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

TABLE OF CONTENTS 2

ABBREVIATIONS 4

DEFINITIONS 5

1.0 INTRODUCTION 6
- 1.1 Commercial-Off-The-Self Equipment 6
- 1.2 Technical Acceptability 6
- 1.3 Equipment Procurement 7
- 1.4 Quantity of Equipment 7

2.0 APPLICABLE DOCUMENTS 8

3.0 REQUIREMENTS 9
- 3.1 General 9
  - 3.1.1 Period of Operation 9
  - 3.1.2 Wires, Cables, Conduits, Ducts 9
  - 3.1.3 Wiring Supervision 9
  - 3.1.4 Sabotage, Tampering and Survivability 9
  - 3.1.5 Human Factors 10
  - 3.1.6 Annunciation and Control Panels 10
- 3.2 System Configuration 10
  - 3.2.1 Hardware 10
  - 3.2.2 Software 11
  - 3.2.3 Redundancy 11
  - 3.2.4 Operator VDUs 12
  - 3.2.5 Operator Controls 13
  - 3.2.6 Maintenance/Satellite VDU 14
  - 3.2.7 Maintenance/Satellite Controls 14
  - 3.2.8 PIDS System Menus 14
- 3.3 PIDS Alarm Processing 15
  - 3.3.1 Alarm Priorities 15
  - 3.3.2 Alarm Simulation Priority 15
  - 3.3.3 Alarm Processing 16
- 3.4 Intrusion Detection Systems 16
  - 3.4.1 Data input 16
  - 3.4.2 Data Output 17
  - 3.4.3 Miscellaneous Inputs 17
  - 3.4.4 Data Protocol 17
- 3.5 PIDS CCTV System 17
  - 3.5.1 General 17
  - 3.5.2 Vertical Interval Switcher 17
  - 3.5.3 Dwell Time 18
  - 3.5.4 VCR Control 18

3.5.5 CCTV Character Generator 18
3.5.6 Unused Camera Ports 18
3.5.7 Miscellaneous CCTV Functions 18
3.6 Time/Date Information 19
3.7 PIDS PA Control 19
3.7.1 PA Control 19
3.7.2 PIDS PA Control Panel 19
3.8 FDS Audio Monitoring Panel 19
3.9 SIDS CCTV Integration 19
3.9.1 General 19
3.9.2 Monitor and Control Panel Integration 20
3.9.3 SIDS VCR Integration 20
3.10 Data Logging 20
3.10.1 General 20
3.10.2 Event Definition 20
3.11 Printer Status 20
3.12 Status Panel 20
3.12.1 General 20
3.12.2 PIU Status Functions 21
3.13 UPS Integration 21

4.0 MECHANICAL CONFIGURATION 22
4.1 General 22
4.2 Console Design 22
4.3 VCR/Printer Rack 22
4.4 Console/Rack Colour Schemes 22
4.5 Environmental Requirements 22
4.6 Power Requirements 23
4.7 PIDS Maintenance Functions 23
4.7.1 PIDS Maintenance Functions 23
4.8 Installation Requirements 24
4.9 Documentation Requirements 24
4.10 Support Requirements 24

5.0 QUALITY ASSURANCE 25
5.1 General 25

6.0 DELIVERY 25

7.0 INTERFERENCE 25

8.0 SAFETY 25

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.