for the implementation of the project.
Off-the Shelf	Equipment currently on the market with available field reliability data, manuals, engineering drawings and parts price list.
Custom Equipment	Equipment designed and/or manufactured specifically for a specific contract.
Perimeter Sector	The phrase Perimeter Sector or Sector used on a stand-alone basis describes one of the discrete, contiguous Radio Frequency detection fields that is aligned with each physical sector making up the complete perimeter and runs parallel to the buried cables.
Detection Zone	The phrase Detection Zone or Zone used on a stand-alone basis describes the area of Radio Frequency sensitivity surrounding and perpendicular to the buried cables.

1 INTRODUCTION

1.1 Overview

.1 This specification defines the essential technical and functional requirements of the Correctional Service of Canada for the procurement and installation of modular, ranging, buried electromagnetic field sensor to be deployed as Motion Detection Sub-System (MDS) for federal correctional institutions. This sub-system is an element of the Perimeter Intrusion Detection Systems (PIDS) installed at many Federal Institutions and will share a Common User Interface with the Fence Disturbance Sensor Sub-System (FDS), the PIDS Public Address sub-system and the PIDS CCTV sub-system.

.2 The sensor must be configurable into discrete detection segments that can be between three (3) metres long and one hundred and fifty (150) metres long. The sensor detection segments must be configurable into discrete detection sectors that can vary in length from three (3) metres to one hundred and fifty (150) metres. The detection sectors must support perimeters up to and including up to two thousand (2,000) metres in length.

.3 The system must consist of the following components:

.1 A buried cable sensor sub-system with a common, protected power, data and sensing cable connected to a network interface unit;

.2 A network interface unit or gateway that provides power and data communications to the sensor network as well as an interface, using a standard based and published protocol, to a Command, Control and Data Acquisition (CCDA) platform.

.3 A Perimeter Intrusion Detection System Integration Unit operating as the CCDA, unless specified in the STR.

.4 A Network Interface Unit, which must provide visibility and control of the manageable attributes of the sensors and the events presented by the sensors to the CCDA.

.5 an MDS application software that runs on the Command, Control and Data Acquisition (CCDA) platform or on a sub-system server that is connected to the Command, Control and Data Acquisition (CCDA) platform, that provides the necessary software functionality to allow the MDS system to be configured, administered, maintained and accessed for reporting services through function specific User Interfaces.

.6 If specified in the STR, a PIDS software application that runs on the Command, Control and Data Acquisition (CCDA) platform that provides the necessary software functionality to manage the MDS sensor sub-system, detect alarm and event notifications from the sensor sub-system and provide the Operator User Interface.

.4 User Interfaces must include:

