CORRECTIONAL SERVICES CANADA
TECHNICAL SERVICES BRANCH
ELECTRONIC SECURITY SYSTEMS

ES/ SPEC -0404
Revision 4
2017 March 16

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

----------THIS PAGE INTENTIONALLY LEFT BLANK----------

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 System
FAR	False Alarm Rate
FDS	Fence Disturbance System
GFE	Government Furnished Equipment
MCCP	Main Communications and Control Post
MDS	Motion Detection System
NAR	Nuisance Alarm Rate
NTP	Network Time Protocol
PIDS	Perimeter Intrusion Detection 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 System (MDS) for federal correctional institutions.

.2 This system is one of a number of subordinate systems, or sub-systems, of the Perimeter Intrusion Detection Systems (PIDS) installed at many Federal Institutions and will share a Common User Interface with the Fence Disturbance Sensor System (FDS), the PIDS Public Address system and the PIDS CCTV system.

.3 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.

.4 These RF signals must form an invisible electromagnetic detection field around the sensor cables that can be used to locate and detect an intruder passing through the field.

.5 The MDS system typically:

.1 includes sensor cables buried below ground between the fences around its perimeter divided into discrete sectors,

.2 includes sensor modules that:

- generate, transmit, receive and process RF signals to and from the sensor cables,
- are connected to the cables, which in turn transmit information to an Application Server or Gateway via an Interface Unit,

.3 generates RF signals that form an electromagnetic field that, when disrupted, detects conductive materials (e.g. people) above them,

.4 includes an Application Server which 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.

.6 The sensor must be configurable into discrete detection sectors or zones that can be between ten (10) metres long and one hundred and fifty (150) metres long.

.7 The sensor must support perimeters up to and including two thousand (2,000) metres in length.

.8 The MDS system must:

.1 consist of either:

- two or more parallel, terrain following, Sensor cables that are buried in the ground between the perimeter fences and that can be configured into discrete detection sectors and calibration sub-sectors by hardware or software means.
- Power and Data signals may also be carried in the same physical cable or provided over separate, supervised cable(s) external to the Sensor cables

.2 support perimeters up to and including two thousand (2,000) metres in length.

.3 Detect, but not necessarily display the position of intruders weighing more than 35 kgs to within +/- 1 meter with a 95% confidence factor,

.4 be supplied with two or more discrete **sensor modules** that transmit and receive the signals in the cables as well as process the signal changes generated in the cables by the presence of an intruder; subsequently providing sensor performance and alarm data to an **Network Interface (NI)**, **Gateway**.

.5 be supplied with an **Network Interface (NI)**, **Gateway** that provides both power and data communications to the sensor network using a standards based and published protocol, to a Command, Control and Data Acquisition (CCDA) platform or on a system server that is connected to the Command, Control and Data Acquisition (CCDA) platform.

.6 be supplied with **MDS application** software that runs on the Command, Control and Data Acquisition (CCDA) platform or on a 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.

.7 If specified in the STR, be supplied with **a PIDS MDS 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 system and provide the Operator User Interface.

.8 If specified in the STR, be supplied with a **Perimeter Intrusion Detection System Integration Unit** operating as an instance of the CCDA, unless specified in the STR.

.9 User Interfaces must include:

.1 If specified in the STR, an Operator User Interface provided by the Perimeter Intrusion Detection System Integration Unit 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.

