Correctional Service Canada
Technical Services Branch
Electronics Systems

ES/SPEC-0401
Revision 2
November 2001

ELECTRONICS ENGINEERING SPECIFICATION

PERIMETER INTRUSION DETECTION SYSTEM INTEGRATION UNIT FOR USE IN FEDERAL CORRECTIONAL INSTITUTIONS

AUTHORITY

This Specification is approved by the Correctional Service of Canada for the procurement and installation of a stand-alone Perimeter Intrusion Detection System (PIDS) Integration Unit in Canadian federal correctional institutions.

Recommended corrections, additions or deletions should be addressed to the Design Authority at the following address: Director, Engineering Services, Correctional Service of Canada, 340 Laurier Avenue West, Ottawa, Ontario, K1A 0P9

Prepared by:

Manager,
Electronics Systems Research

Approved by:

Director,
Engineering Services

TABLE OF CONTENTS

ABBREVIATIONS

The following abbreviations are used in this specification:

CCTV	Closed Circuit Television
CER	Communications Equipment Room
COTS	Commercial-Off-The- Shelf
CSA	Canadian Standards Association
CSC	Correctional Service Canada
DES	Director Engineering Services
EIA	Electronic Industries Association
FAAS	Facility Alarm Annunciation System
FDS	Fence Disturbance Detection System
GFE	Government Furnished Equipment
MCCP	Main Communications and Control Post
MDS	Motion Detection System
PA	Public Address
PIDS	Perimeter Intrusion Detection System
PIU	PIDS Integration Unit
RFP	Request for Proposal
SIDS	Supplementary Intrusion Detection System
SOW	Statement of Work
STR	Statement of Technical Requirements
UPS	Uninterruptable Power Supply
VDU	Video Display Unit

DEFINITIONS

The following definitions are used in this specification:

Design Authority	Director, Engineering Services (DES) - Correctional Service 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.

1.0 INTRODUCTION

This specification defines the design, technical and performance requirements for a stand-alone Perimeter Intrusion Detection System Integration Unit (PIU). It will normally be specified when only the PIU portion of the MCCP Integration Console requires upgrading or replacement.

The PIU is the central controller and supporting infrastructure between the operator and the Perimeter Intrusion Detection System (PIDS) subsystems. The PIU shall incorporate hardware and software necessary to perform status monitoring, alarm processing and display and control over the subsystems.

The contractor shall be responsible for integrating all subsystems and shall provide all material and labour required for the design, supply, delivery, installation, testing and commissioning of the PIU. The contractor shall provide documentation and training to the extent described in this and other identified specifications.

Subsystems to be integrated into the PIU will be identified in the Statement of Technical Requirements (STR) and may include some or all of the following:

a. Motion Detection System (MDS);

b. Fence Disturbance System (FDS);

c. PIDS Closed Circuit Television (CCTV);

d. Supplementary Intrusion Detection System (SIDS);

e. Uninterruptable Power Supply (UPS); and

f. PIDS Public Address (PA) System.

1.1 Commercial-Off-The-Self Equipment

The system shall use commercial off-the-shelf (COTS) equipment and proven designs to the maximum extent possible. All new equipment shall meet the specified lifespan requirements. New equipment designs shall be restricted to unique interfaces and common control console.

1.2 Technical Acceptability

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. 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 shall maintain very high standards of dependability and reliability.

The CSC 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.

The technical acceptance process shall involve system and subsystem evaluation in accordance with the applicable CSC specifications in one of CSC facilities or may be tested in a CSC facility to verify the effectiveness of the proposed technologies when subjected to the restrictive operational environment.

CSC shall also verify in depth any of the system technical specifications called up. CSC may when it deems necessary, request the supplier to arrange for a full site demonstration. 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.

It is the supplier's responsibility to make new developments in products available to CSC for evaluation. Equipment qualification is an ongoing process and can be initiated at any time by a vendor. Any vendor can have access to the CSC specifications and standards. Any new development or products should be submitted to the CSC Engineering Services Division, Technical Authority in a suitable time frame prior to any tendering process to allow for an acceptable evaluation period. The evaluation period may take up to sixteen (16) months.

1.3 Equipment Procurement

Any ordering of equipment/material before the approval of the system design report will be undertaken at the contractor's own risk. The Design Authority may authorize the procurement of certain long lead items at, or shortly after a preliminary design review of the proposed system.

1.4 Quantity of Equipment

The quantity and location of the equipment required for CSC institutions will be contained in the specification identified in the Statement of Technical Requirements (STR).

2.0 APPLICABLE DOCUMENTS

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

ES/SOW-0101	Statement of Work for Procurement and Installations of Electronic Systems
ES/SOW-0102	Statement of Work for Quality Control of Electronic Systems Installations.
ES/SPEC-0103	Specification for Uninterruptable Power Supply
ES/SPEC-0204	Specification for Video Vertical Interval Switchers
ES/SPEC-0402	Specification for PIDS Public Address Systems
ES/SPEC-0403	Specification for an SIDS Closed Circuit Television Systems
ES/SPEC-0409	Specification for PIDS Closed Circuit Television Systems
ES/SPEC-0800	Specification for Communications and Control Consoles
ES/STD-0803	Standard for Video Display Unit
EIA-310-C	Electronic Industry Association Standard for Racks, Panels and Associated Equipment

3.0 REQUIREMENTS

3.1 General

The PIU shall provide the operator with centralized monitoring and control capability over all PIDS to the extent specified in the STR. The PIU shall incorporate industrial quality and commercially available controllers and Video Display Units (VDU). The VDU shall display the status of monitored subsystems and provide software control of system features, to the extent specified herein. The PIU shall include an operator console incorporating the VDU and operator controls.

3.1.1 Period of Operation

The PIU and all associated equipment shall be design for and capable of 24 hours per day, seven days per week operation.

3.1.2 Wires, Cables, Conduits, Ducts

The contractor shall 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 shall be performed in accordance with ES/SOW-0102, Statement of Work and all applicable national, provincial, and local electrical codes.

A wiring diagram shall 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 Government Furnished Equipment (GFE) or 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 STR.

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.

3.1.3 Wiring Supervision

Wiring shall be supervised in all system modes. An alarm shall occur if any system wiring is cut or shorted to other wires or if the system devices are tampered with by unauthorized people or environmental conditions.

3.1.4 Sabotage, Tampering and Survivability

Elements of the system shall have high resistance to damage, destruction. All interconnecting service must be secure against tampering

3.1.5 **Human Factors**

Elements of the system which are used directly by staff (i.e., control panels, annunciators, call originating devices, etc.) shall conform with accepted principles of good human factors design.

3.1.6 **Annunciation and Control Panels**

Mounting space within control posts is usually limited and the problem of determining a suitable equipment mounting location is minimized if the control panels are small. Therefore, the designer should make maximum possible use of annunciation and control devices which combine two or more functions into a single unit. The system shall use Electronic Industries Association (EIA) standard video display units. The design shall be in accordance with the ES/STD-0803, Standard.

3.2 **System Configuration**

3.2.1 **Hardware**

The industrial grade PIDS central controllers shall act as an interface between the operator peripherals and the digital control panels for remote devices and subsystems. Each controller shall incorporate the following physical attributes:

- designed to operate in industrial conditions on a continuous basis;
- built to withstand a harsh, rugged work environment;
- designed with a positive pressure cooling system which passes air through an external synthetic filter element which screens contaminants, then circulates flow through the controller chassis, drives, power supply and cards;
- equipped with a security lock which shuts off keyboard access preventing any tamper activity; and
- powered by a heavy duty power supply sized with 25% spare capacity when driving all expansion ports.

Each industrial grade PIDS controller shall incorporate the following electronic features:

- microprocessor based, modular in structure;
- featuring Pentium III, or equivalent, processor;
- running at a clock speed of 500 MHZ or higher, with zero wait states;
- configured with spare expansion port(s) capability;
- equipped with a CDR;

- equipped with dynamic expandable RAM, sized to suit software requirements;

- equipped with a 3.5 inch floppy drive system; and

- equipped with a fast access hard disk with an access speed of no longer than 28 ms, sized to suit all operating and system requirements, and suitable to hold the data storage/retrieval software and archival data for a period of one year with 25% spare disk capacity.

3.2.2 **Software**

The system software shall be designed specifically for security applications and shall provide for:

- polling and demand requests to monitor status;

- processing alarms according to predefined priorities;

- executing event-initiated software programs and related background software routines;

- controlling and processing communications with operator peripherals; and

- synchronizing all system activity including interfaces to peripherals, digital control panels and all field devices

For reasons of reliability and prevention of inadvertent changes, system software including operating systems and data files shall be maintained in non-volatile memory. The contractor shall also take all reasonable measures to ensure that no computer viruses are present in the delivered system. These measures shall include controls on the use of the software during the development and integration phases, and the tests for the presence of viruses. Similarly, steps must be in place through the careful selection of the operating system to prevent any introduction of software viruses without the constant need for extensive software security measures. The system shall incorporate security featured software for authorized access control by operators, supervisors and maintenance personnel.

The system software, especially for alarm processing, shall be written in a hardware compatible programming language, operating under a real time multitasking operating system to ensure that all priority activities are presented to the operator immediately as they occur. A capability shall be incorporated to ensure that all alarm data can be configured and exported in an appropriate format that can be processed by "DOS" family of operating system software.

3.2.3 **Redundancy**

The PIU shall be configured in a fully redundant hardware and software configuration and consist of two (2) controllers and two (2) interactive peripheral VDUs, capable of sustaining a complete controller failure without affecting the operation of either the PIDS, the FAAS, or any other integrated system. Master-Slave arrangements shall not be accepted. A failure in any integration

system or any system which has the display and controls integrated shall not effect the proper operation of the remainder of the equipment.

Two (2) additional interactive peripheral VDUs are required. These units shall also be in a fully redundant configuration. One unit shall be dedicated for system maintenance requirements, while the second unit shall be dedicated for operational supervisory control purposes or training related duties and may be located away from the MCCP. Neither one of these units will be mounted in the main console, but will be available in a satellite configuration as outlined below. All VDU consoles must function in a simultaneous and independent manner.

All input and output data shall be available to both controllers with a continuous dynamic update occurring in both controllers in order to allow cross-checking of input and output information between the controllers. In case of a discrepancy in the information between the controllers:

- the faulty controller shall be automatically removed from service;
- all system/operating software and current data files shall be automatically driven from the functional controller;
- a system status alarm shall alert the operator that automatic switch-over has occurred; and
- no interruption in service or loss of system status shall be perceivable when switching between controllers

Under normal operating conditions, and where the PIDS and FAAS controls are required, one of the interactive peripheral VDUs shall be dedicated to PIDS operational duties with a second VDU dedicated to FAAS operations. In the event of a controller or VDU failure, it shall be possible to combine PIDS and FAAS operations on a single VDU.

3.2.4 **Operator VDUs**

The primary "operator to system" interface for the display of alarm annunciation and for the command of an operator controlled functions on the PIDS system shall be via colour VDUs.

To eliminate confusion during an emergency situation, VDU screens shall have dedicated areas for alarms, secure and access states, operator prompts, operator commands, as well as time, day and date information.

To enhance operator understanding, full perimeter and facility graphics, complete with language descriptions, shall be used throughout to display and describe all system activity and instruction. The PIDS VDU shall each be capable of generating a minimum of sixteen graphic maps. All descriptions, alarm messages and operator instruction prompts shall be user definable in order to accurately describe unique institution configurations as well as future changes to perimeter/facility areas and operational requirements. Language of preference (French or English) to be determined by location as specified in the STR.

A typical graphic map shall incorporate the following display features as applicable to the area of presentation:

- location of fences, building structures, gates, sallyports, guard towers, patrol roads, etc.;
- location, type, condition, priority and real time status of all perimeter sensors; and
- emergency instruction and operator prompts.

The system graphics shall reduce information clutter to a minimum with the appropriate use of icons, especially to display sensor location and state. The following colours shall be supported for alarm sensors:

- green/light blue secure,
- yellow masked,
- red alarm, and
- purple failed.

The operator displays for the PIDS system shall be based on a 14" high resolution colour CRT with a minimum matrix size of 640 x 350 individually addressable pixels. The VDU shall be capable of displaying, as a minimum, the colours white, black, red, green, blue and all combinations of the primary colours in order to provide flexibility in colour map displays.

All map displays shall be able to be configured and reconfigured from a user friendly graphic software package, accessed from the maintenance menu.

3.2.5 **Operator Controls**

The colour VDUs for the PIDS system shall use a "Touch Screen" employing resistive membrane or surface acoustic wave technology (or equivalent). Plain language descriptions shall be utilized to initiate all system functions, minimizing operator activity and decision making. Typing mnemonic abbreviations, using unlabelled or numerical function buttons or using a mouse is unacceptable. When a function key is touched on the screen, the VDU shall lead the operator through the predefined functions by asking for a choice of options or menus. At every step of alarm processing, a help screen shall be available to guide the operator through system operation. The help screen shall contain information about functions currently available to the operator.

3.2.6 **Maintenance/Satellite VDUs**

The maintenance and the satellite VDUs shall be based on a l2" diagonal high resolution monochrome presentation. The maintenance VDU shall be located in the MCCP. The satellite VDU shall be remotable up to 250 feet. Specific location detail shall be stipulated in the STR. Further operational requirements and parameters for these VDUs are detailed in subsequent sections entitled PIDS System Menus and PIDS Maintenance Functions, sections respectively.

3.2.7 **Maintenance/Satellite Controls**

The maintenance and satellite VDUs shall have an associated keyboard with an integral key-lock switch for command and data input. Multi-level password protection shall be available in software to limit maintenance and satellite access, assignment and editing capability to authorized personnel only. All passwords shall be user definable.

3.2.8 **PIDS System Menus**

The PIDS System Menus shall permit display and control of various system functions, including for the operator:

- a user definable checklist and an emergency instruction set;
- the capability to activate secure or access states for perimeter sensors;
- the ability to clear tamper, jam, fail and diagnostic alarms;
- scanning of all applicable site maps;
- an automatic or manual step through available camera views;
- the ability to set up an automatic camera viewing sequence; and
- the ability to perform sensor(s) test(s).

The maintenance/satellite menus shall permit control of the following:

- system time and date;
- activation or deactivation of any field device;
- generation of status, test and statistical reports for sensors and other field devices with available inputs;
- viewing of equipment configuration;
- generation of field profiles for MDS or FDS with available field inputs;

- generation of system resets, or threshold establishment for MDS or FDS with available field inputs;

- assignment of menus and accessibility for operators;

- creation of checklists and emergency instruction prompts; and

- simulation of alarms for operator training.

3.3 PIDS Alarm Processing

3.3.1 Alarm Priorities

The PIU controller shall have multiple levels of priority for displaying alarms. Each possible alarm type shall be assigned a separate priority level as defined in the STR. All alarms shall be held in non-volatile memory. The PIU controller shall rank the alarms, displaying highest priority alarms at the top of the list and lowest priority alarms at the bottom. The total number and type of alarms to be processed shall also be displayed.

When multiple alarms occur, the first received, highest priority alarm shall be displayed on the VDU until processed by the operator. Then the next highest priority alarm shall be displayed until processed, etc. If a higher priority alarm is received before a lower priority alarm is processed, the high priority alarms shall replace the lower priority alarm on the VDU. The lower priority alarm shall then be retained in memory and be redisplayed after the higher priority alarm has been processed.

The operator shall have the capability of stepping through the list of alarms and dealing with the alarms in any order. If at any time the operator is viewing an alarm which is not the highest priority alarm present in the system, the operator shall have the option of returning directly to the highest priority alarm by activating a single control.

3.3.2 Alarm Simulation Priority

The PIU controller shall be capable of distinguishing between simulated and genuine alarm inputs. In the event that a genuine alarm is received while the alarm simulation is in use, the PIU computer shall:

- cancel all existing simulated alarms;

- ignore any additional simulated alarms; and

- display the genuine alarm.

The PIU controller shall only accept simulated alarms when there are not genuine alarms in the system.