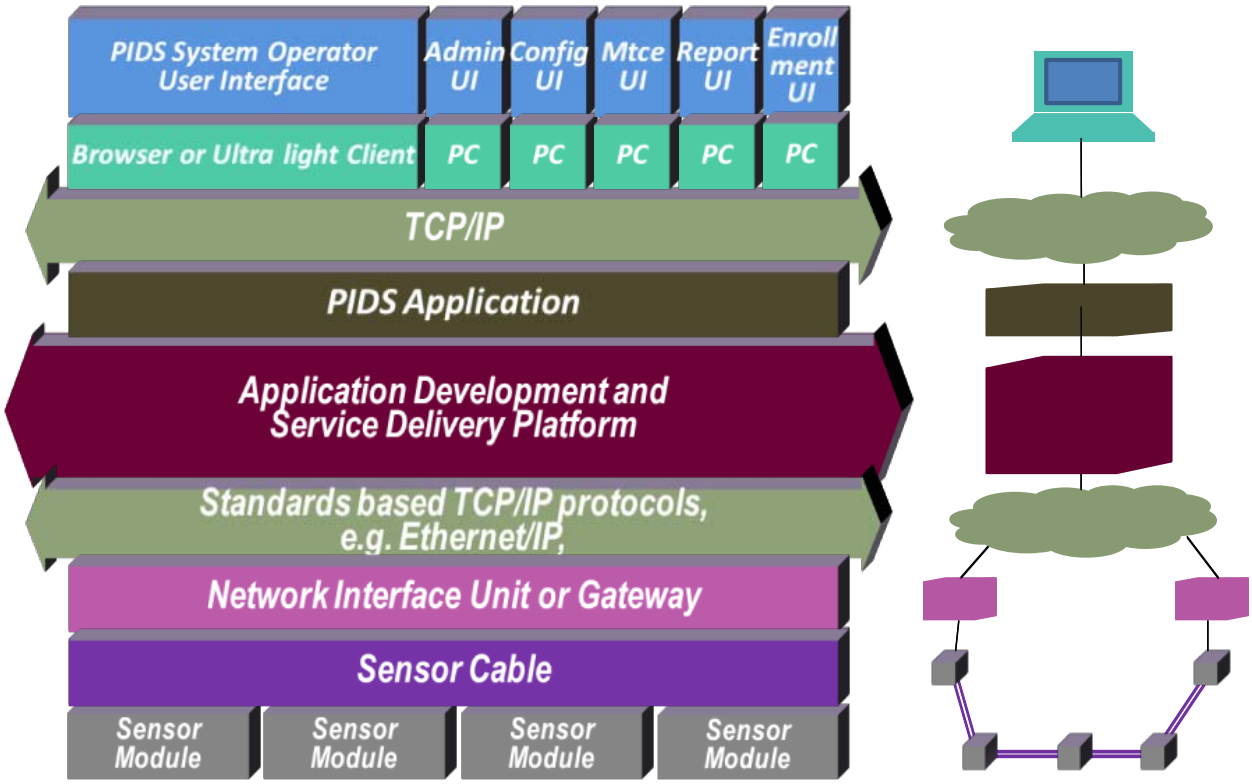
.1 If specified in the STR, an Operator User Interface that presents the Operator with the information needed to manage the functionality to be provided by the MDS sub-system.

.2 An Administrative User Interface.

.3 A Report Development and Generation User Interface.

.4 A Configuration User Interface.

.5 A Maintenance User Interface.



MDS Sub-System Architecture

1.2 Purpose

.1 The primary purpose of a Buried line MDS is to detect attempts by an intruder to penetrate a perimeter around a facility. They must operate in the outdoor environment and must perform reliably in all weather conditions. The detection field must be formed by radio-frequency (RF) signals carried by sensor cables that are buried along the length of the perimeter to be protected. The RF signals must form an invisible electromagnetic detection field around the sensor cables that can locate and detect an intruder passing through the field.

.2 The MDS-subsystem may be used in any institution equipped with a double perimeter fence that meets the spacing requirements for the deployment of a buried cable sensor.

1.3 Commercial Off-The-Shelf Equipment

.1 The MDS must use commercial off-the-shelf (COTS) equipment and proven designs to the maximum extent possible. New technology proposed must be compatible with the Command and Control environment of the Institution at which it will be installed and may be subject to evaluation by CSC to ensure that is technically acceptable following the steps defined in section 1.4.

1.4 Technical Acceptability

.1 The Correctional Service Canada (CSC) operational environment is unique for its diversity of locations, climate exposures and the physical restrictive construction techniques of penal institutions.

.2 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.

.3 The CSC Electronic Security Systems Directorate has established technical specifications and equipment standards for specific electronic security sub-systems which are based on very specific and restrictive operational performance criteria as detailed in its Electronic Engineering Specifications and Standards. Technical acceptability of these sub-systems means that the equipment complies with the relevant CSC specifications and standards.

.4 The technical acceptance process must involve system and sub-system evaluation in accordance with the applicable CSC specifications.

.5 CSC may when it deems necessary, request the supplier to arrange for a full site demonstration.

.6 CSC must verify in depth any of the system technical specifications called up.

.7 CSC may rely on manufacturer's test results for specific areas of the specification where an independent test facility has conducted the test, and the facility is deemed acceptable to CSC.

1.5 Quantity of Equipment

.1 The quantity and location of the MDS equipment required for CSC institutions will be contained in the information identified in the site specific Statement of Technical Requirements or Statement of Work.

2 REFERENCES

2.1 Specifications, Standards, and Statements of Work

.1 Access to non-government specifications is the responsibility of the contractor.