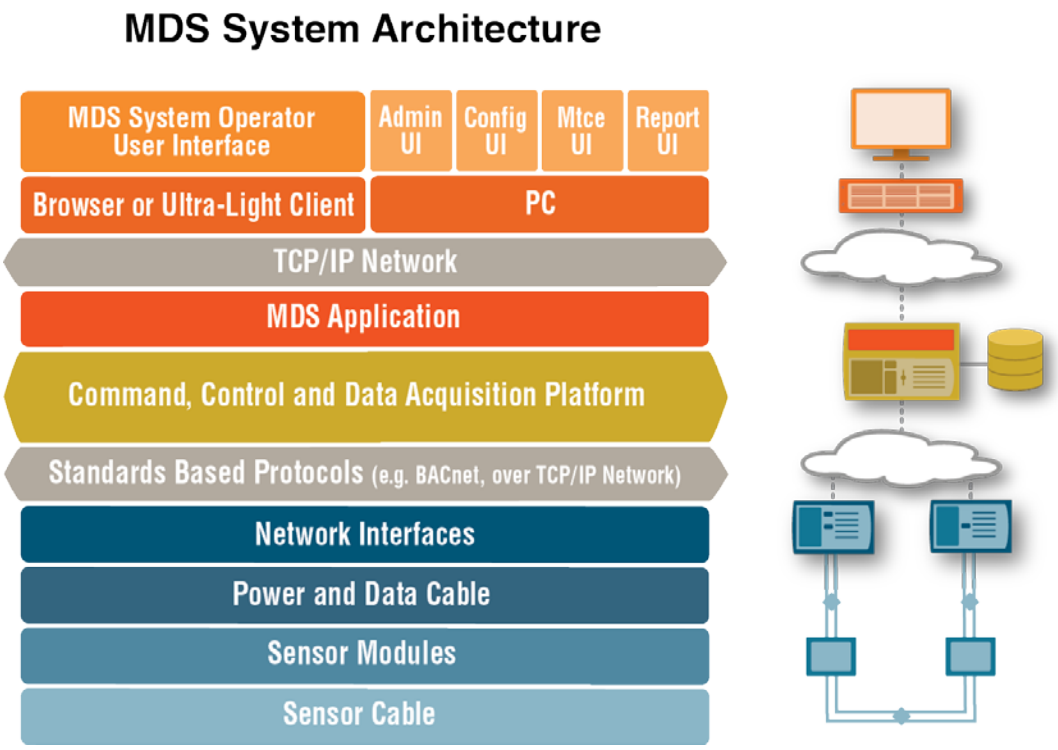
.3 A Report Development and Generation User Interface.

.4 A Configuration User Interface.

.5 A Maintenance and Training User Interface.

Note: The User Interfaces can be instances of an application running on a common workstation.

1.2 Typical MDS System Architecture



1.3 Purpose

.1 The primary purpose of a Motion Detection System is to detect attempts by an intruder to penetrate a perimeter around a Correctional facility in real time.

.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.

.3 In order to be “fit for purpose”, the MDS must:

- .1 operate in an outdoor environment,
- .2 perform reliably in all weather conditions,
- .3 integrate with the PIDS system,
- .4 detect moving intruders that have a significant electromagnetic cross-section (e.g., humans, vehicles, and other large conductive objects) while rejecting other environmental stimuli (e.g., birds, small animals, weather),
- .5 have a high probability of detection (Pd) rate for all intrusion attempts, 99% with a 95% confidence factor,
- .6 detect human intruders who walk, crawl, roll, jump, or run through the detection field,
- .7 have a low nuisance alarm rate (NAR) for fence vibration and stress caused by birds and natural phenomena such as wind, rain, and snow.
- .8 be suitable for deployment in any institution equipped with a single or double perimeter fence that meets the tension and panel configuration requirements for the deployment of a fence mounted sensor on a twelve (12) foot chain link fence with top, middle and bottom rails, topped with concertina razor wire.

1.4 Commercial Off-The-Shelf Equipment

.1 The MDS must use commercial off-the-shelf (COTS) equipment and proven designs to the maximum extent possible.

.2 The MDS may incorporate new technology which must be compatible with the Command and Control environment of the Institution at which it will be installed.

.3 Any new MDS technology proposed may be subject to evaluation by CSC to ensure that is technically acceptable following the steps defined in section 1.4.

1.5 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.

.3 Electronic security systems operating in this unique environment must maintain very high standards of dependability and reliability.

.4 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.

.5 The MDS sub-systems must comply with the relevant CSC specifications and standards in order to be technically acceptable.

.6 CSC may, when it deems necessary

.1 require both systems and sub-systems to be evaluated and accepted in accordance with the applicable CSC specifications

.2 request the supplier to arrange for a full factory or site demonstration.

.3 verify in depth any of the system technical specifications called up.

.4 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.

1.6 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 specifications or standards not prepared by Canada 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 in this specification.