3.3.3 **Alarm Processing**

Activation of any alarm from a PIDS subsystem, connected to the PIU controller shall cause the following action:

- full, plain language description and perimeter graphic display of the alarm condition, type and location
- audible signal, flashing alarm condition and emergency instruction set presentation
- activation of all CCTV related equipment, including automatic video switching to the assessable area, and video recording etc.
- initiation of an audio path via the PIDS public address system
- acknowledgement of the alarm by the operator as his only course of action
- assignment of alarm causes by the operator by choosing from a predefined menu of causes.
- ability to scroll through the previous 25 recorded alarm incidents.

3.4 **Intrusion Detection Systems**

3.4.1 **Data input**

Bi-directional data links shall be provided in order for the PIU controller to receive the following information from the Motion Detection System and the Fence Disturbance Detection System:

a. Alarm annunciation;
b. System test results;
c. Zone tamper annunciation;
d. Zone tamper cancel;
e. System fail annunciation;
f. System fail cancel;
g. Alarm information data (where applicable);
h. Threshold information (where applicable); and
j. Test alarm data and results (where applicable).

These messages shall be available using form C dry contact closures, or an EIA standard RS-232-C or RS-485 data link, as required by the MDS and the FDS system controllers.

3.4.2 **Data Output**

Bi-directional data links shall be provided in order for the PIU controller to provide the following information to the MDS and FDS terminal equipment:

a. Alarm acknowledge
b. Alarm cancel
c. Zone mask
d. Zone secure
e. Zone tamper acknowledge
f. Test target activation (where applicable)
g. System test

These messages shall be available using form C dry contact closures, or an EIA standard RS-232-C or RS-485 data link, as required by the MDS and the FDS system controllers.

3.4.3 **Miscellaneous Inputs**

Where applicable, secondary outputs from FDS sensors, such as audio, shall be PIU software controlled and switchable on a sector by sector basis. In general, only the information from those sectors being assessed or monitored will be relayed for use by the operator.

3.4.4 **Data Protocol**

All RS232 or RS485 signals provided to, and received from, the PIDS should conform to either the Senstar-Stellar Sennet or StarCom protocols. Any driver required for another protocol will be the responsibility of the contractor.

3.5 **PIDS CCTV System**

3.5.1 **General**

The PIU shall integrate the CCTV assessment system described in Specification ES/SPEC -0409 and provided by others. The Contractor shall mount the PIDS CCTV monitors in the PIU console and shall connect the monitors and cameras to the switcher described in 3.5.2.

3.5.2 **Vertical Interval Switcher**

The PIU shall integrate a Video Switcher, outlined in Specification ES/SPEC-0204. The PIU controller will control the video switcher to provide the following sequence options:

a. zone sequence mode - the monitors sequence by zone, simultaneously displaying all cameras associated with a zone.

b. group selection mode - the monitors sequence cameras by predesignated groupings, e.g., all sally port cameras, etc.

c. alarm lock-up mode - all cameras associated with a zone are automatically displayed in the event of an MDS/FDS intrusion or tamper alarm.

Camera/monitor assignments shall be user defined, and variable through software control.

Sequence options (a) and (b) shall be user selectable. Camera sequences shall occur under operator control, or automatically by the PIU controller with a predefined dwell time. In case of an alarm, fail or tamper condition, the system shall revert immediately to the alarm lock-up mode to display the sector in question. Upon completion of the alarm/tamper condition, the system shall return to the sequence mode in use prior to the alarm lock-up mode.

3.5.3 **Dwell Time**

Dwell times used in the PIDS sequence modes shall be generated by the PIU controller and shall be user definable.

3.5.4 **VCR Control**

The PIU controller shall automatically start the record function of the VCRs, supplied by others as per Specification, ES/SPEC-0409, any time an alarm, fail or tamper condition has been received. The VCRs shall continue to record until an alarm cancel, tamper or fail reset has occurred.

Manual operation of the VCRs shall also be possible, using the appropriate VCR record button. VCR activity shall be relayed to the Data Logging system.

3.5.5 **CCTV Character Generator**

The PIU shall incorporate a video character generator interfaced to the video switcher and CCTV monitors. The character generator shall provide the appropriate camera number identification, date and time of day to each monitor. The size of the characters displayed shall be adjustable. The position of the camera number identification and date/time shall be independently adjustable and shall not be restricted to any portion of the monitor screen.

The CCTV character generator may be an integral part of the video switches specified in paragraph 3.5.2.

3.5.6 **Unused Camera Ports**

At anytime a CCTV monitor is unused, the PIU shall route a "video black" signal to the monitor. This may occur if a camera fails, is removed or if less than four PIDS CCTV cameras are assigned to a zone or group.

3.5.7 **Miscellaneous CCTV Functions**

The PIU controller shall be able to sense and annunciate end-of-tape conditions and relay this information to the data logging system.

Similarly, the wiper function of the camera housings, supplied by others as per ES/SPEC-0409 shall be PIU computer controlled on a sector by sector basis. This function shall be user operated and shall involve those units being assessed or monitored at that time.

3.6 Time/Date Information

The PIU controller shall generate accurate time/date information, suitable to act as a central generating unit of this information for all systems forming part of the MCCP. This shall include the video systems and the data logger. Interface to the various systems shall be in either parallel or serial form, as required. The availability of both types of output ports shall be provided to allow for future expansion or interfacing.

3.7 PIDS PA Control

3.7.1 PA Control

The PIU controller shall control the PA, as per Specification, ES/SPEC-0402. The PIDS PA provides one way voice communication to an alarmed sector. The output of the PA shall be switched on a sector by sector basis under alarm conditions as outlined in section 3.3 of this specification. In case of an alarm condition, the output of the PIDS PA shall be switched to the sector being assessed. The activation of the PA shall be under the control of the operator. Only the activation and actual use of the PIDS PA shall be logged by the data logger.

3.7.2 PIDS PA Control Panel

The PIU contractor shall provide a PIDS PA controls panel in the operator console. The panel shall contain a microphone input and test tone generator to permit access to and testing of the PIDS PA subsystem on a sector by sector basis.

3.8 FDS Audio Monitoring Panel

The PIU contractor shall provide an FDS audio monitoring panel in the MCCP console as specified in the STR. The panel shall contain controls to permit the MCCP operator to monitor the audio signals generated by the FDS sensors via remote selection of FDS sector audio. A speaker shall be provided in the MCCP or the operator console for FDS audio monitoring. The contractor shall provide a volume control in the FDS audio monitoring panel to control the audio level. The contractor shall be responsible for the connection to and integration of the audio signals and controls with the audio monitoring panel.

3.9 SIDS CCTV Integration

3.9.1 General

The SIDS CCTV system includes auxiliary cameras, camera controls, monitors and VCRs to provide general surveillance of various parts of the institution. The SIDS camera selection and positioning are controlled directly by the MCCP operator and not by the PIU controller. The SIDS is described in detail in Specification, ES/SPEC-0403.

3.9.2 **Monitor and Control Panel Integration**

The PIU Contractor shall integrate the SIDS CCTV monitors and control panels, in the quantities listed in the STR, into the PIU operator console. The contractor shall connect the monitors and control panels to the UPS power and to the associated cameras at the defined interface. Time and date information from the PIU shall be available on these monitors.

3.9.3 **SIDS VCR Integration**

The SIDS VCRs shall be mounted in the PIU VCR/printer housing as outlined in section 4.3. The contractor shall connect the VCRs to the UPS power and shall interface the VCRs to the SIDS monitors. The contractor shall install VCR RECORD ON/RECORD OFF push-buttons and an end of tape alarm light adjacent to the associated SIDS monitors and shall connect these controls to the VCRs.

3.10 **Data Logging**

3.10.1 **General**

The PIU controller shall provide data logging (ASCII coded text activity archive) storage of over 100,000 lines of subsystem events on hard disk storage. On demand, activity archive stored events shall be sorted by type and/or date and transferred to DOS formatted floppy disks or sent to a printer to provide a hard copy of PIU and integrated subsystems events. For each event, the activity file shall show the date, time and event description.

The PIU controller shall notify the operator via the display when the hard drive has reached 75% capacity, and again when it has reached 90% capacity. It shall prompt the operator to download the oldest files onto floppy diskettes. The PIU controller shall automatically purge the oldest files when the hard drive reaches 95% capacity, bringing the hard drive down to the 50% level.

3.10.2 **Event Definition**

Data logged events will include all status changes of monitored subsystems including PIDS alarms, alarm acknowledgement, alarm clear/reset, UPS failure or bypass, PIU controller switch-over, etc. Normal sequencing of PIDS CCTV cameras will not be data logged.

3.11 **Printer Status**

The printer status shall be monitored by the PIU controller. Failure of the printer or a "paper-out" condition shall generate an alarm.

3.12 **Status Panel**

3.12.1 **General**

The PIU shall contain a status panel containing indicators and controls for the major PIU units. The status panel shall also contain status lights for the UPS.

3.12.2 **PIU Status Functions**

The status panel shall provide the following indicators and controls:

a. PIU controller fail indicator; and

b. Active PIU computer selection control.

3.13 **UPS Integration**

The contractor shall connect UPS power into all PIU equipment racks. The UPS will be provided as GFE and will be in accordance with Specification ES/SPEC-0103. Power shall be taken from the AC regulator output or from an equivalent point in a distribution panel if available. All PIU equipment shall be connected to the UPS power. UPS status shall be monitored as per section 3.12.3.

4.0 MECHANICAL CONFIGURATION

4.1 General

The PIU equipment shall be installed in at least two distinct and separate units: an operator console and equipment racks. Displays and controls including GFE required by the operator shall be installed in a contractor provided operator console. Other equipments shall be installed in EIA standard 19-inch racks located in the CER or other location as required by the STR. All racks and console bays shall include side panels and rear doors. Requirements for raised flooring, cable entrances and/or rack cooling ducts shall be specified in the proposal.

4.2 Console Design

The operator console shall be ergonomically designed to provide the operator with a logical, easily understood display and control layout. All displays shall be clearly viewable and all controls shall be easily reachable from a seated position. The console shall contain a work surface at normal desk height not less than 18 inches in depth and extending the full width of the console. The work surface shall be covered with a scratch-resistant plastic covering. Detailed design requirements will be outlined in the STR.

The contractor shall provide a separate table or attachment to the console for mounting the MCCP operator telephones; if an attachment is provided, it shall not cause the telephones to block any display or control. The contractor shall provide a standard non-tip swivel-base chair with casters and arms for the PIU operator. Specification ES/SPEC-0800 shall apply to the console design.

4.3 VCR/Printer Rack

The PIU contractor shall provide a separate rack or stand to be located near the operator console for mounting the PIDS VCRs, SIDS VCRs and printer. All equipments installed below the top surface of the rack shall be mounted on slide out shelves equipped with positive stops. The VCR/printer rack shall be readily movable.

4.4 Console/Rack Colour Schemes

The operator console, telephone table/attachment and VCR/printer rack shall be covered with a high quality paint using a standardized colour scheme. Racks for other equipment shall utilize a common-colour scheme for racks, end panels and doors.

4.5 Environmental Requirements

The PIU shall operate over the following indoor environmental conditions:

4.5.1 Temperature: 0° C to +50° C; and

4.5.2 Humidity: 0 to 90% relative, non-condensing.

4.6 **Power Requirements**

The system shall use VAC power within the following limits:

4.6.1 Voltage: 120 VAC ±10%;

4.6.2 Frequency: 60 Hz ±1.5%;

4.6.3 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 shall not cause damage to the unit; and

4.6.4 Power: power consumption shall not exceed 100 watts.

4.7 **PIDS Maintenance Functions**

Monitoring the PIU and the PIDS subsystems shall be made available through the PIU controller and the maintenance and satellite VDUs. User-definable password protection shall be provided to limit access to authorized personnel.

The following information shall be available to the standby data logger via the EIA standard RS-232-C port, as well as displayed on the maintenance and satellite VDUs.

4.7.1 **PIDS Maintenance Functions**

The PIDS maintenance menus shall allow:

a. Automated PIU systems and equipment fault diagnostics;

b. Two-way data interface with MDS and FDS systems to provide sensor information such as test activation and results, thresholds, status reports, etc ., where applicable;

c. MDS and FDS sensor calibration, where applicable;

d. PIU data base cross check information;

e. Processor unit error monitoring;

f. Data Logging port assignments;

g. Statistical PIDS activity summary for MDS and FDS alarms and total "Mask" times, on a sector by sector basis, since the previous request for this data; and

h. MDS and FDS target response information, where available.

4.8 **Installation Requirements**

The Perimeter Intrusion Detection System Integration Unit shall be installed at the site in accordance with the ES/SOW-0101, Statement of Work and the ES/SOW-0102, Statement of Work.

4.9 **Documentation Requirements**

All final Perimeter Intrusion Detection System Integration Unit documentation shall be provided in accordance with the ES/SOW-0101, Statement of Work.

4.10 **Support Requirements**

The Perimeter Intrusion Detection System Integration Unit maintenance and spares support shall be provided in accordance with the ES/SOW-0101, Statement of Work.

4.11 **Training Requirements**

Operator training and maintenance training on the Perimeter Intrusion Detection System Integration Unit shall be in accordance with the ES/SOW-0101, Statement of Work.

5.0 QUALITY ASSURANCE

5.1 General

The Perimeter Intrusion Detection System Integration Unit Quality Assurance programme shall be provided as detailed in the ES/SOW-0101, Statement of Work.

All on-site installation work, test plans and Perimeter Intrusion Detection System Integration Unit acceptance testing shall be conducted in accordance with the ES/SOW-0101, Statement of Work.

6.0 DELIVERY

Delivery requirements for the Perimeter Intrusion Detection System Integration Unit documents, drawings, plans, manuals, etc. (where applicable) shall be in accordance with the ES/SOW-0101, Statement of Work.

Delivery requirements of the Perimeter Intrusion Detection System Integration Unit equipment shall be in accordance with the ES/SOW-0102, Statement of Work.

7.0 INTERFERENCE

Performance of the Perimeter Intrusion Detection System Integration Unit shall not be affected by the use of standard electronic equipment used at the institution. Distance limits of standard electronic equipment shall be in accordance with the ES/SOW-0101, Statement of Work.

8.0 SAFETY

All Perimeter Intrusion Detection System Integration Unit electrically powered elements shall meet the applicable Canadian Standards Association (CSA) standards.

Correctional Service Canada
Technical Services Branch
Electronics Systems

ES/SPEC-0402
Revision 2
8 March, 2002

ELECTRONICS ENGINEERING SPECIFICATION

PIDS PUBLIC ADDRESS SYSTEM FOR USE IN FEDERAL CORRECTIONAL INSTITUTIONS

AUTHORITY

This Specification is approved by the Correctional Service of Canada for the procurement and Installation of Perimeter Intrusion Detection System (PIDS) Public Address (PA) systems in Canadian federal correctional institutions.

Recommended corrections, additions or deletions should be addressed to the Design Authority at the following address: Director, Engineering Services, Correctional Service of Canada, 340 Laurier Avenue West, Ottawa, Ontario, K1A 0P9

Prepared by :

Manager,
Electronic Systems Research

Approved by :

Director,
Engineering Services

8 Mar 02

TABLE OF CONTENTS

ABBREVIATIONS

The following abbreviations are used in this specification:

CER	Common Equipment Room
COTS	Commercial-Off-The- Shelf
CSA	Canadian Standards Association
CSC	Correctional Service Canada
DES	Director Engineering Services
EIA	Electronic Industries Association
GFE	Government Furnished Equipment
MCCP	Main Communications and Control Post
PA	Public Address
PIDS	Perimeter Intrusion Detection System
RFP	Request for Proposal
SOW	Statement of Work
STR	Statement of Technical Requirements

DEFINITIONS

The following definitions are used in this specification:

Design Authority	Director, Engineering Services (DES) - Correctional Service 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.

1.0 INTRODUCTION

1.1 General

This specification defines the essential technical and functional requirements of the Correctional Service Canada (CSC) for the procurement and installation of a Public Address (PA) system to be used in conjunction with the Perimeter Intrusion Detection System (PIDS) in federal correctional institutions.