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

Number	Title
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-0005	Specification for Main Communications and Control Post Integration Consoles
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
ES/STD-0806	Standard for Icon Design for the User Interface for use in Federal Correctional Institutions (draft)
ES/STD-0807	Standard for the Look and Feel of the User Interface for use in Federal Correctional Institutions (draft)
ES/STD-0808	Standard for the Design of the Framework for the User Interface for use in Federal Correctional Institutions (draft)
EIA-310	Electronic Industry Association Standard for Racks, Panels and Associated Equipment

3 OPERATIONAL REQUIREMENTS

3.1 General

.1 The MDS sub-system at an institution consists of sensor cables buried below ground between the fences around its perimeter divided into discrete sectors. These sensor cables transmit and receive an electromagnetic field that, when disrupted, detects conductive materials (e.g. people) above them. The cables are connected to sensor modules which transmit information to a Network Interface Unit or Application Server. The Application Server, in turn, processes, analyses, interprets, and stores that information as well as receives input from the Operator at a Command and Control user Interface, typically a Perimeter Intrusion Detection System Integration Unit, or PIU, in existing installations.

3.2 System Capacity

.1 The MDS sub-system must provide a number of discrete perimeter sectors which will typically be between 2 and 25.

.2 The system must be of a modular design and it must be possible at a future date to add more sectors and associated sensor modules, processing and control equipment to the basic installed complement without replacing existing hardware.

.3 The MDS sub-system must provide the following capabilities at each sensor module:

.1 Relay outputs - 1 Form C, {One (1) Alarm A and B, Supervision and Fail};

.2 Auxiliary inputs - Two (2) supervised inputs;

.3 The ability to expose alarms, notifications and management of these inputs and outputs to the CCDA;

.4 USB Port.

3.3 Sensor Detection Field

.1 Buried Line sensors must detect and annunciate any disturbances in the electromagnetic field between the transmit cable and the receive cable as an intruder approaches a detection zone. Typically these sensors use Ported Coaxial Cables as the transmitter and receiver cables, but other cable configurations are acceptable.

.2 The detection pattern must be elliptical in shape, a minimum of one (1) metre and a maximum of one and a half (1.5) metres above the ground and two (3) metres to three (3) metres wide depending on cable spacing and soil composition.

.3 The detection pattern must also extend below the ground to a depth of least half (0.5) a metre.

.4 Once calibrated to the suppliers specifications, the sensor must not detect a person that is at least two (2) metres from the nearest sensor cable.

.5 System coverage must be limited to the detection zone. Potential targets outside the detection zone must not be detected by the system.

3.4 Sensor Sensitivity

.1 The sensor must detect an intruder weighing a certain mass attempting to walk, run, crawl or jump the detection zone. (The nominal mass of the intruder will be in excess of 35 kg.)

.2 The sensitivity of each segment of each sector of the sensor sub system must be adjustable from the sub-system Maintenance User Interface.

.3 Remote testing of each of sector of the sensor sub system must be provided as part of the system functionality and the ability to initiate, monitor and capture the results of sensor

testing must be provided through an open API or gateway to a higher level Command, Control and Data Acquisition system (CCDA).

3.5 Sensor Supervision

.1 The sensor cables will be continuously monitored and if they are cut at any point, a Tamper alarm will be generated.

.2 The sensor module enclosures will be equipped with tamper switches that must be continuously monitored and if the enclosures are opened, a Tamper alarm will be generated.

.3 The sensor modules that form the active components of the system will be continuously monitored and if they fail, a Fault alarm must be generated.

3.6 Dead Zones

.1 Any area of reduced or non-detection in accordance with section 3.1 with a width which is greater than 0.5 m must be identified as a dead zone.

.2 The accumulation of all areas of reduced detection or non-detection must be less than 0.5% of the total length of the system.

.3 Any accumulation of reduced detection or non-detection which is greater than the specified minimum, or any dead zone found in the system coverage during the 12 month period following system commissioning must be corrected at the contractor's expense.

3.7 Nuisance Alarms

.1 Nuisance Alarms are defined as those alarms which occur as a result of the detection of non valid target within the specified environmental conditions. Nuisance Alarms may be caused by:

.1 Changes in atmospheric conditions;
.2 Small animals (less than 45 kg);
.3 Ground/air vibration;
.4 Other observable causes (other than valid targets);
.5 Electrical or radio frequency interference;
.6 Personnel, structures, or vehicles outside the detection zone; and
.7 Alarms due to unknown causes but which cannot be classified as false alarms.