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-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 Serve
EIA-310	Electronic Industry Association Standard for Racks, Panels and Associated Equipment
IEC EN55024	International Electrotechnical Commission Information technology equipment immunity characteristics – Limits and methods of measurement
IEC EN60529	International Electrotechnical Commission International Protection Marking

3 OPERATIONAL REQUIREMENTS

3.1 General

.1 The MDS must consist of the following components:

.1 In any of the following configurations:

- two or more parallel, terrain following, **common sensor, power and data cables** that are buried in the ground between the perimeter fences connected directly or indirectly to a network interface or gateway,
- two or more parallel, terrain following **sensor and power cables** that are buried in the ground, supported by **separate data cables**, between the perimeter fences connected directly or indirectly to a network interface or gateway,
- two or more parallel, terrain following **sensor and data cables** that are buried in the ground, supported by **separate power cables**, between the perimeter fences connected directly or indirectly to a network interface or gateway, or
- two or more parallel, terrain following **sensor cables** that are buried in the ground, supported by **separate power and data cables**, between the perimeter fences connected directly or indirectly to a network interface or gateway that can:
  - provide coverage of perimeters up to and including two thousand (2,000) metres in length,
  - be configurable into discrete detection sectors that can be between ten (10) metres and one hundred and fifty (150) metres long,
  - be further configurable by hardware or software means into discrete detection sub-sectors within each sector that can be between ten (10) metres and one hundred and fifty (150) metres long.
  - be configurable from non-contiguous sub-sectors.

.2 two or more **sensor modules** that typically:

- transmit, receive and process signals from attached sensor cables,
- communicate with the network interfaces over the redundant common or separate data cables,
- obtain power from the power cable provided over the common or separate power cables.

.3 Two or more **network interfaces** or **gateways,** each of which can:

- provide power to any sensor modules attached to the sensor cables,
- support data communications to the sensor network,
- provide an interface, using a standards based and published protocol, to a Command, Control and Data Acquisition (CCDA) platform or to a standalone Display and Control System
- provide visibility of the events monitored by the sensors to the CCDA,
- support the control of the manageable attributes of the sensors from the CCDA.

.4 **MDS application software** that runs on the Command, Control and Data Acquisition (CCDA) platform or on a server that is connected to the Command, Control and Data Acquisition (CCDA) platform, that provides the necessary software functionality to enable the FDS system to:

- process,
- analyse,

- interpret, and
- store information from the NIUs or Gateways,
- receive input from the Operator at a Command and Control user Interface, typically a Perimeter Intrusion Detection System Integration Unit, or PIU, in existing installations or User Interface Application Software running on a CCDA platform in future systems.

.5 the **MDS application software** also provides the necessary software functionality and User Interfaces to enable the MDS system to be:

- configured,
- administered,
- maintained, and
- accessed for reporting services

through individual, function specific, User Interfaces.

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

.2 **MDS User Interface application software** that runs on a stand-alone Display and Control System that that provides the necessary software functionality and User Interface to manage the MDS sensor sub-system, detect alarm and event notifications from the sensor system and provide the Operator User Interface, unless specified in the STR.

3.2 System Flexibility and Extensibility

.1 The MDS must meet the following design requirements:

.1 be of a modular design,
.2 be sufficiently flexible to allow the overall number and layout of sectors to be arrived at by design review, subject to approval by the Design Authority,
.3 be extensible such that at a future date, more sectors and associated sensor modules, processing and control equipment may be added to the installed system and configured appropriately without replacing existing sensor modules, interface units or server hardware.

.2 The MDS sensor module must support the input/output flexibility defined in section 6.3.

3.3 Sensor Sensitivity and Calibration

.1 The MDS sensors must:

.1 detect and annunciate any disturbances in the electromagnetic field between the transmit cable and the receive cable as an intruder approaches a detection zone,
.2 provide a detection pattern that is elliptical in shape, a minimum of one (1) metre and a maximum of one and a half (1.5) metres above the ground and between two (2) metres to three (3) metres wide depending on cable spacing and soil composition,
.3 provide a detection pattern that also extends below the ground to a depth of least half (0.5) a metre,
.4 limit system coverage to the detection zone,

.5 not detect potential targets outside the detection zone.
.6 not detect a person weighing more than 35 kg that is at least two (2) metres from the nearest sensor cable once calibrated to the suppliers specifications,
.7 detect an intruder, weighing 35 kg or more, attempting to walk, run, crawl or jump the detection zone. (The nominal mass of the intruder will be in excess of 35 kg.)
.8 provide the capability to remotely test each sector of the MDS,
.9 provide the ability to remotely calibrate the system by adjusting the sensitivity of the sensor sectors in three (3) to ten (10) metre increments by directly connecting to the Sensor Modules and remotely from the Maintenance User Interface.
.10 provide the ability to adjust the sensitivity of each sub-sector of each detection sector of the MDS by directly connecting to the Sensor Modules and remotely from the Maintenance User Interface.
.11 support the ability to initiate, monitor and capture the results of sensor testing through an open API or gateway to a higher level Command, Control and Data Acquisition system (CCDA).