1.2 Purpose

The PIDS Public Address System provides the Main Communication and Control Post (MCCP) operator with one-way voice access into each zone of the PIDS-protected perimeter. The operator will use this system to communicate with intruders detected and observed by the PIDS system.

The system described herein would be applicable to new institutions to be constructed. It could also be retrofitted into existing institutions whenever it becomes necessary to add a perimeter Public Address capability or replace existing obsolete equipment.

1.3 Commercial-Off-The-Shelf Equipment

The PIDS PA system shall use commercial off-the-shelf (COTS) equipment and proven designs to the maximum extent possible. All new equipment shall meet the specified lifespan requirements. New equipment designs shall be restricted to unique interfaces and common control consoles.

1.4 Technical Acceptability

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. 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 shall maintain very high standards of dependability and reliability.

The CSC 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.

The technical acceptance process shall involve system and subsystem evaluation in accordance with the applicable CSC specifications in one of CSC facilities or may be tested in a CSC facility to verify the effectiveness of the proposed technologies when subjected to the restrictive operational environment.

CSC shall also verify in depth any of the system technical specifications called up. CSC may, when it deems necessary, request the supplier to arrange for a full site demonstration. 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.

It is the supplier's responsibility to make new developments in products available to CSC for evaluation. Equipment qualification is an ongoing process and can be initiated at any time by a vendor. Any vendor can have access to the CSC specifications and standards. Any new development or products should be submitted to the CSC Engineering Services Division, Technical Authority in a suitable time frame prior to any tendering process to allow for an acceptable evaluation period. The evaluation period may take up to sixteen (16) months.

1.5 Equipment Procurement

Any ordering of equipment/material before the approval of the PIDS PA system design report will be undertaken at the contractor's own risk. The Design Authority may authorize the procurement of certain long lead items at, or shortly after a preliminary design review of the proposed system.

1.6 Quantity of Equipment

The quantity and location of the PIDS PA equipment required for CSC institutions will be contained in the specification identified in the Statement of Requirements (STR).

2.0 APPLICABLE DOCUMENTS

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

ES/SOW-0101	Statement of Work for Electronic Systems for Correctional Service of Canada Institutions.
ES/SOW-0102	Statement of Work for Quality Control for installation of Electronic Systems in Federal Correctional Institutions.
ES/SPEC-0005	Specification for Main Communications and Control Post Integration Consoles
ES/SPEC-0401	Specification for Perimeter Intrusion Detection System Integration Units
EIA-310-C	Electronic Industry Association Standard for Racks, Panels and Associated Equipment

3.0 REQUIREMENTS

3.1 General

The contractor shall design, supply, install, test and provide documentation and training for a Perimeter Intrusion Detection System Public Address system in accordance with the Standards, Specifications and Statements of Work specified in Section 2.0.

3.1.1 System Configuration

The PIDS Public Address system elements shall be deployed zone by zone at the perimeter of the institution corresponding to the alarm and detection zones of the PIDS system. The system shall consist of the following elements in quantities to be determined by the contractor as required to support this requirement.

a. PIDS Public Address Switcher consisting of:

- a zone selector panel;
- a microphone; and
- test tone generator.

b. Loudspeaker assemblies, one or more per zone, consisting of:

- loudspeaker and matching transformer;
- horn; and
- mounting fixture.

c. Common equipment (amplifiers, power supply, etc.)

d. Interconnecting wire, cable, conduits, ducts, junction boxes, etc.

3.1.2 System Capacity

The number of loudspeaker assemblies and the number of zones served by each shall be as specified in the STR. The system shall be of a modular design and it shall be possible at a future date to add more associated equipment to the basic installed complement without requiring the existing hardware.

3.1.3 Period of Operation

The system and all associated equipment shall be rated for and capable of 24 hours per day, seven days per week operation.

3.2 System Requirements

3.2.1 Wires, Cables, Conduits, Ducts

The contractor shall 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 shall be performed in accordance with ES/SOW-0102, Statement of Work and all applicable national, provincial, and local electrical codes.

A wiring diagram shall 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 Government Furnished Equipment (GFE) or 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 STR.

3.2.2 Control Equipment

The maximum feasible amount of common control equipment (power supplies, logic boards, amplifiers, etc.) shall be located in Terminal Equipment Spaces (TES) and Common Equipment Room (CER) provided for the purpose. These areas will be identified in the STR. It is preferred that only equipment such as control panels, etc., which the operator must access directly, should be located in the Control Posts.

3.2.3 Interface to Data Logger

The contractor shall supply and install all necessary wiring and control equipment required to interface the system to the PIU Data Logger described in ES/SPEC-0005, Specification.

3.3 Design Requirements

3.3.1 General

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

A design objective is to minimize the number of wires required between all elements of the system.

A space-diversity approach to system planning shall be employed to ensure that loss of one interconnection routing does not impair the operational capability of the complete system.

3.3.2 Wiring Supervision

Wiring shall be supervised in all system modes. An alarm shall occur if any system wiring is cut or shorted to other wires or if the system devices are tampered with by unauthorized people or environmental conditions.

3.3.3 Speaker Locations

Speakers shall be located to provide complete coverage of the assigned zones.

3.3.4 Speaker Output

At any point in the assigned zone, the voice output shall be intelligible in the presence of the highest level of background audio interference normally encountered at that point (e.g., high wind, etc.)

3.3.5 PA Switcher

The PIDS PA Switcher shall be controlled by the PIU processor. The switcher shall enable the selection of a one-way voice path to each perimeter zone on a mutually exclusive basis. The zone selected shall be visible on the front panel of the PIDS PA switcher.

The PIDS PA switcher shall meet the following requirements:

a. equipped with an adjustable test tone generator;

b. capacity for up to 15 perimeter zones;

c. installed in an Electronic Industries Association (EIA) standard 19" equipment rack;

d. equipped with connectorized inputs/outputs; and

e. system alarm outputs for power supply failure, loop continuity failure, and switching relay failure.

3.3.6 Microphone

The microphone shall be co-located with the PIDS Public Address Control Panel, and shall be used to communicate with the selected zone. The microphone shall be equipped with an integral push-to-talk switch which will permit the operator to open the voice path to the selected zone. The microphone shall be a hand-held type and attached to the PIU console via a spring clip retainer.

3.3.7 Speaker Mounting

The speakers shall be installed outdoors and shall be rugged, weatherproof units capable of satisfactory operation under the environmental conditions of this specification. The speaker units and their mountings shall exhibit high resistance to damage or destruction due to deliberate, physical abuse. The contractor shall submit a sample of the unit he proposes to use for approval prior to proceeding with procurement of these parts. Speakers shall be mounted so as to be unreachable without climbing aids such as ladders, etc. Speakers shall be mounted on the outside of the inner perimeter fence.

3.3.8 Matching Transformer

The matching transformer shall be part of the speaker assembly and shall have a number of selectable taps to permit on-site selection of the proper power level to be delivered to each speaker. The taps shall be provided with a secure cover to inhibit unauthorized adjustment.

3.3.9 Interchangeability

Speakers and associated equipment shall be readily interchangeable. Where feasible, all major components shall be of modular plug-in design.

3.3.10 Facilities

Power for this system is available at each institution from the domestic source through the Emergency Power Distribution System. The latter system consists of a diesel-electric set which typically requires twenty (20) seconds to take over the load on sensing failure of the domestic source.

3.3.11 System Performance on Switch over

The PIDS PA system shall incur no failure or damage directly attributable to switch over of power sources as described in this specification. On completion of a switch over action, this system shall provide normal system operation.

3.3.12 **Sabotage, Tampering and Survivability**

Elements of the system must operate in areas exposed to inmate access and shall have high resistance to damage, destruction, or conversion to other uses (including weapons). All interconnecting service must be secure against tampering or improper eavesdropping interference.

3.3.13 **Power Failure**

Loss or restoration of primary power to the system shall not produce spurious annunciations or outputs to the data logger. When power is returned after a power failure, the system shall resume normal operation without operator action.

3.3.14 **System Failure**

A system failure shall be deemed to have occurred when any required annunciation is not produced or when any required control function cannot be performed.

3.3.15 **Human Factors**

Elements of the system which are used directly by staff or inmates (i.e., control panels, etc.) shall conform with accepted principles of good human factors design.

3.3.16 **Existing Equipment**

In most installations, control elements of the system will share console space with other electrical/electronic equipment such as door controls, 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 system according to accepted human engineering principles to ensure a uniform appearance and commonality of a layout to assist the operator in the performance of his duties.

3.3.17 **Control Panels**

Mounting space within control posts is usually limited and the problem of determining a suitable equipment mounting location is minimized if the control panels are small. Therefore, the designer should make maximum possible use of control devices which combine two or more functions into a single unit.

The system shall use EIA standard display and control panels. The design of the display and control panel shall be in accordance with the ES/STD-0802, Standard.

3.4 Functional Requirements

3.4.1 PA Control

The Perimeter Intrusion Detection System Integration Unit shall control the PIDS PA. In the event of a perimeter alarm condition, the output of the PIDS PA shall be automatically switched to the perimeter sector being assessed by the CCTV system. The output of the PA shall be switched on a sector by sector basis under alarm conditions. The PIDS PA shall provide the MCCP operator one way voice communication to an alarmed sector. The activation of the PA shall be under the control of the operator using the push-to-talk switch on the microphone. Only the activation and actual use of the PIDS PA shall be logged by the PIU data logger.

3.4.2 PA Control Panel

The contractor shall provide a PIDS PA controls panel in the operator console. The panel shall contain a microphone input and test tone generator to permit access to and testing of the PIDS PA system on a sector by sector basis.

3.5 Environmental Requirements

The amplifier, microphone and speaker equipment shall comply with all requirements of this specification over the following environmental ranges:

3.5.1 Indoor Equipment

- temperature 0°C to 50°C; and
- humidity 0% to 95% Non Condensing.

3.5.2 Outdoor Equipment

- temperature -40°C to +55°C; and
- humidity up to 100% Condensing.

In addition, outdoor equipment shall continue to operate in full compliance with all parts of this specification and shall not be damaged by any of the following conditions in any combination:

- exposure to direct sunlight;
- any amount of frost;

- wind velocity up to 100 Km per hour;
- rain;
- snow;
- hail stones up to 2 cm in diameter;
- ice buildup to a thickness of 2 cm; and
- any air-to-ground or ground-to-air lightning strikes outside a 1 Km radius.

3.6 **Power Requirements**

The system shall use VAC power within the following limits:

3.6.1 Voltage: 120 VAC ±10%;

3.6.2 Frequency: 60 Hz ±1.5%;

3.6.3 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 shall not cause damage to the unit; and

3.6.4 Power: power consumption shall not exceed 100 watts.

3.7 **Installation Requirements**

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

3.8 **Documentation Requirements**

All final system documentation shall be provided with a Copyright Release for the documentation delivered in support of the system. The documentation shall be in accordance with the ES/SOW-0101, Statement of Work.

3.9 **Support Requirements**

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

3.10 **Training Requirements**

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

4.0 QUALITY ASSURANCE

4.1 General

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

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

4.2 System Check Out

During the system check out, the contractor shall measure PIDS PA system sound levels as follows:

For each speaker, measure the test tone & voice sound levels between the perimeter fences at two locations:

- directly in front of speakers; and
- the midpoint between two (2) speakers

The contractor shall record the sound level readings and submit the test results to the Design Authority.

4.3 Final Acceptance Test Procedures

The Design Authority will repeat the system check out tests with the contractor, using the same sound level metre that was used for the system check out.

5.0 DELIVERY

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

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

6.0 INTERFERENCE

Performance of the system shall not be affected by the use of standard electronic equipment used at the institution. Distance limits of standard electronic equipment shall be in accordance with ES/SOW-0101, Statement of Work.

7.0 SAFETY

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

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:

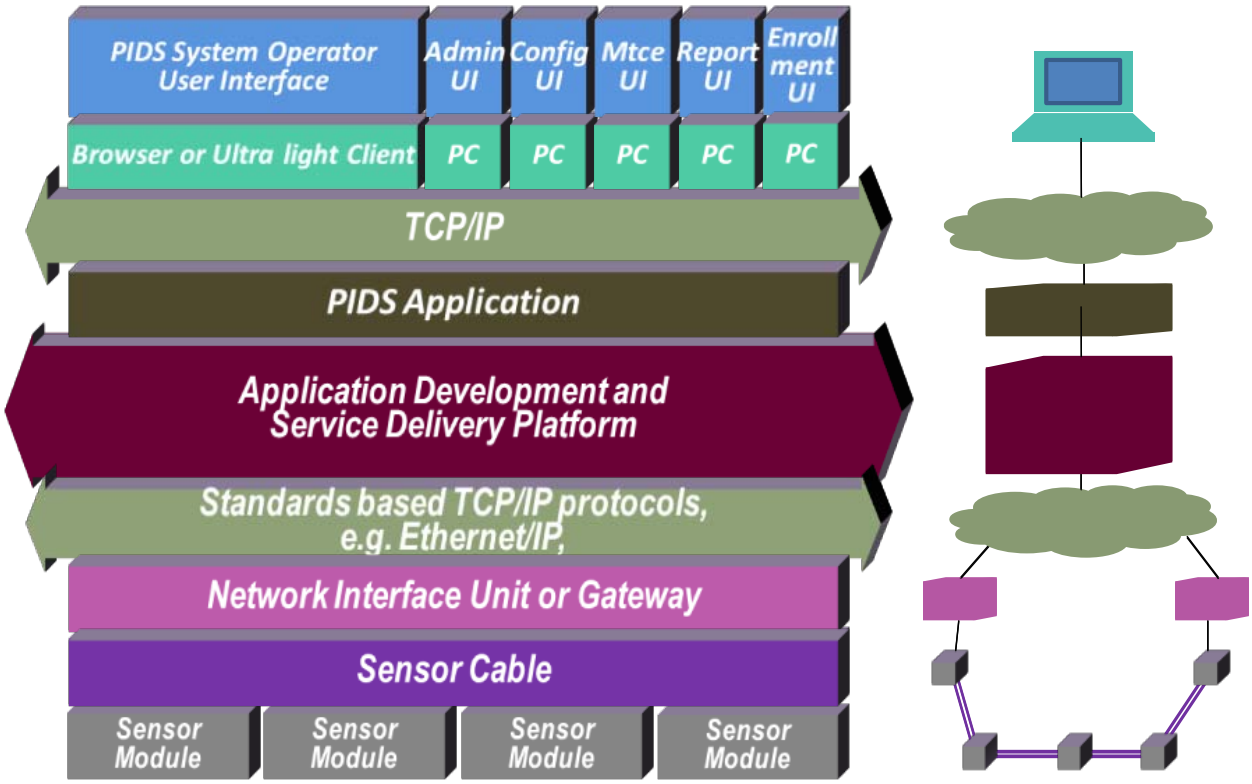
.1 If specified in the STR, an Operator User Interface that presents the Operator with the information needed to manage the functionality to be provided by the MDS sub-system.

.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.

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.