.2 Alarms caused by "Tests" are not classified as nuisance alarms.

.3 Within the specified environmental conditions, the system's nuisance alarm rate must not exceed:

.1 10 per 24 hour period;
.2 Monthly average of 0.60 alarms per day per sector; and/or
.3 7 alarms per sector in any one day.

.4 The contractor must state the expected nuisance alarm rate for this installation. This stated rate must form part of any resulting contract. Persistent nuisance alarm rates in excess of the stated number during the 12 month period following commissioning must necessitate corrective action

3.8 False Alarms

.1 False Alarms are defined as those alarms that are caused by phenomena internal to the sensor. Such phenomena may include intermittent faults and transients due to changes in

status of incoming power or may be related to the sensor's signal processing. The False Alarm Rate must not exceed one per sector per year for the entire system.

3.9 Tamper/Fault Alarms

.1 The MDS sensors must be self monitoring for short and open circuits, and must generate an appropriate alarm message that can be used to trigger a visual and audible sector alarm signal at the Operator User Interface when a sensor or associated interconnect circuit is shorted, cut, disconnected, or looses system power.

3.10 System Test

.1 It must be possible to remotely test the operational status of the sensor system from the Maintenance User Interface on receipt of a command that manually places a sector or group of sectors in a "test" mode.

3.11 System Failure

.1 A power failure within the sensor, malfunction of processing or related circuitry, a short or open of any sensor cable or signal cable must generate a Tamper alarm.

.2 A sub-system failure must be deemed to have occurred when any required motion detection is not produced or when any required control function cannot be performed.

3.12 Perimeter Sectors

.1 In order to provide prompt identification of the location of an attempted intrusion, the perimeter must be divided into multiple sectors. The overall number and layout of sectors must be arrived at by design review, subject to approval by the Design Authority.

3.13 Operational Alarm Notifications

.1 The MDS sub-system, must report the following operational alarms through an open API or gateway to a higher level Command, Control and Data Acquisition system (CCDA):

.1 Sensor alarm/reset;

3.14 Fault Alarm Notifications

.1 The MDS sub-system, must report the following fault alarms through an open API or gateway to a higher level Command, Control and Data Acquisition system (CCDA):

.1 Sensor fault;
.2 Sensor tamper;
.3 System fault;
.4 System Tamper;

3.15 Event Notifications

.1 Each MDS sub-system, must report the following report the following events through an open API or gateway to a higher level Command, Control and Data Acquisition system (CCDA) for data-logging purposes using a TCP/IP encapsulated version of the Starcom Protocol:

.1 All Operational alarms
.2 All fault alarms
.3 All tamper alarms
.4 All maintenance log in and log out actions

.5 All changes in user access parameters;

3.16 Report Generation

.1 The MDS sub-system application software must enable the generation of reports, at the Report Generation User Interface that provides the following data, where applicable:

.1 Alarm date and time, including sector number and any text descriptor associated with the alarm action, such as “mask”, “secure”, “fault”, tamper;
.2 Event date and time, including sector number and any text descriptor associated with the event status.

.2 The MDS sub-system application software must be able to:

.1 select a date and time range for all reports to a fifteen (15) minute or smaller resolution;
.2 print all reports;
.3 Save all reports as a file.

3.17 System Definition Deliverables and Parameters

.1 The Contractor must:

.1 include an open SDK for the display interface generation,
.2 provide an object model for each type of device that is managed by the MDS sub-system. This will allow the sensor device functionality, including both events and manageable parameters, to be accessed, normalised and exposed to the PIDS application or other applications that may eventually run on the platform,
.3 provide a copy of the database structure and schema,
.4 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.

4 PHYSICAL REQUIREMENTS

4.1 Equipment installed outdoors:

.1 The dimensions of the equipment must be application specific within the following limits:

.1 All outdoor fence mounted signal processing and distribution equipment must be housed in weatherproof, tamper-proof enclosures;

.2 Tamper devices must be provided inside all equipment boxes and enclosures with removable covers, housings or other accessible units to detect unauthorized opening or tampering.