.2 The MDS sensors may:

.1 use Ported Coaxial Cables as the transmitter and receiver cables, but other cable configurations are acceptable as long as the detection specifications are maintained.

3.4 Supervision

.1 The MDS must be continuously monitored

.1 such that if the sensor, power or data cables are cut at any point, a Tamper Alarm is generated and annunciated at the operator user interface,
.2 using tamper devices such that if sensor modules or equipment boxes and enclosures with removable covers, housings or other accessible areas are opened or tampered without prior authorisation, a Tamper Alarm is generated and annunciated at the operator user interface,
.3 such that if a Sensor Module is opened or damaged, a Tamper or Fault Alarm must be generated and annunciated at the operator user interface,
.4 such that the failure of an active component of the system causes a Fault Alarm to be generated and annunciated at the operator user interface
.5 such that if the power supply to the sensor modules that form the active components of the system varies out of its specified operational range, a Power Fail alarm must be generated and annunciated at the user interface.

3.5 Probability of Detection

.1 The MDS system must provide continuous coverage that will support the detection of a living entity weighing more than 35 kg in a specified detection zone with a statistical probability of (Pd) of 98% at a confidence level of 95%.

3.6 Elimination of Dead Zones

.1 Should the MDS demonstrate an area of reduced or non-detection in accordance with section 3.3 with a width which is greater than 0.5 m during testing, this must be identified as

a dead zone and remedial measures must be taken to ensure the system meets its performance targets.

.2 The MDS must demonstrate the accumulation of all areas of reduced detection or non-detection is be less than 0.5% of the total length of the system in order to meet acceptable performance requirements.

.3 Should the MDS demonstrate an accumulation of reduced detection or non-detection which is greater than the specified minimum, or if any dead zone is found in the system coverage during the 12 month period following system commissioning, the detection levels 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.

.2 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.

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

.4 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 seven (7) alarms per sector in any one day.

3.8 False Alarms

.1 MDS False Alarms are defined as those alarms that are caused by phenomena internal to the sensor.

.2 False Alarms may include intermittent faults and transients due to changes in status of incoming power or may be related to the sensor's signal processing or communications.

.3 The False Alarm Rate must not exceed one per sector per 6 (six) months for the entire system.

.4 A 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.

3.9 `Operational Alarm Notifications

.1 The MDS 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;

3.10 Fault Alarm Notifications

.1 The MDS must report all:

.1 sensor disturbance alarms,
.2 sensor or device tamper alarms,
.3 sensor or device fault alarms including cuts, short circuits and disconnections,
.4 system and power failure alarms

using the TCP/IP encapsulated version of the Starcom Protocol, “Starcom over IP”.

3.11 Event Notifications

.1 The MDS must log all:

.1 sensor disturbance alarms,
.2 sensor or device tamper alarms,
.3 sensor or device fault alarms including cuts, short circuits and disconnections,
.4 system and power failure alarms
.5 log in and log out actions at all User Interfaces except the Operator User Interface, if equipped, and
.6 configuration change notifications,

to the CCDA using the TCP/IP encapsulated version of the Starcom Protocol.

3.12 System Definition Deliverables and Parameters

.1 The MDS deliverables must include:

.1 an open SDK for the display interface generation,
.2 a published object model for each type of device that is managed by the sub-system,
.3 a copy of the database structure and schema(s), and
.4 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 configuration of the equipment must be application specific within the following limits:

.1 All outdoor fence or post 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 The MDS system equipment installed indoors must meet the following criteria:

.1 all equipment must be designed to mount in EIA standard rack mounts, (Note: Desktop computers in rack mounts will not be acceptable.)

.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 extended to the MCCP using an appropriate extender and must:

- be equipped with a folding screen that occupies no more than one Rack Unit,
- have a minimum display resolution of at least 1920 X 1080,
- include a touchpad integrated into the keyboard.