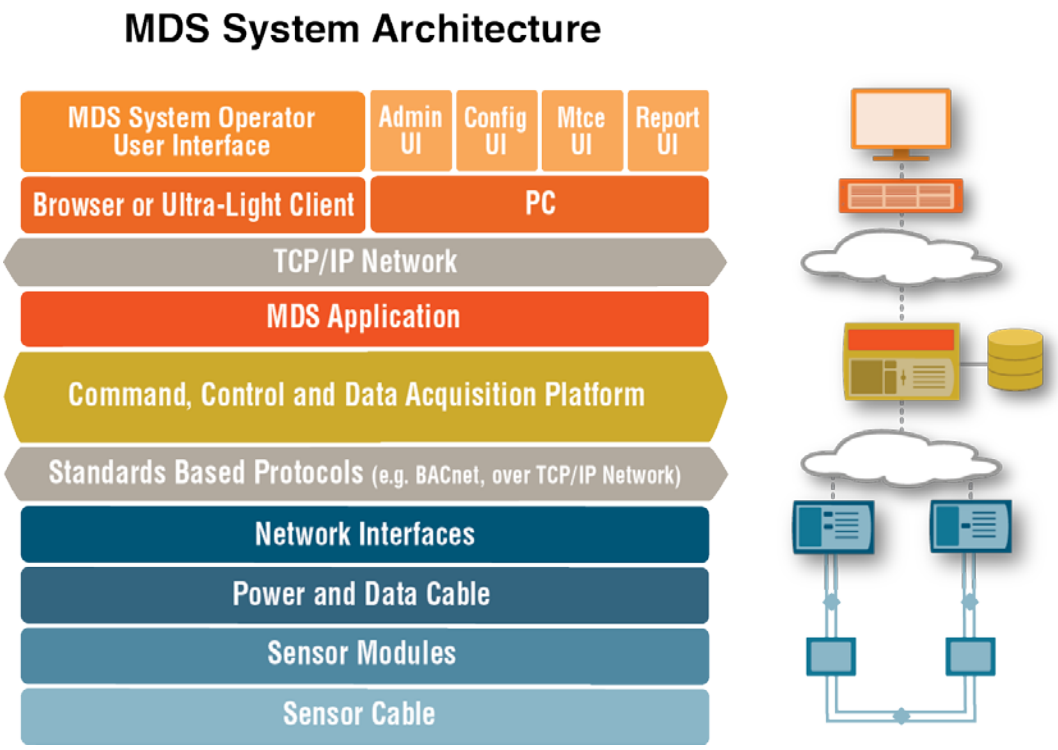
.3 A Report Development and Generation User Interface.

.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 ----------

Correctional Service Canada
Technical Services Branch
Electronics Systems

ES/SPEC-0409
Revision 3
November 2001

ELECTRONICS ENGINEERING SPECIFICATION

PERIMETER INTRUSION DETECTION SYSTEM CLOSED CIRCUIT TELEVISION SYSTEM FOR USE IN FEDERAL CORRECTIONAL INSTITUTIONS

AUTHORITY

This Specification is approved by Correctional Service Canada for the procurement and Installation of Digital Field Switchers in Closed Circuit Television (CCTV) Systems in Canadian federal correctional institutions.

Recommended corrections, additions or deletions should be addressed to the Design Authority at the following address: Director, Engineering Services, Correctional Service of Canada, 340 Laurier Avenue West, Ottawa, Ontario, K1A 0P9

Prepared by:

Manager,
Electronics Systems Research

Approved by:

Director,
Engineering Services

TABLE OF CONTENTS

ABBREVIATIONS

The following abbreviations are used in this specification:

CCTV	Closed Circuit Television
CER	Common Equipment Room
COTS	Commercial-Off-The- Shelf
CSA	Canadian Standards Association
CSC	Correctional Service Canada
DES	Director Engineering Services
EIA	Electronic Industries Association
FDS	Fence Disturbance Detection System
FOV	Field of view
GFE	Government Furnished Equipment
MDS	Motion Detection System
MCCP	Main Communications and Control Post
PIDS	Perimeter Intrusion Detection System
PW&GSC	Public Works and Government Services Canada
RFP	Request for Proposal
SOW	Statement of Work
STR	Statement of Technical Requirements
TES	Terminal Equipment Space

DEFINITIONS

The following definitions are used in this specification:

Design Authority	Director, Engineering Services (DES) - Correctional Service 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.

1.0 INTRODUCTION

1.1 General

This specification defines the essential technical and functional requirements of the Correctional Service Canada (CSC) for the procurement and installation of a Perimeter Intrusion Detection System (PIDS) Closed Circuit Television (CCTV) system for federal correctional institutions.

The system described herein would be applicable to new institutions to be constructed. It could also be retrofitted into existing institutions whenever it becomes necessary to add a PIDS CCTV capability or replace existing obsolete equipment.

1.2 Purpose

The primary use of the PIDS CCTV system is to provide a surveillance and assessment capability for the staff in the Main Communications and Control Post (MCCP) of an institution with fenced and/or walled perimeters as follows:

1.2.1 Fenced Perimeters

For the standard double fence perimeter which uses a Fence Disturbance Detection System (FDS) sensor and the Motion Detection System (MDS) sensor, the CCTV coverage area is defined as the institution side of the inner perimeter fence fabric plus a minimum distance of 3 metres inside the inner perimeter fence and the complete area between the two fences. For a single fence perimeter, this coverage area is defined as the institution side of the inner perimeter fence fabric plus a minimum distance of 3 metres inside the inner perimeter fence.

1.2.2 Walled Perimeters

The CCTV coverage area is defined as the top and inside of the perimeter wall from a point 2 metres above the wall to a point 3 metres from the base of the wall. The target shall be in full view when positioned anywhere on top of the wall.

1.3 Commercial-Off-The-Self Equipment

The CCTV system shall use commercial off-the-shelf (COTS) equipment and proven designs to the maximum extent possible. All new equipment shall meet the specified lifespan requirements. New equipment designs shall be restricted to unique interfaces and common control console.

1.4 Technical Acceptability

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. 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 shall maintain very high standards of dependability and reliability.

The CSC 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.

The technical acceptance process shall involve system and subsystem evaluation in accordance with the applicable CSC specifications in one of CSC facilities or may be tested in a CSC facility to verify the effectiveness of the proposed technologies when subjected to the restrictive operational environment.

CSC shall also verify in depth any of the system technical specifications called up. CSC may when it deems necessary, request the supplier to arrange for a full site demonstration. 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.

It is the supplier's responsibility to make new developments in products available to CSC for evaluation. Equipment qualification is an ongoing process and can be initiated at any time by a vendor. Any vendor can have access to the CSC specifications and standards. Any new development or products should be submitted to the CSC Engineering Services Division, Technical Authority in a suitable time frame prior to any tendering process to allow for an acceptable evaluation period. The evaluation period may take up to sixteen (16) months.

1.5 Equipment Procurement

Any ordering of equipment/material before the approval of the PIDS CCTV system design report will be undertaken at the contractor's own risk. The Design Authority may authorize the procurement of certain long lead items at, or shortly after a preliminary design review of the proposed system.

1.6 Quantity of Equipment

The quantity and location of the PIDS CCTV equipment required for CSC institutions will be contained in the specification identified in the Statement of Technical Requirements (STR).

2.0 APPLICABLE DOCUMENTS

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

ES/SOW-0101	Statement of Work for Procurement and Installation of Electronic Systems
ES/SOW-0102	Statement of Work for Quality Control of Electronic Systems Installations
ES/SPEC-0400	Specification for Perimeter Intrusion Detection Systems
ES/SPEC-0401	Specification for Perimeter Intrusion Detection System Integration Units
ES/SPEC-0403	Specification for Perimeter Intrusion Detection System Video Switchers
ES/SPEC-0404	Specification for Motion Detection Systems
ES/SPEC-0405	Specification for Fence Disturbance Detection Systems
ES/STD-0202	Standard for Monochrome, CCD Cameras
ES/STD-0204	Standard for Fixed/Zoom Lens
ES/STD-0205	Standard for Outdoor Enclosures
ES/STD-0211	Standard for Time Lapse Video Cassette Recorders
ES/STD-0212	Standard for Monochrome Video Monitors
EIA-310-C	Electronic Industry Association Standard for Racks, Panels and Associated Equipment

3.0 REQUIREMENTS

3.1 General

The contractor shall design, supply, install, test and provide documentation and training for a PIDS CCTV system in accordance with the Specifications, Standards and Statement of Works specified in Section 2.0 of this specification.

3.1.1 System Configuration

The PIDS CCTV system shall consist of the elements in the quantities given in the STR. The system shall be of a modular design and it shall be possible at a future date to add more associated CCTV equipment to the basic installed complement without replacing the existing hardware.

3.1.2 Period of Operation

The PIDS CCTV system and all associated equipment shall be rated for and capable of 24 hours per day, seven days per week operation. Components of the system located outdoors shall be designed to operate over the range of temperature, wind, precipitation and humidity conditions expected on the site and as noted in this specification.

3.2 System Requirements

3.2.1 Camera Siting

The CCTV PIDS camera locations shall be chosen to provide full assessment for all sectors of the perimeter as described in the STR. The perimeter will be divided into zones, nominally two per side, unless the technology of the chosen intrusion alarm systems constrains this assignment.

The Design Authority shall approve the siting of all PIDS CCTV cameras before installation can commence.

3.2.2 Perimeter Lighting

The PIDS CCTV cameras shall meet the requirements as specified in the Standard, ES/STD-0202 for monochrome CCD cameras. The existence of perimeter illumination levels less than the specified camera light sensitivity level, uneven distribution of light, or any other related lighting problems shall be identified to the Design Authority prior to system design.

3.2.3 Camera Mounting

Cameras and enclosures shall be mounted with sufficient height to ensure a clear view of the observed sector with minimal reduction of see-through ability by fence mounted wire fixtures at the extremes of the sector under observation. Camera mounting designs for guard towers and/or institution structures must be submitted to and approved by the Design Authority.

3.2.4 Tower and Camera Stability

All PIDS CCTV cameras mounted on camera towers shall be mounted such that under worst case wind conditions, i.e., 100 km/hour, the video displacement as viewed on a monitor shall not exceed five TV Lines.

3.2.5 Anti-Climbing Devices/Maintenance Foot Stand

Camera towers shall be equipped with climbing fixtures above the 3.1 m (10.0 ft.) level only. Where the contractor supplies an open structure tower, anti-climbing fixtures shall be attached from the 2.5 m (8.0 ft.) to 3.1 m (10.0 ft.) of the tower. If an open tower is provided, and it is necessary to provide visibility through the lower part then anti-climbing fixtures must be attached to the tower beginning at the 2.5 m (8.0 ft.) level. Anti-climbing devices must also be included inside the tower to prevent climbing through the center.

Camera towers shall be equipped with two (2) foot stands to provide a stable platform for maintenance personnel when working on either side of the camera. Safety harness hook up ring bolts shall be properly located at belt level when standing on the maintenance foot stands.

3.2.6 Interchangeability

Cameras, mounts, monitors and associated equipment shall be readily interchangeable wherever possible. All major components shall be of modular plug-in design.

3.2.7 Facilities

Power is available for this system at each institution through the internal wiring of the emergency power system on site.

3.2.8 Emergency System Start-Up

The emergency system consists of a diesel-powered generator with controls which sense commercial power failure and initiate diesel start-up. The elapse time to emergency power following mains (domestic) failure is typically 20 seconds.

Following a switch over to emergency power, and/or a return to commercial power from an emergency, the CCTV System shall revert automatically to normal service status.

The Design Authority will identify the locations of the emergency VAC power source in the STR.

The contractor shall be responsible for connecting all cameras, enclosures, and associated outdoor CCTV equipment to the institution's emergency VAC power supply. Each camera location, including the enclosure, shall be provided with its own circuit breaker.

Control of power to cameras and enclosures shall be exercised from the MCCP console via relay, small switches, and Class II circuits. The control switches shall be located inside the MCCP console, accessed from the back of the console.

The contractor shall provide the status of camera power on/off switches with form C contact closures to the PIDS Integration Unit (PIU).

3.2.9 **Wiper Control**

Control of camera enclosure wipers shall be exercised from the front panel of the MCCP console. The CCTV wiper control interface shall be capable of accepting a Form C contact closure to control each wiper.

3.2.10 **Wires, Cables, Conduits, Ducts**

The contractor shall 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 shall be performed in accordance with ES/SOW-0102, Statement of Work and all applicable national, provincial, and local electrical codes.

A wiring diagram shall 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 Government Furnished Equipment (GFE) or 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 STR.

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.

3.2.11 **Control Equipment**

The maximum feasible amount of common control equipment (power supplies, logic boards, amplifiers, etc.) shall be located in the Common Equipment Room (CER) provided for the purpose. These areas will be identified in the STR. It is preferred that only equipment which the operator must access directly should be located in the Control Posts.

3.2.12 Interface to Time Lapse Video Cassette Recorder

The contractor shall supply and install all necessary wiring and control equipment required to interface the PIDS CCTV system to the Time Lapse VCR described in ES/STD-0211, Standard.

3.3 Design Requirements

3.3.1 General

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

A design objective is to minimize the number of wires required between all elements of the system.

A space-diversity approach to system planning shall be employed to ensure that loss of one interconnection routing does not impair the operational capability of the complete system.

3.3.2 CCTV Cameras

The PIDS CCTV cameras shall meet all the technical requirements as specified in Standard, ES/STD-0202. The contractor shall be responsible for mounting all cameras on camera towers, guard towers and/or buildings.

With many cameras being used simultaneously, an external synchronization source shall be provided to genlock all cameras to the same sync source to prevent video roll or jitter on the monitor during video switching.

3.3.3 CCTV Monitors

The PIDS CCTV monitors shall meet all the technical requirements as specified in Standard, ES/STD-0212. The contractor shall be responsible for mounting these monitors either in the MCCP console or on the walls or ceiling in the MCCP. Wall and/or ceiling mounting structure shall be the responsibility of the CCTV contractor and shall be approved by the Design Authority. The requirement for ceiling and/or wall mounted monitors shall be included in the STR.

3.3.4 Camera Enclosures

The PIDS CCTV camera outdoor enclosures shall meet all the technical requirements as specified in the Standard, ES/STD-0205. The contractor shall be responsible for mounting all camera enclosures on camera towers, guard towers and/or buildings.

3.3.5 **Camera Lenses**

The PIDS CCTV camera lenses shall meet all the technical requirements as specified in Standard, ES/STD-0204. The contractor shall be responsible for mounting all cameras lenses on the cameras.

3.3.6 **Time Lapse Video Cassette Recorders**

The PIDS Timer Lapse VCRs shall meet all the technical requirements as specified in Standard, ES/STD-0211. The contractor shall be responsible for providing and installing all VCRs in appropriate VCR racks in the MCCP.

3.3.7 **Video Sequential Switcher**

The Video Switcher for the PIDS CCTV system shall meet all the technical requirements as specified in Specification, ES/SPEC-0403.

3.3.8 **Wiring Supervision**

Wiring shall be supervised in all system modes. An alarm shall occur if any system wiring is cut or shorted to other wires or if the system devices are tampered with by unauthorized people or environmental conditions.

3.3.9 **Sabotage, Tampering and Survivability**

Elements of the system must operate in areas exposed to inmate access and shall have high resistance to damage, destruction, or conversion to other uses (including weapons). All interconnecting service must be secure against tampering or improper eavesdropping interference.

3.3.10 **Power Failure**

When power is returned after a power failure, the system shall resume normal operation without operator action and shall automatically start from a "no-calls-present," cleared condition with no cells disabled.

3.3.11 **System Failure**

A system failure shall be deemed to have occurred when any required video surveillance is not produced or when any required control function cannot be performed.

3.3.12 **Human Factors**

Elements of the system which are used directly by staff or inmates (i.e. control panels, etc.) shall conform with accepted principles of good human factors design.

3.3.13 Control Panels

Mounting space within control posts is usually limited and the problem of determining a suitable equipment mounting location is minimized if the control panels are small. Therefore, the designer should make maximum possible use of control devices which combine two or more functions into a single unit.

3.4 Operational Requirements

3.4.1 System Resolution

Under normal night-time perimeter lighting conditions, specified in paragraph 3.1.4 of this specification, each camera and monitor combination (including interconnecting cable and video switcher identified in paragraph 3.1.8 of this specification) shall retain the camera's resolution rating. The VCR is excluded from this requirement.

3.4.2 Target Resolution

A circular target object measuring 47.8 cm (18.8 in.) in diameter shall be resolved with a minimum of 5 TV Lines when viewed at the farthest extreme of the required field of view (FOV). If the target is to be viewed through one or more layers of fence fabric, the minimum resolution becomes 10 TV Lines.

3.4.3 System Synchronization

The PIDS CCTV system shall be designed such that when the perimeter cameras are connected to the MCCP monitors through the Video Sequential Switcher as specified in the Specification, ES/SPEC-0403, no tearing, rolling or distortion shall be observed on the monitor when sequencing or manually switching from one camera to another.

3.4.4 Video Stability

The video image displayed on each monitor shall be stable, free of roll, jitter and tearing. There shall be no degradation of this requirement when the system operates through a video switcher. There shall be a minimum RF isolation of 40 dB between any pair of video circuits.