.3 All outside enclosure penetrations must be from the bottom unless the system design requires penetrations from other directions.

.4 All outdoor mounted equipment must be housed in weatherproof enclosures equipped with tamper switches; and

.5 All covers required to be removed for maintenance must be secured by security screws.

4.2 Dimensions and packaging of equipment installed indoors:

.1 All equipment must be designed to mount in EIA standard rack mounts

.2 The maximum feasible amount of common control equipment (network interfaces, servers, maintenance user interfaces, etc.) must be located in the Common Equipment Room (CER) provided for the purpose.

.3 Computers supporting the Operator User Interface, if specified in the STR, must be also be located in the CER and made available to the Control Post using an appropriate extender.

.1 All computers, however they may be configured, or network interface units must be rack mounted and specified as industrial grade.

4.3 Floor Space

.1 The contractor must state in the Preliminary Design Report (PDR) the amount of floor space that will be required to house the electronic control and processing equipment.

4.4 Equipment Racks

.1 The contractor must provide all necessary racks to mount the network interface units or servers.

4.5 Wires, Cables, Conduits, Ducts

.1 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.

.2 All installation workmanship must be performed in accordance with ES/SOW-0102, and all applicable national, provincial, and local electrical codes.

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

.4 Conduits, cables, ducts, trays, etc. may be either Government Furnished Equipment (GFE) or supplied and installed by the contractor depending on the particular institution.

.5 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

4.6 Identification of equipment:

.1 Each item of equipment installed must:

.1 Have a permanently affixed label on the interior of the unit which identifies the manufacturer, and the model or assembly number;

.2 Have a permanently affixed label on the exterior of the unit which identifies the manufacturer, and the model or assembly number.

4.7 Sector Numbering

.1 MDS sectors must be installed and numbered sequentially from one (1) to the sector total, beginning beside the main gate of the institution, and continuing in sequence clockwise around the perimeter.

.2 The physical sector numbers will correspond to the numbered sectors on the perimeter map that will be displayed on the Operator User Interface.

.3 The contractor must supply and install robust, easily readable signs that indicate the beginning and end of each sector on the chain link fence unless otherwise indicated in the STR.

4.8 Safety

.1 All system electrically powered elements must meet the applicable Canadian Safety Association (CSA) standards

5 ENVIRONMENTAL REQUIREMENTS

5.1 Environmental limits

.1 The MDS must have a high Pd and low NAR over the following environmental conditions in any combination once the system has been calibrated and adapted to the terrain:

.1 Temperature: -40° C to 55° C (outdoor equipment);
0° C to 40° C (indoor equipment);

.2 Humidity: 0 to 100% non-condensing (outdoor equipment);
20 to 95% non-condensing (indoor equipment);

.3 Ground frost or freezing conditions;

.4 Rainfall up to 25 mm/hour;

.5 Hail stones up to 2 cm in diameter;

.6 Temperature changes causing quick ground freezing or thawing conditions;

.7 Sunrise/Sunset;

.8 Fog;

.9 Snowfall up to 30 cm/hour;

.10 Sandstorms;

.11 Seismic Vibrations;

.12 Acoustic or magnetic disturbances;

.13 Snow accumulation up to 50 cm;

.14 Lightning strikes outside a radius of 1 km; and

.15 Any site-specific phenomena as may be expected and/or published in other documents.

5.2 Interference

.1 Performance of the system must not be affected by the use of standard electronic equipment used at the institution. Distance limits of standard electronic equipment must be in accordance with the interference limitations defined in ES/SOW-0101, Statement of Work, unless modified by the following distance limitations.

.1 5 watt CB transceiver at 1 metre or more;

.2 6 watt VHF and UHF transceivers at 1 metre or more;

.3 25 mW 420-430 MHz Personal Portable Transmitters at 1 metre or more;

.4 Other radio frequency transmitting, receiving, and distribution equipment at 5 metres or more;

.5 Computer work stations at 5 metres or more;

5.3 Reliability

.1 All MDS components must have an MTBF of at least 5 years.

5.4 Safety

.1 All system electrically powered elements must meet the applicable Canadian Safety Association (CSA) standards.

.2 All components must meet IEC 60950-1 or the CSA equivalent.