.4 where specified in the STR, the Administrative, Maintenance and Configuration User Interfaces may share an existing Touch Screen User Interface through the use of KVM that accepts a minimum of eight (8) inputs and supports video display of at least 1920 X 1080 pixels at 60 fps.

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 Unless specified in the STR, the MDS must be equipped with all necessary racks to mount all indoor mounted equipment such as network interface units or servers.

4.5 Wires, Cables, Conduits, Ducts

.1 The MDS must be supplied with 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 The MDS installation must be performed in accordance with ES/SOW-0102, and all applicable national, provincial, and local electrical codes.

.3 The MDS must include a wiring diagram in the Installation section of the Maintenance Manual to detail where connections terminate and how wires are routed and terminated.

.4 The MDS may include conduits, cables, ducts, trays, etc. that are supplied and installed as either Government Furnished Equipment (GFE) or by the contractor depending on the particular institution, details to be included in the STR.

.5 The MDS must ensure that connectors on the ends of any cable 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 MDS equipment installed must:

.1 be equipped with a machine printed label permanently affixed to the interior of the unit which identifies the manufacturer, and the model or assembly number;

.2 be equipped with a machine printed label permanently affixed to the exterior of the unit which identifies the manufacturer, and the model or assembly number.

4.7 Sector Numbering

.1 The MDS sectors at the Perimeter fence must be supplied such that:

.1 they are aligned with existing sensor zones,

.2 sensor cable sectors will be 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,

.3 sector numbers will correspond to the numbered sectors on the perimeter, and

.4 robust, easily readable signs indicating the beginning and end of each sector installed on the chain link fence are installed unless otherwise indicated in the applicable STR or SOW.

4.8 Safety

.1 All system electrically powered elements must meet the applicable IEC 60950-01 or CS equivalent standard.

5 ENVIRONMENTAL REQUIREMENTS

5.1 Environmental limits

.1 The MDS must have a high Pd, as defined in section 3.5, 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 The performance of the MDS must not be affected by the use of standard electronic equipment deployed at an institution.

.2 All components of the MDS must be certified to be complaint with IEC EN 55024 immunity characteristics.

5.3 Reliability

.1 All MDS components must have an MTBF of at least 100,000 hrs.

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 The MDS components including NIUs, Gateways or equivalent and servers must:

.1 be equipped with interfaces over IPV4 TCP/IP to the CCDA or higher level system,
.2 be equipped with interfaces to legacy Senstar PIDS PIU and FAAS FIU systems for system management, alarm reporting and event logging using the Starcom over IP protocol as described in Appendix B when identified in the Statement of Technical Requirements,
.3 be able to operate on 100Base-TX (IEEE 802.3u);
.4 connect using an RJ-45 connectors 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, preferably based on existing network standards such as SNMP.

.2 The MDS must be able to accept time settings from a Network Time Protocol (NTP) server.
.3 The MDS must be configured such that:

.1 the sensors must communicate with the NIUs at two distinct points,
.2 the outdoor sensor elements use rugged, moisture proof connectors that are fit for purpose.
.3 failure of one data cable 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 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 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 module must be capable of providing the following auxiliary inputs:

.1 2 supervised inputs
.2 Expandable with universal input card

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

.1 USB port or RS 232 connector for direct management of the Sensor Module

.4 The MDS System must have the ability to expose alarms, notifications and management of these inputs and outputs to the MDS Application software and MDS User Interface,

6.4 Power

.1 The MDS must be powered from standard commercial VAC power, supplied from the UPS in the CER, provided as Government Furnished Equipment unless specified in the STR, within the following range:

.1 voltage: 120 VAC ±10%;
.2 frequency: 60 Hz ±1.5%
.3 power: not to exceed 100 watts;
.4 support: it is expected that the GFE UPS will support the system in operation for a minimum of one (1) hour.
.5 power failure: following any power failure, the system must return to the operating mode that it was in prior to the power failure.
.6 transients: power fluctuations up to five times nominal voltages for up to 100 msec durations must not cause damage to the unit.

.2 The MDS must:

.1 not produce spurious alarms or events on loss or restoration of primary power
.2 resume normal operation without operator or maintenance staff action when power is restored after a power failure.

.3 Sensor Power/Redundancy

.1 The MDS 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.

.4 All MDS equipment, including Network Interfaces, must be connected to a UPS capable of supporting a minimum of one hour of operation.