3.5 Environmental Requirements

The PIDS CCTV system shall operate over the indoor and outdoor environmental conditions as specified in the Standards and Specifications listed in Section 2.0 if the specification. The contractor may meet these requirements through the use of suitable environmental enclosures.

Any associated CCTV equipment installed outdoors, i.e. video line, amplifiers, sync distribution amplifiers, etc.; which is rated as indoor equipment, shall be installed in heated enclosures.

The contractor shall provide lightning protection on all cables and terminal equipment which are installed indoors and outdoors. Towers and cameras shall be grounded via a buried grounding rod.

3.6 Power Requirements

The PIDS CCTV system shall use VAC power within the limits specified in the Standards and Specifications listed in Section 2.0 of the specification.

3.7 Installation Requirements

The PIDS CCTV system shall be installed at the site in accordance with the ES/SOW-0101, Statement of Work and the ES/SOW-0102, Statement of Work. The installation shall include all necessary labour, wire, cable, camera towers, conduit, trenching, site preparation, power supplies, amplifiers, cameras, lenses, enclosures, monitors, videocassette recorders, and control panels for operation in the institutional environment.

3.8 Documentation Requirements

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

3.9 Support Requirements

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

3.10 Training Requirements

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

4.0 QUALITY ASSURANCE

4.1 General

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

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

5.0 DELIVERY

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

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

6.0 INTERFERENCE

Performance of the PIDS CCTV system shall not be affected by the use of standard electronic equipment used at the institution. Distance limits of standard electronic equipment shall be in accordance with ES/SOW-0101, Statement of Work.

7.0 SAFETY

All PIDS CCTV system electrically powered elements shall meet the applicable Canadian Safety Association (CSA) standards.

Correctional Service Canada
Technical Services Branch
Electronics Systems

ES/SOW-0101
Revision 3
15 April 2004

ELECTRONICS ENGINEERING STATEMENT OF WORK

PROCUREMENT & INSTALLATION OF ELECTRONIC SECURITY SYSTEMS

AUTHORITY

This Statement of Work is approved by Correctional Service Canada for the procurement and installation of all telecommunications and electronic security systems, subsystems, and equipment in Canadian penal institutions.

Recommended corrections, additions or deletions should be addressed to the Design Authority at the following address: Director, Engineering Services, Correctional Service of Canada, 340 Laurier Avenue West, Ottawa, Ontario, K1A 0P9

Prepared by:

Manager,
Electronics Systems Research

Approved by:

Director,
Engineering Services

15 Apr 04

RECORD OF REVISIONS

Revision	Paragraph	Comment
3	10.1 – Manuals and Drawings	Added equipment operating software
	10.4 – Documentation Format	Added equipment operating software

TABLE OF CONTENTS

ABBREVIATIONS

The following abbreviations are used in this specification:

ATP	Acceptance Test Plan
CM	Corrective Maintenance
COTS	Commercial-Off-The-Shelf
CSC	Correctional Service Canada
DA	Design Authority
DCR	Design Change Request
DES	Director, Engineering Services
DL	Deficiency List
FDR	Final Design Report
MRT	Mean Response Time
MTBF	Mean Time Between Failures
MTTR	Mean Time To Repair
PDR	Preliminary Design Report
PM	Preventative Maintenance
PW&GSC	Public Works & Government Services Canada
QA	Quality Assurance
RFP	Request For Proposal
SOW	Statement of Work
STR	Statement of Technical Requirement

DEFINITIONS

The following definitions are used in this specification:

Design Authority	Director, Engineering Services (DES) - Correctional Service 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.

1.0 INTRODUCTION

This Statement of Work (SOW) defines the work and responsibilities for the design, procurement, installation, test and integration of all telecommunications and electronic security equipment in CSC Institutions.

The SOW provides guidelines, procedures and responsibilities to the contractor and/or the project officer for the implementation of all telecommunications and electronic security systems in CSC facilities.

All work performed shall adhere to this SOW, CSC Specifications, Standards and Statement of Technical Requirements (STRs).

1.1 Commercial-Off-The-Shelf Equipment

The contractor shall use commercial off-the-shelf (COTS) equipment and proven designs to the maximum extent possible. All new equipment shall meet the specified lifespan requirements. New equipment designs shall be restricted to unique interfaces and common control console.

1.2 Technical Acceptability

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. 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 shall maintain very high standards of dependability and reliability.

The CSC 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.

The technical acceptance process shall involve system and subsystem evaluation in accordance with the applicable CSC specifications in one of CSC facilities or may be tested in a CSC facility to verify the effectiveness of the proposed technologies when subjected to the restrictive operational environment.

CSC shall also verify in depth any of the system technical specifications called up. CSC may when it deems necessary, request the supplier to arrange for a full site demonstration. 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.
It is the supplier's responsibility to make new developments in products available to CSC for evaluation. Equipment qualification is an ongoing process and can be initiated at any time by a vendor. Any vendor can have access to the CSC specifications and standards. Any new development or products should be submitted to the CSC Engineering Services Division, Technical Authority in a suitable time frame prior to any tendering process to allow for an acceptable evaluation period. The evaluation period may take up to sixteen (16) months.

1.3 Equipment Procurement

Any ordering of equipment/material before the approval of the final design report will be undertaken at the contractor's own risk. The Design Authority may authorize the procurement of certain long lead items at, or shortly after the preliminary design review.

1.4 Quantity of Equipment

The quantity and location of the equipment required for CSC institutions will be contained in the specification identified in the STR.

2.0 APPLICABLE DOCUMENTS

CSC Specifications, Standards and STRs are approved by the Director of Engineering Services (DES) for the procurement and installation of all telecommunications and electronic security systems in all CSC facilities. These documents promulgate DES policy and shall not be modified or changed without prior consultation and approval of the Director. The documents of the issue in effect will form part of the Request for Proposal (RFP) issued by the contract authority.

3.0 REQUIREMENTS

3.1 The contractor shall:

a. Design, procure or manufacture, install, test and document the installation of all electronic security and telecommunications systems in accordance with the CSC specifications, standards and STR;

b. Provide the operator and maintenance training in accordance with the CSC requirements;

c. Provide the maintenance support and spares in accordance with the CSC maintenance requirements;

d. Provide quality assurance (QA) to ensure equipment performance and reliability are in accordance to CSC requirements;

e. Provide warranty coverage to include spare parts provision and equipment repair;

f. Provide a program schedule to show all major elements from a contact award to completion of the warranty period and shall include anticipated time of occurrence, interrelationships between events, and time scale; and

g. Be responsible for the integration of the proposed system to any existing telecommunications and electronic security systems.

h. Provide a lightning protection system for the installation of all electronic security systems/equipment in the CSC facilities. As a minimum, surge suppression type lightning arrestors shall be required for all power, communications and antenna cables/wires entering or leaving a building.

4.0 SYSTEM DEVELOPMENT

The contractor shall design systems and equipment to meet all of the requirements stipulated in the applicable CSC specifications. The system design shall be modular and address the following criteria:

a. ease of operation and maintenance;

b. optimize and concentrate control functions and capabilities;

c. enhance the security of the working environment, extend staff capabilities to observe and control; and

d. minimize the number and types of display and control devices.

4.1 Preliminary Design

The preliminary design baseline shall be established by the review and approval of the preliminary design report (PDR) by the Design Authority (DA) or his designate. Specifications, drawings and the approved PDR shall make up the preliminary design baseline.

The contractor shall prepare and submit two (2) copies of the PDR to the Design Authority and one (1) copy to the Contract Authority at least ten (10) days prior to the PDR meeting. The PDR shall consist of:

a. performance specifications with functional block diagrams of the proposed system. The technical analysis and equipment performance data shall verify system requirements;

b. preliminary equipment layouts including control consoles and racks;

c. list of off-the-shelf equipment with part number, model number, manufacturer and the quantity of each item;

d. list of custom designed equipment with model number and the quantity of each item;

e. functional schematics for all custom designed equipment;

f. conceptual drawings for all custom designed equipment;

g. a proposed product assurance plan;

h. a proposed maintenance plan;

l. proposed sparing plan; and

j. proposed training plan.

4.2 **Preliminary Design Review**

The PDR meeting shall be convened by the contractor to review the PDR contents. The contractor shall provide the venue and all of the necessary facilities. The Design Authority will identify any portions of the PDR that are not acceptable to CSC.

4.3 **Final Design**

The final design baseline shall be established by the review and approval of the Design Authority of the final design report (FDR). It establishes the start of change control in equipment design and performance. The FDR shall consist of:

a. all elements of the preliminary design baseline;

b. control console mockups, ergonomics considerations, etc., as necessary;

c. drawings and operational descriptions for the custom designed equipment including interface specifications;

d. Installation drawings and instructions; and

e. availability model and analysis updates to reflect the final system design and hardware selection.

The FDR shall be prepared to good commercial practice. Two (2) copies shall be submitted to the Design Authority at least ten (10) working days before the FDR meeting.

4.4 **Final Design Review**

The final design review meeting shall be convened to review the contents of the FDR. The contractor shall provide the venue and all of the necessary facilities. All of the contractor's staff responsible for the system/equipment engineering shall be available.

4.5 **Design Change Control**

Design changes shall be in accordance with the following procedure:

4.5.1 **Type I.** Changes that affect cost, schedule, reliability, maintainability, or availability shall be submitted as a design change request (DCR).

Changes shall not be actioned until specifically directed in writing by the Design Authority through the Contract Authority.

4.5.2 **Type II.** Changes to correct a design error without affecting cost, schedule, reliability, maintainability, or availability shall not require a DCR.

Changes shall be reported to the Design Authority and the final design baseline shall be updated by the contractor. The Design Authority will review and acknowledge the change.

4.6 Design Change Request (DCR)

Type I changes shall be forwarded to the Design Authority through the Contract Authority on DCRs initiated by either the contractor or the Design Authority.

DCRs shall be reviewed and approved before implementation and shall include:

a. specification requirement being effected;

b. final design baseline element being changed;

c. description of the design change;

d. reason for the change;

e. impact on cost, schedule, reliability, maintainability and availability; and

f. trade-off recommendations.

4.7 In-Plant Testing

Details of in-plant tests are contained in the ES/SOW-0102, Statement of Work. In-plant tests shall be performed according to the Design Authority approved procedures.

Equipment with deficiencies as the result of the in-plant tests shall be subject to retest. The Design Authority reserves the right to add or modify tests.

5.0 SYSTEM INSTALLATION

The contractor shall be responsible for ensuring that sufficient site utilities are available. No work will be permitted at the site before the approval of the Design Authority. All installation activities shall be conducted in accordance with ES/SOW-0102, Statement of Work.

5.1 Schedule

The contractor shall provide a detailed work schedule for the installation activities. This schedule shall reflect the complete implementation plan by identifying the nature of the work to be performed and the area affected.

5.2 On-Site Inspections

Design Authority or an appointed CSC representative shall perform ongoing inspections of the contractor's activities. These inspections shall verify compliance with the project requirements, the quality of work performed and assess the contractor's progress in relation to the approved schedule. Installation deficiencies requiring corrective action will be brought immediately to the contractor's attention in writing.

5.3 On-Site Coordination

Design Authority shall be responsible for the appointment of an on-site CSC representative. This representative will handle all site related manners and will periodically inspect the installation.

When electronic system installations are part of a construction program or a major redevelopment that involves Public Works & Government Services of Canada, the electronic system installation contractor shall coordinate all activities with the relevant site manager and shall comply with this SOW.

5.4 Facility Criteria

The contractor shall provide the facility criteria data in the proposal. Details as to the power, cooling, space and/or other requirements relating to electronic security system installation at the site must be provided. Final facility criteria information must be provided as part of the FDR.

5.5 Installation Design

The system installation design and planning shall make maximum use of existing ducts, conduits, and other cable routing facilities. Where this is not possible, the contractor shall design and install facilities in a manner acceptable to the Design Authority.

5.6 **Subcontractor Supervision**

The contractor shall provide an on-site supervision of all subcontractors. The subcontractors shall abide by the regulations of this Statement of Work and the conditions in the contract.

5.7 **System Checkout**

Before conducting the formal on-site testing for the CSC acceptance, the contractor shall conduct and document a system checkout to assure the system readiness for formal testing and on-line operations. The test sheets used for the system checkout shall be signed by a company representative and provided to the Design Authority at least seven (7) days prior to the scheduled date of the Acceptance testing. The Design Authority will verify readiness through review of the checkout report. The report may be used as reference during the formal witnessed testing for acceptance.

5.8 **As-Built Drawings**

Thirty (30) days after the system installation acceptance, the contractor shall deliver a complete set of equipment and installation as-built drawings for Design Authority's review and approval. Within thirty (30) days after CSC approval, two (2) complete sets of revised drawings shall be delivered to the Design Authority.

The contractor shall update these drawings throughout the warranty period by the design control procedures. Within thirty (30) days of completion of the warranty period, the contractor shall deliver one (1) set of final revised drawings reflecting all changes to the Design Authority. Upon final CSC approval, the contractor shall deliver two (2) sets of original prints of the final drawings.

6.0 SYSTEM ACCEPTANCE

System acceptance shall occur when the acceptance testing has been completed according to the ES/SOW-0102, Statement of Work and when all of the other requirements of the contract have been completed to the satisfaction of the Design Authority. A final acceptance certificate signed by the Design Authority shall certify the system acceptance.

On-site system acceptance testing shall not begin until all of the on-site iInstallation activities have been completed.

6.1 Acceptance Test Plans (ATPs)

The contractor shall provide ATPs for all system, subsystem and equipment tests for Design Authority review and approval. The requirements for the ATP are detailed in the ES/SOW-0102, Statement of Work.

6.2 System Testing

The contractor shall conduct the approved ATP and record the results. The Design Authority or an appointed CSC representative shall witness the tests.

6.3 Deficiency Lists (DL)

The contractor shall prepare and submit a list of deficiencies divided into three categories:

a. Visual/Mechanical,

b. Operational, and

c. Technical/Functional.

6.4 Technical Acceptance

Upon verifying that all of the deficiencies have been corrected, the Design Authority shall issue a letter of Technical Acceptance.

7.0 QUALITY ASSURANCE (QA)

The QA program shall include quality control and system tests/verification programs to verify that new design and off-the-shelf equipment requirements have been met. System tests/verification will be conducted by the contractor in-plant and on-site, and may be witnessed by the CSC representatives where appropriate. The system shall pass all tests before approval will be given to commence the operator and maintenance training programs and warranty period.

7.1 Quality Control Program

The contractor shall provide a description of their internal quality control programs for CSC review and approval. CSC reserves the right to audit and verify that all materials destined for use in CSC systems have been thoroughly inspected and that QA procedures are applied during production and testing.

7.2 System Test Program

The contractor shall prepare and provide the documents describing: number, type and details of equipment, subsystem and system tests for CSC review and approval. These documents must be approved before any formal testing and will consist of the following:

7.2.1 System Test Plan.

This plan shall contain the test philosophy, the tests to be conducted, the pass-fail criteria, the retest requirements, and the instructions for the validation and the sign-off of all final design baseline requirements.

Before witnessing these tests, the CSC representative will perform a visual and mechanical inspection to ensure that the system installation meets the requirements of ES/SOW-0102, Statement of Work.

7.2.2 Test Procedures. These procedures shall ensure that:

a. all equipment supplied meets the performance specification;

b. each subsystem meets the applicable performance requirements; and

c. the overall system meets the performance requirements.

d. test procedure contains the step sequence for each test to be conducted, and the expected results.

7.2.3 **Contractor Testing.**

All tests are conducted by the contractor and may be witnessed by an appointed CSC representative. Tests are conducted as stipulated in the approved plan and procedures. The contractor shall inform CSC at least five (5) working days before the test start date.

7.2.4 **Test Reports.**

The contractor shall submit final copies of the test results for CSC review and approval within ten (10) working days of the completion of the testing. Two copies of the report shall be submitted and shall include:

a. a summary description of the tests;

b. test results consisting of completed test procedures verified by a CSC representative;

c. incident reports, including analysis and corrective action; and

d. results of any retest.