6 INTERFACE REQUIREMENTS

6.1 Connectivity

.1 All MDS sub-system cabling must be secured against tampering and improper eavesdropping in metal conduit where installed in inmate accessible or exposed locations.

.2 The MDS sub-system network interface units or servers must:

.1 Interface over IPV4 TCP/IP to the CCDA or higher level system;

.2 Interface to legacy Senstar PIDS PIU and FAAS FIU systems for system management, alarm reporting and event logging using the Starcom protocol as described in ES/SPEC-0005;

.3 Be able to operate on 100Base-TX (IEEE 802.3u);

.4 Connect using an RJ-45 connector to the CCDA or to a higher level system;

.5 provide a published or standard protocol for communications between all TCP/IP managed devices and the MDS sub-system, preferably based on existing network standards such as SNMP.

.3 The MDS sub-system must be able to accept time settings from a Network Time Protocol (NTP) server.

.4 Sensor communications

.1 The MDS sub-system sensors must communicate with the network interface at two distinct points.

.2 Connect to the MDS sub-system sensor network using rugged, moisture proof connectors that are fit for purpose.

.3 Failure of one data line will not cause the system to fail, i.e. the communications must be fully redundant.

6.2 Sensor Module Integration and Power capabilities

.1 All MDS sub-system cabling must be secured against tampering and improper eavesdropping in metal conduit where installed in inmate accessible or exposed locations.

6.3 Sensor Module capabilities

.1 Each MDS sub-system module must be capable of providing the following relay outputs:

.1 Alarm A, Alarm B, Supervision, Fail

.2 Form C, 1.0 A 30 VDC max

.3 Expandable with relay output card

.2 Each MDS sub-system module must be capable of providing the following auxiliary inputs:

.1 2 supervised inputs

.2 Expandable with universal input card

.3 Each MDS sub-system module must be capable of providing the following port type:

.1 USB port

6.4 Cabling and Equipment Supervision

.1 Wiring must be supervised in all system modes. An alarm must occur if any sensor or sub-system cabling is cut or shorted to other wires or if the system devices are tampered with by unauthorized people or environmental conditions.

6.5 Power

.1 The MDS sub-system must be powered from standard commercial VAC power, supplied from the UPS in the CER, within the following range:

.1 Voltage: 120 VAC ±10%;
.2 Frequency: 60 Hz ±1.5%
.3 Power: not to exceed 100 watts; Following any power failure, the system must return to the operating mode which it was in use prior to the power failure.
.4 Transients: power fluctuations up to five times nominal voltages for up to 100 msec durations must not cause damage to the unit.
.5 Loss or restoration of primary power to the MDS sub-system must not produce spurious alarms or events to the data logger.
.6 When power is restored after a power failure, the system must resume normal operation without operator or maintenance staff action.

.2 Sensor Power/Redundancy

.1 The MDS sub-system sensor cables must be powered from two independent power supplies connected to the system at two distinct points.
.2 Failure of a single supply must not cause the system to fail, i.e. either power supply can power the entire system.

.3 Back Up Power

.1 The contractor must identify any built in or optional power failure protection available with the equipment.

.4 All MDS sub-system equipment , including Network Interface Units, must be connected to a UPS capable of supporting a minimum of one hour of operation.

6.6 User Interfaces

.1 Operator User Interface

.1 If specified in the STR, 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 SMSS, including the visual and audible parameters that the operator will respond to and use to interact with the system.
.2 The Operator User Interface must be capable of displaying all instructions in both English and French.
.3 The Operator User Interface must accept an input to toggle between languages, or display both simultaneously.

.2 Administrative User Interface

.1 An Administrative User Interface on a Display equipped with a keyboard and a pointing device that provides the Regional Technical Authority with the ability to add or delete system users and to assign them system privileges.

.3 Configuration User Interface

.1 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 MDS sub-system, including the sensor

calibration and testing and the creation of screen layouts, maps, positioning of devices etc if the STR calls for an Operator User Interface.

.4 Maintenance User Interface

.1 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 MDS sub-system.

.2 The Maintenance User Interface will allow access to all configure all of the functionality associated with the other User Interfaces, except for the Administrative User Interface.