6.5 User Interfaces

.1 The MDS Operator User Interface must meet the following requirements:

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

.2 The MDS Administrative User Interface must meet the following requirements:

.1 be equipped with 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 any or all system users and to assign them system privileges must be provided.
.2 access to the Administrative User Interface must be password controlled,

.3 The MDS Configuration User Interface must meet the following requirements:

.1 be equipped with 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 FDS, including:

- add or remove sensor modules,
- create, modify or delete sensor lengths and configurations,
- sensor calibration,
- sensor testing,
- creation of screen layouts, maps, positioning of devices etc. must be provided.

.2 access to the Configuration User Interface must be password controlled,

.4 The MDS Maintenance User Interface must meet the following requirements:

.1 be equipped with 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 must be provided, including, but not limited to:

- sensor calibration,
- sensor testing.

.2 the Maintenance User Interface must allow an authorised user with access to all of the functionality associated with the other User Interfaces, except for the Administrative User Interface.

.3 access to the Maintenance User Interface must be password controlled,

.5 MDS Report Development User Interface must meet the following requirements:

.1 be equipped with 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 must be provided.

.2 provide reports as a minimum that include:

- Sector Detail
- Sector Summary
- Sector Edit

.3 provide report headers that include:

- the name of the institution
- the name of the report
- the date of the report
- headers for all columns

.4 select report types and criteria through the use of a mouse alone,

.5 present all reports on the User Interface,

.6 provide the report data in either a pdf form or a “csv” text form for export to another application from which the data may be printed following further formatting if required as no “local” printing capability will be available or required in the CER.

.7 provide Sector Detail reports with:
- a resolution of one (1) day
- the ability to select any individual, group or all sectors

.8 provide Sector Detail reports with, sorted in ascending start time order:
- Sector Number
- Event Type
- Event Time with a one (1) second resolution and using a 24 hour clock format

.9 provide Sector Detail events including:
- Sector alarms, acknowledgements and cancellations
- Sensor module alarms, acknowledgements and cancellations,
- Tamper alarms, acknowledgements and cancellations
- Sector mask, secure (unmask) and test, (including results)
- System alarms, acknowledgements and cancellations

.10 provide Sector Summary reports with:
- a resolution of one (1) day

.11 provide Sector Summary reports, sorted in ascending order by sector number:
- Sector number
- Alarm count
- Length of time in alarm state with one (1) second resolution
- Mask count
- Length of time in mask state with one (1) second resolution
- Fault Count
- Length of time in fault state with one (1) second resolution

.12 provide Sector Summary reports with system fault alarms and duration with one (1) second resolution.

.13 provide Sector Edit report inputs with:
- a time range with one (1) day resolution

.14 provide Sector Edit reports with inputs, sorted in ascending order by sector number:
- Sensor Module
- Modification of System Configuration
- The Date and Time on which the modification was made with one (1) second resolution on a twenty four hour clock

.15 make the Sector Edit report available at the Configuration User Interface only:

.16 provide a Sector reports which does not require inputs.

.17 provide Sector Summary reports, sorted in ascending by sensor module and sector number:
- Sensor module number
- Sectors on Sensor Module with sub-sectors
- Additional configured sensor inputs, if any
- Additional configured sensor outputs, if any

.18 Sample report layouts must be provided as part of the PDR and will be reviewed and approved by the Design Authority.

7 INSTALLATION REQUIREMENTS

7.1 Perimeter Signal & Power Cables

.1 Where needed, the MDS signal and power distribution cables:

.1 must be mounted at or near the top of the outer perimeter fence, other than sensor cables, where required,

.2 must be carried in rigid steel conduit and buried where they leave the fence AND run from the top of the fence to the sensors, pull boxes, etc.

.3 carrying power, if required on the perimeter, must be provided by buried cables or cables that are run in rigid steel conduit or enclosed cable trays along the top of the outer perimeter fence or integrated into the communications cables e.g. POE,

.4 must be carried in buried conduits where they run from the perimeter to the Common Equipment Room (CER) and/or Main Communication & Control Post (MCCP),

.5 must be equipped with cables for which the connectors supplied on the ends of any cable mate with the corresponding connector on the equipment, and

.6 must not be supplied with cables with adapters from one type of connector to another.

7.2 Sector Calibration

.1 The MDS 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 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.

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 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 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 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.

---------- End of Text ----------