8.0 TRAINING

The contractor shall develop, document and conduct training for both the operational and the technical staff. The training shall be conducted on-site at the institution in the period designated by the schedule.

8.1 Classroom Training

Classroom lectures and demonstrations will be conducted on-site to train operations staff in the use and technical personnel in the maintenance of the systems.

8.2 Training Documentation

The contractor shall develop and deliver a complete training plan to the Design Authority for comments and approval. This plan must be submitted to CSC at least thirty (30) days in advance of the training date to allow for CSC review. As a minimum, the training material shall contain:

a. training plans for CSC operations trainers and technical personnel;

b. manuals for each student to add notes;

c. training aids; and

d. student materials.

Training material shall be provided in the language that is dominant at the site (French in Quebec). Sufficient copies of all student materials shall be provided by the contractor at the beginning of the training course to assure one copy for each student. CSC shall stipulate the number of staffs who are to be trained. Upon approval by the Design Authority, two (2) copies of all material shall be delivered to CSC.

9.0 MAINTENANCE and SPARES

The contractor shall provide maintenance and spares support plans according to the ES/SOW-0102, Statement of Work for the Design Authority approval. These plans shall be submitted according to the schedule.

9.1 Maintenance Plan

The maintenance plan shall describe the philosophy, the Preventive Maintenance (PM) procedures and schedules, the Corrective Maintenance (CM) methods and response times, Mean-Time-To-Repair (MTTR) for all systems. The plan shall recommend tools, jigs and test equipment, and detail the recommended manning method for the system. Issue of the final maintenance support plan will be contingent on Design Authority approval.

9.2 Spares Plan

The spares plan shall list the required spares and recommended quantities. The quantity recommendations shall be supported by system availability and reliability analysis and available experience data. The bidder shall identify spare parts and components by their original manufacturer's code, cross-referenced to the equipment vendor's part number.

9.3 Spares List

The spares list shall identify the following:

a. the spare parts and the subassemblies with the recommended quantities;

b. the cross-reference listings between the vendors and the original manufacturer's codes;

c. the unit and extended prices for stocking; and

d. the expected life or the annual consumption of each part.

The contractor shall maintain the spares plan through to the end of the warranty period, and shall ensure that any changes because of approved design changes are incorporated in the spares list.

9.4 Test Equipment

The contractor shall provide a list of test equipment required for the on-site maintenance of the system within thirty (30) days from Design Authority's acceptance of the final design.

10.0 DOCUMENTATION

All final documentation in hard-copy format shall be in a 3-ring binder with all foldout pages having reinforced ring holes.

10.1 Manuals and Drawings

The following items make up the final documentation requirements:

a. Operator Manual,

b. Maintenance Manual,

c. Installation As-built Drawings,

d. Equipment As-built Drawings, and

e. Equipment Operating Software.

The contractor shall prepare and submit all manuals and drawings to the Design Authority for review and approval. The manuals and drawings will be approved when all changes have been satisfactorily incorporated. All drawings must be produced with AUTOCAD (latest available version)

10.2 List of Equipment

The contractor shall provide a list of equipment itemizing the location, quantity, model number, serial number and revision level of all installed equipment.

10.3 Baseline Measurements

The contractor shall provide a copy of the final test results. These results will be used as a reference baseline measurement for monitoring system degradation over time.

10.4 Documentation Format

All manuals, documentation including as-built drawings, lists of equipment and baseline measurements shall be submitted as per the following schedule:

- One (1) hard-copy version of all documentation.

- One (1) electronic version of all documentation in a ‘read-only’ format on a 3½ inch diskette medium; suitable for duplication without any special requirements.

- One (1) electronic version of all documentation in a full 'read-write' format to serve as a master of the documents and drawings.

- all software requirements to access the electronic versions of the documentation.

- One (1) CD containing the equipment operating software.

10.5 **Operator Manuals**

The contractor shall provide CSC approved manuals to support the operation of the system in the format as outlined in section 10.4 of this specification. These manuals shall be prepared to the best commercial standards. Photo copies shall not be accepted. All hard-copy versions shall be on paper stock 8 ½" x 11" and shall be presented in a 3-ring binder. The manuals shall comply with the following format and content requirements:

a. title page;

b. revision notice page, lined, with columns for revision numbers, dates and initials;

c. table of contents;

d. warnings and cautions;

e. introduction - general information including a description of equipment or system and summary of capabilities;

f. theory of operation including an explanation of all major system components;

g. detailed description and use of all user accessible computer screens; and

h. block diagrams.

A hard copy draft version of the manual(s) shall be submitted for CSC approval on or before the date given in the schedule. Upon acceptance and approval by the Design Authority, a total of two copies shall be provided for use during the warranty period. The contractor shall update these manuals through the warranty period and provide revision bulletins to record manufacturers' recommended modifications, etc. during the life of the equipment.

Within thirty (30) days of the warranty expiry date the contractor shall submit one (1) set of final, updated manuals for CSC approval. Following the final CSC approval, the required number of sets of operator manuals shall be delivered to the Design Authority in the format as specified in section 10.4 of this Statement of Work.

10.6 **Maintenance Manuals**

The contractor shall provide CSC approved manuals to support the maintenance of the system in the format as outlined in section 10.4 of this specification. These manuals shall be prepared to the best commercial standards. Photo copies shall not be accepted. All hard-copy versions shall be on paper stock 8 ½" x 11" and shall be presented in a 3-ring binder. The manuals shall comply with the following format and content requirements:

a. title page;

b. warranty page - explaining the warranty period and expiry dates;

c. revision notice page, lined, with columns for revision numbers, dates and initials;

d. table of contents;

e. introduction - general information including a full description of equipment or system, technical summary, specifications and detailed block diagrams;

f. theory of operation including a detailed explanation of all circuits and parts;

g. alignment and test procedures;

h. repair procedures including step by step fault finding or fault localizing;

I. block diagrams;

j. circuit schematics (clear, easy to read, foldout type);

k. complete parts list;

l. mechanical drawings, chassis layout illustrations and wiring data lists; and

m. drawings including as-built and as-installed drawings.

A hard copy draft version of the manual(s) shall be submitted for CSC approval on or before the date given in the schedule. Upon acceptance and approval by the Design Authority, a total of two copies shall be provided for use during the warranty period. The contractor shall update these manuals through the warranty period and provide revision bulletins to record manufacturers' recommended modifications, etc. during the life of the equipment.

Within thirty (30) days of the warranty expiry date the contractor shall submit one (1) set of final, updated manuals for CSC approval. Following the final CSC approval, the required number of sets of maintenance manuals shall be delivered to the Design Authority in the format as specified in section 10.4 of this Statement of Work.

11.0 PROJECT PROVISIONS

11.1 Monthly Progress Reports

The contractor shall submit monthly progress reports. These reports shall report the activities for the previous period. One (1) copy shall be delivered to the Design Authority and one (1) copy to the Contract Authority by the fifth (5th) day of each month. A review meeting may be required.

Monthly reports shall contain the following:

a. summary of the month's activities;

b. scheduled shortfalls and rescheduled dates;

c. problem areas and proposed solutions;

d. review of next month's activities;

e. summary of meetings held during the month; and

f. cash flow forecast.

11.2 Monthly Review Meetings

Review meetings shall be held at the contractor's premises, Design Authority's office, Contract Authority's office, or the site depending on the need. The contractor shall make the design staff members available upon request by the Design Authority.

11.3 Maintenance Support

During the training period, the contractor shall provide maintenance support. This support is expected to be not less than on-site coverage during the normal working day.

11.4 **Shipment and Delivery**

Contractor shall be responsible for the shipment and delivery of equipment and materials to the site. Packing, crating, and shipment of equipment shall be to good commercial practice, and any damage to, or loss of equipment shall be repaired or replaced to the satisfaction of CSC. The contractor must properly label all shipments to assure correct identification and disposition on arrival at the site, as specified in ES/SOW-0102, Statement of Work.

12.0 SYSTEM AVAILABILITY

All elements of customed and off-the-shelf equipment shall be designed to operate in a highly reliable fashion, consistent with available technology, with a minimum of system downtime due to scheduled and unscheduled maintenance. System availability will be achieved when each of the included subsystems availabilities have been proved as required.

12.1 Common Facilities

Where units or subsystems are integrated into common facilities no single failure of a component, assembly subassembly, or subsystem shall result in the failure of any other subsystem; nor result in reduced capacity or quality of performance of other subsystems or parts of it.

12.2 Single Point of Failure

The system shall be designed such that no failure of a single component, unit, subassembly or subsystem will result in failure of the next higher hierarchical elements of that subsystem or the system.

12.3 Availability Model

The bidder's technical proposal shall include a complete model and analysis of the availability of each subsystem and of the complete system being offered. This analysis shall include both MTBF and MTTR calculations and shall treat the Mean-Response-Time (MRT) as zero. This availability analysis may be based on either:

a. summation of failure rates of the individual components; or

b. the bidder's documented experience with the same equipment operating in a similar physical environment.

In either case, the source of all failure-rate shall be clearly shown.

The contractor shall maintain the availability model and analysis up-to-date throughout the contract period. A statement of impact of the proposed change would have on the availability model and analysis shall be submitted with all Type I DCRs.

12.4 Availability

Availability is the probability that the system, or subsystem will meet operational performance requirements at all time. Time includes the operating time, the active repair time and the administrative and logistic time. To calculate this availability, the contractor must include all of the pertinent factors such as:

12.4.1 **Mean Time Between Failure (MTBF)**.

The total operating time of the equipment divided by the total number of failures of that equipment.

12.4.2 **Mean Time To Repair (MTTR).**

The repair time divided by the number of failures.

12.4.3 **Mean Response Time (MRT).**

The time to respond to a call for service divided by the number of calls.

12.5 **Expected Life Duration**

This is the time during which the equipment is expected to provide useful service, without an unusual amount of service and without becoming obsolete.

13.0 INTERFERENCE

13.1 Interference to the System

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

13.1.1 CB transceivers at 1 metre or more;

13.1.2 VHF and UHF transceivers at 1 metre or more;

13.1.3 Other radio frequency transmitting, receiving and re-distribution equipment at 5 metres or more; and

13.1.4 Personal computer and/or computer work stations at 5 metres or more.

13.2 Interference by the System

The system shall not interfere with any standard electronic equipment used at the institution, any commercial TV or radio equipment at a minimum distance of 5 metres, or any other electronic security systems at a distance of 1 metre or more.

14.0 LIGHTNING PROTECTION

Surge suppression-type lightning arrestors shall be installed to protect all power, communications and antenna cables or wires entering or leaving a building.

These arrestors must be installed where the cable enters the building i.e. not in the CER or other equipment room.

Correctional Service Canada
Technical Services Branch
Electronics Systems

ES/SOW-0102
Revision 6
1 May, 2008

ELECTRONICS ENGINEERING STATEMENT OF WORK

QUALITY CONTROL FOR PROCUREMENT AND INSTALLATIONS OF ELECTRONIC SECURITY SYSTEMS

AUTHORITY

This Statement of Work is approved by Correctional Service Canada for the procurement and installation of all telecommunications and electronic security systems, subsystems, and equipment in Canadian penal institutions.

Recommended corrections, additions or deletions should be addressed to the Design Authority at the following address: Director, Engineering Services, Correctional Service Canada, 340 Laurier Avenue West, Ottawa, Ontario, K1A 0P9

Prepared by:

Manager,
Electronics Systems Research

Approved by:

Director,
Engineering Services
18 Aug 06

RECORD OF REVISIONS

Revision	Paragraph	Comment
3	5.1 - Design Considerations	Tabletop or wall mount power supplies/transformers
4	3.1.1 - Wiring/Cabling Methods	Wiring/cable access
	3.2.1 - AC Wiring	Power outlet strip
		Separate circuit breakers connected to opposite phases of the AC feed
	3.2.2 - AC Power Connections	Power connections via flexible armoured cable
5	Abbreviations	Additions
	1.4 – Manufactured Equipment	Approval of custom equipment
	1.5 – Commonality of Equipment	Add security screws
	3.1.1 – Wiring and cabling	Single conductor wire only on IDC connectors
		Identification of conductors
	3.1.2 – Cable/Wiring Labelling	Acceptable labelling
	3.2.1 – AC Wiring	Mounting of power strips
	3.3.4 - Labelling	Acceptable labelling of racks, boxes, etc.
	5.1 – Design Considerations	DIN rail power supplies preferred
6	2.1 – Environmental Conditions	Expand airborne containments
	2.6 – Finish Application	Change finish material definition
	2.2.2 - Plastic	Remove last sentence
	3.1.1 – Wiring/Cabling Methods	Change “Hydro Codes” to “Electrical Authority”
	3.3.2 - Enclosures	Add requirement to meet IP64

TABLE OF CONTENTS

ABBREVIATIONS

The following abbreviations are used in this specification:

AC	Alternating Current
ATP	Acceptance Test Procedure
BER	Beyond economical repair (repair cost in excess of 60% of replacement cost)
CER	Common Equipment Room
COTS	Commercial -of-the-Shelf
CSC	Correctional Service Canada
CSA	Canadian Standards Association
DC	Direct Current
DA	Design Authority
DES	Director, Engineering Services
EIA	Electronic Industries Association
EMT	Electrical Metallic Tubing
IDC	Insulation Displacement Connector
ISO	International Standards Organization
PCB	Printed Circuit Board
PVC	Polyvinyl Chloride
QA	Quality Assurance
RFP	Request For Proposal
STR	Statement of Technical Requirements

DEFINITIONS

The following definitions are used in this specification:

Design Authority	Director, Engineering Services (DES), Correctional Service Canada (CSC) is responsible for all technical aspects of the system design and implementation.
Contract Authority	Public Works and Government Service Canada (PW&GSC) and/or the Materiel Management Division of CSC is responsible for all contractual matters associated with the system design and implementation.
Project Manager	A CSC employee and/or a contracted person designated by DES to be responsible for the implementation of the project.
Project Officer	A CSC employee and/or a contracted person designated by DES to provide technical and/or engineering services in support of the project.
Contractor	The company selected as the successful bidder.
Off-the-shelf	Equipment which is commercially, complete with field reliability data, manuals, engineering drawings and parts price list.
Custom Equipment	Equipment designed and/or manufactured specifically for a specific contract.

APPLICABLE DOCUMENTS

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

CSA STANDARD C22.1-1986	Canadian Electrical Code - Part 1 Safety Standard for Electrical Installations
EIA STANDARD EIA-310-D	Racks, Panels and Associated Equipment
CSA STANDARD C22.2	Canadian Electrical Code - Part II
EIA RS-406/IPC-C--405A	Connectors, Electric, Printed Wiring Boards

Any other applicable industrial safety and control standards governing specific aspects for equipment and/or installations.

1.0 INTRODUCTION

1.1 General

This document defines the quality control requirements for the design, installation, testing and acceptance of telecommunications and electronic security systems in all Correctional Service Canada (CSC) facilities.

1.2 Scope

This specification has been developed to ensure high standards for the installation of electronic systems. It defines workmanship standards which may not be fully covered in subsidiary specifications. All contractor's documentation and installation procedures shall meet this specification for equipment reliability, maintainability, longevity, appearance and operational use.

1.3 Off-The-Shelf Equipment

The contractor shall provide commercial off-the-shelf (COTS) equipment wherever possible. COTS equipment shall meet or exceed the manufacturing standards as listed in this specification.

1.4 Manufactured Equipment

Where COTS equipment is unavailable or unsuitable for a specific application, the contractor may manufacture or arrange for the manufacturing of a particular item to suit the requirements. Manufactured equipment shall meet or exceed the best commercial equipment manufacturing standards. Approval of the final design, appearance and ergonomics of all custom manufactured equipment shall rest with the DES, Project Manager or CSC delegate.

1.5 Commonality of Equipment

The contractor shall provide commonality of hardware components within the design parameters ie. switch locks, racks, panels, security screws, etc. All equipment, if appropriate shall be interchangeable.