.5 Report Development User Interface

.1 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 database and to run preconfigured reports from the database using a report generation menu or to develop and run custom reports using report generator such as Crystal Reports.

7 INSTALLATION REQUIREMENTS

7.1 Perimeter Signal & Power Cables

.1 Where needed, signal distribution cables for the MDS sub-system must be mounted at or near the top of the inner perimeter fence.

.2 All cable runs from the top of the fence to sensors, pull boxes, etc. must be carried in rigid steel conduit and buried where it leaves the fence.

.3 If power is required on the perimeter for the MDS sub-system, the power cables must be buried or run in rigid steel conduit along the top of the outer perimeter fence.

.4 All cables run from the perimeter to the common equipment room and/or Main Communication & Control Post (MCCP) must be carried in buried conduits.

.5 Connectors provided on the ends of any cable must mate with the corresponding connector on the equipment.

.6 Adapters from one type of connector to another are not acceptable.

7.2 Sector Calibration

.1 The MDS sub-system must provide the capability for the sensitivity of each threshold to be calibrated on a sector by sector basis from the Maintenance User Interface.

.2 The contractor must state the following requirements in the technical proposal:

.1 Number of personnel to complete the adjustments;

.2 Special calibration equipment (if required); and

.3 Length of time to adjust each sector's threshold.

7.3 Sector Alignment

.1 A preferred sector may be made up of more than one MDS sub-system sector; however, the original boundaries must be maintained in order to coordinate with the FDS and CCTV subsystem.

.2 A suggested sector layout will be provided in the site-specific documentation.

7.4 Installation Procedures

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

.2 The installed system must not impede the free movement of service vehicles (for snow removal, weed control, etc.) between the perimeter fences.

.3 Cables pull boxes, distribution panels and all exposed equipment must be secured against tamper and inmate attack. Steel enclosures must be used throughout the installation, either locked or secured with a maximum of two (2) screws.

.4 Cables, pull boxes, distribution panels and all exposed equipment must be protected from damage due to lightning.

.5 Appropriate steps must be taken to ensure the protection of any buried cable against damage, including that which may be caused by the surrounding media. Action should also be taken to contain, on a long term basis, any protective media immediately surrounding the cable in question.

.6 Where necessary, appropriate steps must be taken to provide adequate drainage between the fences in order to ensure no loss of detection capability.

8 QUALITY ASSURANCE REQUIREMENTS

8.1 General

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

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

8.2 System Check Out

.1 The MDS sub-system contractor must provide, as a minimum, the following System Check Out Test results to the Design Authority prior to the scheduling of the on-site acceptance tests:

.1 Sensitivity profile of each MDS sector.

.2 Normal walk around the perimeter, the centre point of the detection zone.

.3 Normal walk crossings of the detection zone at four (4) foot intervals in each MDS sector.

.4 Two (2) normal walks around the perimeter & between the fences:

- Along the inner perimeter fence
- Along the outer perimeter fence which will indicate the system's detection zone is contained within the fences.

.5 Vehicle drive around the perimeter as close as possible to the outer perimeter fence, further indicating the containment of the detection zone.

8.3 Acceptance Test Procedures (ATP)

.1 The Design Authority will determine the appropriate number of locations to perform the special crossing tests. The Design Authority will perform the "slow walk" crossing first, which will identify the approximate location of the detection zone boundary.

.2 All special crossings performed during the on-site ATP must be detected before the Design Authority can approve this section of the acceptance tests. The human/vehicle containment tests will be repeated during the on-site ATP.

.3 If any MDS sub system sector requires the physical relocation of sensor equipment or the adjustment of detection thresholds due to failed on site tests, the System Check Out tests must be repeated for the failed sector(s).

9 DELIVERY REQUIREMENTS

9.1 Documentation

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

9.2 Support

.1 The MDS sub-system maintenance and spares support must be provided in accordance with the ES/SOW-0101, Statement of Work.

9.3 Training

.1 Operator training and maintenance training for the MDS sub-system must be in accordance with the ES/SOW-0101, Statement of Work.

9.4 Hand Over

.1 Following System Acceptance and the delivery of Documentation, Spares, as required, and Training, the contractor will supply a Hand Over Report.

.2 A sample of a Hand Over report is provided in Annex A.