2.0 MATERIAL AND EQUIPMENT REQUIREMENTS

2.1 Environmental Conditions

All materials and equipment which is used in CSC installations shall be equal to, or better than the standards established in the original equipment and shall be chosen with due consideration being given to the intended use, safety, retention of appearance, maintainability and durability under rugged operating conditions. These materials shall be suitable to perform over the following environmental ranges:

a. **Indoor Equipment**

Temperature: 0° C to 40° C; and
Humidity: 20% to 95% non-condensing.

b. **Outdoor Equipment**

Temperature: -40° C to +50° C; and
Humidity: 0 to 100%, condensing.

Outdoor equipment shall operate reliably and not be damaged by combinations of direct exposure to the sun, wind, rain, lightning, hail, snow and ice as may be expected to occur at each institution location.

Complete assemblies of indoor equipment shall be resistant to liquid spills, airborne contaminants (dust, pollen and water droplets), shock and vibration.

2.2 Materials

2.2.1 Metals

Metals used shall be either corrosion resistant or be suitably treated to resist corrosion in all potential atmospheric conditions, including tear gas, to which the installation may be subjected.

For the connection of copper to a cadmium or galvanized surface, effective "wiping" of the copper surface shall be considered satisfactory protection.

No cut galvanized fitting shall be used without protection equal to or greater than the original galvanized surface. All parts shall be free from burrs and sharp edges.

Metal which has been cut, scraped, or drilled shall be properly treated (primed and painted) to retain a uniform appearance.

2.2.2 **Plastic**

Plastic materials must be stable and shall retain their original shape and finish over the range of operating environmental conditions specified in 2.1

No material shall be used that softens or hardens within the storage environment in a way which is detrimental to its suitability as replacement parts for existing equipment.

Metal screws shall not be threaded into plastic materials.

2.2.3 **Natural Rubber**

The use of natural rubber is prohibited.

2.2.4 **Wood**

The use of wood or wood products is not acceptable.

2.3 **Toxic Materials**

Materials capable of producing harmful toxic effects under any operating condition, equipment malfunction, or accidental cause shall not be used.

2.4 **Flammable Materials**

Materials, used either for electrical insulation or mechanical purposes which are combustible or capable of causing an explosion, shall not be used.

2.5 **Fungus and Insect Supporting Materials**

Materials capable of providing a nutrient medium for fungus or insects shall not be used.

2.6 **Finish Application**

Finish shall be applied to all surfaces where consideration of appearance and protection against corrosion, toxicity, and other deterioration exists.

Application of finish shall not impair equipment performance, and will maintain uniformity in outward appearance.

Finish materials must be scratch resistant, not react to normal cleaning products and applied so as to last at least ten years.

3.0 INSTALLATION REQUIREMENTS

3.1 Wiring and Cabling

Prior to the installation, all wires and cables shall be tested in accordance with the manufacturer's instructions and shall meet all performance parameters.

Wire and cable harnesses shall be neatly formed and clamped in position. If brackets, forms or clamps are required, these shall be the responsibility of the contractor.

All wires and cables shall be stranded. Single conductor type wires are not acceptable except when such cables are specified to terminate on an IDC type connector. This does not apply to coaxial cables with single centre conductors.

Electrical tape, masking tape, or its equivalent shall not be used on wires, cables or any installed equipment.

3.1.1 Wiring/Cabling Methods

Three (3) or more individual wires or cables which are located in one(1) cable run shall be formed into a cable harness, properly dressed, supported and securely tied with flat lacing twine or equivalent.

Wires and cables which are installed by the contractor external to consoles, equipment racks, pull boxes and junction boxes shall be contained in securely mounted conduit or cable tray systems.

Plastic PVC conduits may be used in underground installations unless otherwise specified at time of bidder's conference.

A rigid steel conduit shall be used in indoor, security sensitive areas and outdoor above-ground applications.

Signal and 120 VAC power wiring shall not be run in the same conduit, cable tray, or raceway; and shall be separated in accordance with the local Electrical Authority.

Wire splicing in cable runs shall not be permitted. All cable runs shall be continuous. If continuous cable runs are not possible, terminal block configurations are acceptable provided they are approved by the Design Authority.

Cross-connects installed on BIX. or similar blocks, must not pass across the face of the block, but must be carried around the block, so as not to impede access to the connections.

BIX, or similar, blocks are to be used for solid wire only. Stranded wires are not to be directly terminated on BIX, or other IDC terminations.

Wires in multi-conductor cables which terminate on connectors, and which are not being used, must be twisted around the cable in a neat fashion. They are not to be cut off.

Wires in multi-conductor cables which terminate on BIX or similar IDC connector blocks, and which are not being used, must be punched down on the block. They are not to be cut off.

All conductors on IDC and any other type of terminal block will be identified with a cable marker and cross referenced in the as-built drawings.

Rectangular slots shall be cut in the computer floor, underneath any cabinets, racks, and consoles, for the running of cables. These slots must constitute at least 1/2 of the available floor area. Sharp edges on the computer floor shall be supplied with suitable protection to eliminate possible nicks, tears or wear in cable insulation sheaths. Individually drilled holes for the purpose of carrying cables from the under floor to the inside of the cabinet, rack or enclosure are not permitted.

3.1.2 **Cable/Wiring Labelling**

The contractor shall label all cables and cable runs. The labelling method shall be logical and conform to industry standards.

All cables shall be identified with commercially produced or machine printed alpha numeric labels protected by clear heat shrink tubing. Hand printed labels are not acceptable.

All wiring shall be identified at both ends of the wire. The coding shall enable a technician to identify the wire or cable without referring to manual tracing methods, test equipment or as-built drawings.

Cable identification labels shall be attached as follows:

a. within 30 cm of the termination for both ends.

b. in the middle of any access point, i.e. pull box, wall shaft opening, cable tray, etc.

All individual wires shall be labelled according to a cable numbering system or wire function plan, which is acceptable to the Design Authority.

All terminal strips shall be identified with its own unique terminal number and function.

3.1.3 **Exterior Cabling**

Where a cable enters or exits an exterior box, chassis, or conduit, the cable entrance shall be completely sealed to prevent an influx of water. A drip loop shall be formed in the cable to assist in maintaining this weather tight seal.

Conduit bushings shall be used on all conduit entrances/exits.

Sharp edges on metal boxes or chassis enclosures shall be supplied with suitable protection to eliminate possible nicks, tears or wear in cable insulation sheaths.

3.1.4 **Slack**

Wires and cables shall be as short as practical, with sufficient slack to:

a. allow a minimum of three (3) reconnects due to wire breakage;

b. prevent undue stress on cable forms, wires, terminals and connections;

c. enable parts to be removed and replaced during servicing without disconnecting adjoining wires or circuits;

d. facilitate movement of equipment for maintenance purposes; and

e. provide drip loops in exterior cabling.

Slack shall be provided in junction boxes where space permits. Slack shall not exceed one single loop of cable forming the circumference of the junction box.

Slack shall be provided below equipment racks and shall be neatly coiled below the access flooring. The length of slack shall be equal to the height of the associated equipment rack. Units in drawers and slide out racks shall be provided with sufficient slack to permit removing the units without severing connections.

All cross connection wiring shall be neat and tidy, properly bundled, and tied. This procedure shall allow sufficient slack for tracing of individual wires via manual methods.

Parts mounted on a hinged door shall be wired by means of a single cable, and arranged to flex without being damaged by the opening and closing of a door. If physical separation between wires is essential so as to make a single cable impractical, more than one flexible cable may be utilized.

3.1.5 **Terminations**

All terminations relying on friction for electrical and mechanical connection shall be tested in accordance with the manufacturer's instructions and shall meet the performance requirements detailed therein.

Terminal fanning strips shall be used where a number of wires are contained in a harness, shall be used unless a multi-pin connector is provided.

Spade terminal lugs shall be used on all wiring, connections to screw-thread terminals, except where solder or other type of terminal is specified.

Where wires are connected to lugs, which are clamped under screw terminals in the form of a terminal connection strip, no more than one wire shall be attached to each lug, in order that each wire may be removed individually. This requirement will not apply in the case of common connections, daisy chain distribution circuits, or similar terminations where wires will not need to be disconnected for servicing.

No more than two (2) lugs shall be attached to each terminal.

Wire and cable insulation shall be stripped back to allow for proper connection to the lug. No bare wire shall be visible between the terminal lug and the insulator.

Terminal strips must be fastened to a hard surface using a screw, or nut and bolt. Adhesive supports to secure the terminal strip, or floating terminal strips are not acceptable.

3.1.6 **Splicing and Joining**

Splicing of wires on new installations is not permitted.

Where connectors are used on cable assemblies, they shall be a locking type which will not disengage under tension.

All joints or splices in underground cable runs shall be located inside accessible, secure, waterproof, and lockable steel enclosures. The enclosures shall be located at least one (1) metre above grade and be firmly secured to existing structures or to stub pole supports.

Splices in underground cable runs, if required to repair Crown caused damage, shall be subject to approval from the Design Authority.

Stranded conductor splices shall be held by wire binding terminals in order to prevent stray strands from causing either short circuits or grounds.

Joints and splices shall be soldered and encased in waterproof shrink tubing for protection against leaching, oxidization, moisture damage, etc.

Joints and splices shall be clearly and accurately identified on applicable as-built drawings.

3.1.7 **Shielding**

Shielding shall be secured on wires and cables to prevent accidental contacting or shorting exposed current-carrying parts, grounded metal objects, or structures.

Shielding shall terminate at sufficient distance from the exposed conductors of the cable to prevent shorting or arcing between the cable conductor and the shielding.

Ends of the shielding material shall be secured against fraying.

3.1.8 **Protection**

Wires and cables shall be strategically located and protected to avoid contact with rough, irregular surfaces or sharp edges.

Wires and cables shall be protected by suitable grommets or bushings when passing through openings in metal.

Guards or other suitable protection shall be provided on insulated high voltage cables.

3.1.9 **Support**

Wires and cables shall be properly supported with adequate strain relief to prevent excessive strain on the connections, devices, or joints of any electrical apparatus connected therein.

Adhesive supports with ty-wrap products shall not be used unless they are secured by a nut and bolt device.

3.1.10 **Clearance**

Physical clearance between wires/cables and associated heat emitting parts, i.e. amplifiers, shall be sufficient to prevent deterioration of the wires or cables. Refer to Table 19 of CSA Standard C22.1 Part 1.

3.1.11 **Inductive and Capacitive Effects**

Wires and cables, including harness wire and cables, shall be located such that inductive and capacitive effects do not adversely affect system operation. The amount of twists in paired wires shall be increased over the length of wire not covered by the cable sheath.

3.2 **Power Wiring**

The contractor shall not employ "Marette" (TM) type connectors regardless of CSA Standard C22.1 regulations. All wiring shall terminate on an insulated or protected barrier strip or terminal board, and be provided with spade terminal lugs where required.

Where control and signal wires which are run in conduit, cable-harness, or cable-trough systems, shall be run in separate wire ways. The separation shall be a physical barrier of suitable material and shall conform to applicable building codes and wiring methods.

All high voltage and/or high current terminations shall be provided with protective guard devices by the contractor. The device shall be mounted to allow for maintenance access to the terminals.

Terminal lugs shall be used on all power wiring, both VAC and VDC.

Warning labels must be installed in accordance with the CSA guidelines to warn maintenance personnel of any hazardous voltages and currents.

3.2.1 **AC Wiring**

AC wiring methods shall conform to all local and national wiring regulations.

Outlet boxes shall be installed such that all outlets are clear of any obstructions including wiring and cabling, and shall be easily accessible.

Power distribution within a cabinet or rack shall be via a power outlet strip, as provided by the original cabinet or rack manufacturer. A third party outlet strip is not acceptable. All power strips must be mounted into the equipment cabinet with rack mounting hardware.

All power cable installations shall be completed in a neat and sturdy fashion and shall meet all requirements of the specifications detailed herein.

Power cords within equipment cabinets and racks shall be maintained as short as practicable with due consideration for maintenance needs.

Systems which use redundant equipment, such as dual microprocessors, shall power each unit from two separate breakers connected to opposite phases of the AC feed.

3.2.2 **AC Power Connections**

All AC power connections from the cabinet or rack power outlet strip to the AC junction box shall be via flexible armoured cable. AC power connectors are not permitted.

3.3 **Conduits, Enclosures, Cable Troughs and Raceways**

3.3.1 **Conduits**

Conduits installed above ground, and accessible to the inmate population, shall be rigid steel.

Metal conduits installed in secure and inmate accessible areas shall be fitted with double the normal quantity of support hangars.

In locations subject to extreme temperature changes, and/or where conduit lengths are of non-standard size, the contractor shall make provisions for the inclusion of conduit expansion joints.

Rigid PVC conduits shall be used only in buried applications.

Rigid PVC conduits shall not be threaded, but may be used with approved adapters and couplings applied in a manner consistent with industry standards.

EMT conduit may be used in administrative areas, and locations which are not normally assessable to the inmate population.

Liquid-tight flexible metal conduits may be used where a flexible connection is required, i.e. cameras, microwave dishes, etc. In such applications, the length of "flex" conduit shall not exceed one (1) metre.

PVC conduits which cross roadways shall be encased in poured concrete.

The contractor shall provide a suitable means of protecting the buried conduit against damage caused by digging or excavating. The preferred method is installing a tape marker directly above the conduit path.

In addition to these requirements, the applicable industrial standards apply, including:

a. CSA Standard C22.2 No. 45-M1981 - Rigid Metal Conduit

b. CSA Standard C22.2 No. 56-1977 - Flexible Metal Conduit

3.3.2 **Enclosures**

All electrical connections, terminations, and cross connections shall be made within lockable, covered steel enclosures, using good quality locks. At least two keys must be supplied to CSC.

Outdoor enclosures shall be environmentally sealed and gasketed to provide a moisture/dust free and secure environment.

Enclosures which contain electrical equipment such as circuit breakers, relays, switches, and transformers, or cable networks, connections and terminations, shall be weatherproof and dust-tight and meet the provisions of IP64.

All enclosures such as junction boxes, racks and consoles shall be positioned for ease of maintenance, service, and connection/disconnection of cables and cable harnesses.

The contractor shall provide a proper drain hole in all enclosures which are grouted in concrete.

All floor mounted cabinets, racks, and consoles shall be secured to prevent overturning when associated drawers, shelves and movable parts are extended, or when heavy objects are placed on pull out shelves or writing tables.

In addition to the provisions stated herein, the applicable industrial standards shall apply, including:

a. CSA Standard C22.2 No. 29-M1983 for Industrial Products.

b. CSA Standard C22.2 No. 94-1976 for Special Purpose Enclosures.

3.3.3 Cable Troughs and Raceways

Cable troughs and raceways shall be continuous and shall be constructed of metal.

The contractor shall provide adequate mounting devices which will permit the use of fastening devices that will not damage conductor insulation.

Cable troughs, raceways, and fittings shall be free from burrs or other sharp edges which may cause damage to the cable or insulated conductors.

Cable troughs and raceways shall be installed as a complete system before the conductors or cables are installed.

Cable troughs may be either ventilated or solid and unless otherwise specified, shall be equipped with covers and steel guards to protect against damage.

In addition to these provisions, the appropriate standards shall apply, including:

a. CSA Standard C22.2 No. 126-M1980 - Cable Troughs and Fittings.

b. CSA Standard C22.2 No. 79-1978 - Raceways and Fittings.

c. CSA Standard C22.2 No. 62-1972 - Surface Raceways and Fittings.

3.3.4 Labelling

The contractor shall label equipment racks, junction boxes etc. The labelling method shall be logical and conform to industry standards. All equipment racks and junction boxes shall be identified with commercially produced or machine printed alpha numeric labels. Hand printed labels are not acceptable.

Identification of chassis equipment shall be located in a suitable location within the rack and affixed to the rack, not the chassis.

Approved materials used for labels include lamicoyd strip, etched metal, stamped labels, or indelible ink.

3.4 Soldering

On solder connections, the insulation on individual wires shall not be stripped back more than 1.5 mm from the solder area.

Soldering shall be executed so that positive electrical and strong mechanical connections are assured.

Leads shall not be wrapped more than once around the terminal.

Soldered connections on the back of connector plugs, i.e. cannon plugs, switches, relay sockets or any other device employing solder lugs, shall be insulated by means of a short length of insulating tubing placed over each wire in the connector.

"Cold" solder joints, and excessive solder on connections shall not be acceptable.

Each soldered connection shall be tested for mechanical and electrical strength to ensure that a strong connection is achieved.

Use of acid based solder flux is not permitted.

Where insulation material is subject to heating during soldering, the material shall be undamaged and the fastened parts shall not be loosened.

3.5 Welding

All welds shall be free of harmful defects such as cracks, porosity, undercuts, voids and gaps.

There shall be no burn through.

Weld fillets shall be uniform, smooth, and shall cover a sufficient area of the welded surface to ensure that a solid bond is achieved.

Surfaces to be welded shall be free of extraneous particles which may affect the mechanical elements of the welded area.

3.6 Crimping

Crimp connections shall be made in accordance with the manufacturer's instructions. Industry standards shall be observed at all times.

Solid conductors may be used with crimp connections where the use of solid conductor wiring cannot be avoided. In all other cases only stranded wiring shall be used on crimp connections.

Solid conductors which are connected to terminals by crimping shall be soldered as well. This provision only applies to terminal lugs. It does not apply where wires may be spliced by crimping except in the case of some LED's and indicator lights which employ pigtail leads which should be soldered or connected by screw terminals.

3.7 Cleaning

Upon completion of the installation, the equipment shall be cleaned of smudges, loose or excess solder, weld beads, metal chips, burrs, mold release agents, or any other foreign material which might detract from the intended operation, function, or appearance of the equipment.

All corrosive materials shall be removed.

The cleaning processes employed shall leave no harmful residues and shall not have a negative effect on the equipment or its parts.

4.0 GROUNDING REQUIREMENTS

4.1 General

Grounding source and distribution points shall be provided by the Crown unless otherwise specified at the bidder's conference, in the Statement of Technical Requirement (STR), or any applicable documents.

The grounding shall be such that the signal ground, equipment ground, and electrical power ground shall be connected at one point and shall follow the shortest possible path. Where necessary, ground isolation techniques shall be employed.

The path from the tie point to any ground shall be permanent, continuous, have sufficiently low impedance to limit the potential above ground, and facilitate the operation of the 'over current' devices in the circuits.

Ground conductors shall be made of copper, sized for a minimum of 200 circular mils for each 300 mm length of conductor.

Inactive wires installed in long cable or conduit runs shall be grounded to prevent stray or static electrical discharges, with proper consideration given to prevent ground loops or other grounding problems.

Installation must be such that ground loops are prevented.

4.2 Signal Ground

Signal grounds shall be used to provide a ground potential reference which is independent of the frame ground and the power equipment ground.

An insulated grounding conductor shall be connected from the equipment signal ground terminal to the main ground connection point for single units such as equipment racks.
An insulated ground plate shall be used with insulated grounding conductors for multiple units, such as common equipment room (CER) equipment, from each equipment signal ground terminal connected to the plate. The plate shall be connected to the main ground connection point by means of a single insulated grounding conductor.

4.3 **Frame Ground**

The ground connection of the receptacle may be used for the frame ground as long as that ground connection is isolated and insulated from the power equipment ground system. Such receptacles shall be clearly identified so that they will not be used to supply equipment that does not require frame grounds.

The receptacle ground connection conductor shall be insulated and isolated from the power equipment grounding system, and shall be connected from the receptacle ground connection to an isolated ground plate.

The isolated ground plate may be an insulated buss bar for low power applications,.

Size of grounding conductors shall be in accordance with the requirements of CSA Standard C22.1 Section 10 and Table 17.

4.4 **Combined Signal and Frame Ground**

Connection between the signal ground terminal and the frame ground terminal shall be part of the equipment wiring. The connection to the main ground connection point shall be similar to that for a frame ground.

4.5 **Main Ground Connection Point**

Main ground connection point shall be installed in accordance with CSA Standard C22.1 Section 10, and C22.2 No. 41.

4.6 **Ground to Chassis**

Ground connections to an electrically conductive chassis or frame shall be made by:

a. soldering to a spot-welded terminal lug.

b. soldering to a portion of the chassis or frame that has been formed into a soldering lug.

c. using a terminal on the ground wire and securing the terminal by a screw, nut and lockwasher.

When using a terminal on a ground wire which is secured by a screw, nut and lockwasher, the screw shall fit in a tapped hole in the chassis or frame, or it shall be held in a through hole by a nut.

When the chassis or frame is painted, the metal around the screw hole shall be scraped clean and plated (or tinned) to provide a corrosion resistant connection.

4.7 Shielding

Shielding on wire and cable shall be grounded to the chassis or frame, in the manner specified in Section 2.5.5

4.8 Lightning Protection

All equipment with external cabling including radiating cables or other forms of antennas which may be susceptible during lightning strikes or other static discharges shall be protected fully in accordance with the relevant safety rules and regulations.

The ground rod used for lightning protection shall be copper or copper-plated steel, and shall be a minimum of 2.5 metres in length. Where the ground conditions preclude installation of a single ground rod, multiple rods of a shorter length may be used in parallel to provide the lightning protection.

The copper ground conductor shall be fastened to the ground rod using a thermic welding technique. Clamps are not acceptable.

5.0 ELECTRICAL/MECHANICAL DESIGN REQUIREMENTS

5.1 Design Considerations

All equipment shall be manufactured and finished with a degree of uniformity and grade of workmanship which shall comply with applicable industry standards, and the generally accepted principles of safe practice.

Exposed and moving parts that might constitute a safety hazard shall be provided with protective guards and warning labels.

All elements of the equipment shall be designed to operate in a highly reliable fashion, consistent with available technology, with a minimum of system downtime due to scheduled and unscheduled maintenance.

Where units or subsystems are integrated into common facilities, no single failure of a component, sub- assembly, assembly, or sub-system shall result in the failure of any other sub-system or reduced capacity or performance of other sub-systems or parts thereof.

The system shall be designed such that no failure of a single component, unit, subassembly, or subsystem will result in failure of the system or the next higher hierarchical elements.

All equipment shall be designed and installed to provide useful service, with minimal maintenance for a period of no less than 10 years, unless otherwise specified.

Tabletop or wall-mount power supplies or transformers shall not be used to power equipment installed within equipment racks and cabinets. Power supplies or transformers used within racks and cabinets shall be securely fastened to the rack equipment rails or side of the cabinet. DIN rail mounted power supplies are preferred.

5.2 Assemblies

The contractor (or manufacturing agent) shall apply special considerations in the execution of assembling system component parts.

Rack mounted equipment chassis; whose depth from the front face panel to the rear of the chassis exceeds 25 cm shall be equipped with rack slides.

Each assembly shall have a permanently fixed label showing the model number, serial number, and power requirements.

Materials used in assemblies shall be chosen with due consideration being given to the intended use, safety, durability, retention of appearance, and ability to resist corrosion from a variety of causes including tear gas.

In addition to applicable CSC/DES specifications, the appropriate industrial standards shall apply, including:

a. EIA-310-D Racks, Panels, and Associated Equipment.

b. CSA C22.2 No. 94-1976 Special Purpose Enclosures.

c. CSA C22.2 No. 29-M1983 Panel boards and Enclosures.

5.3 **Printed Circuit Board (PCB)**

PCBs shall be constructed of non-flammable material, preferably a glass epoxy base.

The contractor shall provide extractor devices at the front of each card assembly.
All cards shall have keyed edges to prevent accidental replacement by another type of card.

Each device shall be identified and properly labelled, showing card type, and revision number.

All PCBs shall be etched. Wire wrap connections are not acceptable.

In addition to the requirements set forth herein the appropriate industrial standards shall apply, including:

a. CSA C22.2 No.154-M1983 Data Processing Equipment.

b. CSA C22.2 No.0.7-M1985 Equipment Electrically Connected to a Telecommunications Network.

c. EIA RS-406/IPC-C-405A General Document for Connectors, Electric, Printed Wiring Boards.

5.4 **Components**

All electrical equipment, i.e. power supplies, amplifiers, etc. attached to the equipment structure shall be fastened securely and rigidly not using nuts and lockwashers.

Electrical components used in manufacturing in-house products shall be of commercial quality and shall comply with the standards of the Canadian Electrical Code, Part II.

Electronic circuit components, such as resistors, capacitors, inductors, or semiconductor devices which have no applicable standards in the Canadian Electrical Code, Part II shall comply with the test parameters as set forth in CSA C22.2 No. 154-M1983 Part 6.

6.0 QUALITY ASSURANCE REQUIREMENTS

The contractor shall provide objective evidence that the system and any major component therein have been designed, manufactured, inspected and tested under the umbrella of a quality assurance program capable of meeting the requirements of the applicable ISO Standard 9002 Series. More stringent requirements will be identified on a case by case basis, as needed.

In addition, the contractor shall develop a site-acceptance test/inspection procedure to demonstrate that all parameters of the system are fully operational and conform to the Statement of Technical Requirements.

6.1 In-plant Inspection

The equipment shall meet all functional, electrical, and visual/mechanical test parameters and shall have been fully tested and inspected by the contractor. Results shall be documented and reported to the Design Authority. Periodic inspections may be done by the Design Authority or his designated representative to verify that the equipment meets all requirements.

Particular attention shall be given to the following:

a. Inventory of received equipment.

b. Physical condition of equipment i.e.: scratches, dents, paint chips, etc . . .

c. Construction techniques, board and components accessibility.

d. Neatness, clamping and tying of wiring, cabling and harnesses.

e. Strain relief of cables and wire connections.

f. Legibility of nameplates, identification plates, and markings.

g. Safety and protective covers, warning labels and grounding.

h. Tightness of connectors, screw type fasteners, etc.

i. Soldered and weld joints.

j. Completeness.

k. Operation of drawers, adjustable and sliding parts, controls etc.

l. Shielding.

m. Cable and wire connections, ground clamps and terminal strips.

n. Type and quality of paint finish.

o. Quality of printed circuitry, etching, the electronic components and other associated parts.

p. Quality of locks, cabinets and other materials.

It must be noted that the in-plant tests are performed as a requirement of the financial arrangements and serve to guarantee that the design parameters of the FDR are followed and will meet the requirements of the applicable system specification. Sign-off of in-plant tests will not denote any form of final acceptance of the equipment and design.

6.2 Test Equipment

All test equipment shall be supplied by the contractor.
All instruments and test equipment shall be checked periodically by the QA Inspector in order to ensure accuracy of measurement. Records showing when the test equipment was last calibrated are to be provided as proof of accuracy.

6.3 Calibration

All test equipment used by the contractor shall bear a calibration seal showing the date calibrated and the due date for the next calibration.

The contractor shall ensure that the test equipment's calibration due date does not occur during the test period.

All equipment performance measurements shall be made with instruments whose accuracy and calibration guarantee that the results comply with the terms of the contract.

CSC reserves the right to furnish and/or require the use of any applicable instruments and standards in order to ascertain the accuracy of any measurements.

Test equipment suspected of being damaged or out of calibration shall be rejected by the Design Authority.

6.4 Safety Design Aspects

Particular attention is to be given to the safety design aspects of CSC installations, so as to minimize any hazards while in gaining access to, operating and servicing equipment. Such design aspects shall include the proper grounding of equipment, the installation of protective covers and warning labels over high voltage areas, the installation of warning labels on x-ray equipment, etc.

Radio and TV camera towers must receive careful attention in regards to make them accessible for servicing, especially during inclement weather.

7.0 ON-SITE INSTALLATION

7.1 Inspections

Inspections will be performed by the Design Authority or their designated representative. A thorough visual and mechanical inspection of the installation shall be performed to ensure that all applicable requirements and safety precautions have been met.

7.2 Damage to Government Property

Damage to Government property, including buildings, equipment, etc. during the course of the installation shall be made good by the contractor.

The contractor shall replace all equipment which has suffered major damage, i.e. damage which renders the equipment BER, unserviceable, or subject to deterioration.

If stocks of the applicable equipment are at such a level that replacement of the damaged items cannot be made, and the contractor cannot readily obtain new equipment in order to allow the installation to proceed without delay, the contractor shall:

a. repair the damage immediately with available materials.

b. return to the site and replace the equipment as soon as new equipment is procured.

Minor damage shall be repaired in a manner which leaves the government property in a condition equivalent to its original state and performing the original function, with no deterioration in appearance, performance, and/or reliability.

Any equipment where the paint finish becomes scratched or marred during the installation shall be completely refinished and repainted consistent with the appearance of new equipment.

Equipment shall neither be exposed to rain, nor be left out-of-doors during inclement weather. This stipulation does not apply to construction materials.

7.3 Protection of Surfaces

The contractor shall obtain approval from the appropriate Institution authority before moving heavy loads or equipment on floors, roofs and other surfaces.

The contractor shall adequately protect floors, finished surfaces and roofs from damage during the installation and shall implement special measures when moving heavy loads or equipment on them.

The contractor shall keep the floors free of oils, grease, or other materials likely to damage or discolour them.

The contractor shall provide dust protection for the equipment during the installation period, as related construction activities may occur simultaneously.

7.4 Cutting, Patching and Digging

The contractor shall perform all cutting, patching or digging necessary for the installation of the system.

The contractor shall be responsible for changes or damage to any existing work, cables or equipment by cutting, welding, drilling, or digging without prior consent from the Design Authority.

The contractor shall promptly repair any damage for which he is responsible in order to restore the facilities to their original condition.

7.5 Visual-Mechanical Inspection

Inspection shall be performed by the Design Authority or his designated representative.

Prior to the commencement of performance and operational testing, the installation shall be inspected to ensure that all applicable requirements and standards have been met.

Particular attention shall be given to the following:

a. Physical condition and positioning of equipment.

b. Neatness, clamping and tying of wire and cable harnesses.

c. Cable and wire connections, ground clamps, and terminal strips.

d. Soldered and welded joints.

e. Strain relief of cables, wire connections, and cable harnesses.

f. Cleanliness of equipment boxes under computer flooring.

g. Nameplates, identification methodology and markings.

h. Operation of drawers, adjustable and sliding parts and controls.

i. Equipment fit, fastening devices and accessibility of parts.

j. Construction and finishes.

k. Legibility of labels and tags.

l. Safety aspects, including secure provisions for climbing and working on towers.

m. Shielding.

n. Grounding.

o. Equipment Cooling Provisions.

p. Washers and lock-washers.

q. Tightness of screw type fasteners & connectors.

r. Screws, nuts and bolts shall show no evidence of cross-threading or mutilation.

s. Bottom of equipment racks etc. shall be free of debris and loose parts.

7.6 **Final System Acceptance**

The system shall be accepted when all of the following items have been completed to the satisfaction of the Design Authority and with the written certification of the project manager:

a. performance and operational tests.

b. all documentation.

c. all training.

d. all other terms and conditions.

The system warranty shall be deemed to begin at the completion of the Final System Acceptance or when the system is taken into service with accepted deficiencies, whichever comes first.

7.7 On-Site Maintenance

Building and site maintenance shall be interpreted to include all the areas in which the contractor is carrying out installation activities.

All sites and buildings shall be maintained by the contractor in a clean and tidy condition.

Upon completion of each day's work, all areas such as hallways, stairways, elevators and storage rooms used by the contractor in delivering or storing equipment shall be left in a clean and tidy condition.

The contractor shall store all electronic components not yet installed in a lockable storage room/trailer at the end of each workday. This procedure will reduce the probability of damaged and/or stolen equipment prior to system acceptance. Prior to the commencement of performance and operational testing, the installation shall be inspected to ensure that all applicable requirements and standards have been met.

8.0 DELIVERY

8.1 Packaging

All equipment shall be packaged to ensure that the equipment will not be damaged during shipment and/or delivery to the institution, as well as any associated handling on site.

Fragile components must be clearly identified and labelled.

All circuit cards, equipment modules, etc. shall be protected by the original packaging material until the equipment is placed into service.

8.2 Addressing

Address labelling shall be clearly marked in a minimum of two (2) locations on each package. The following format shall be observed:

a. Complete name of the institutional site.

b. Complete shipping address.

c. Clear description of contents.

d. Complete name of the Institutional representative.

All of the above addressing items will be provided at the Bidder's Conference.

- END OF TEXT -