SPECIFICATION FOR
FIBER OPTIC INTRUSION DETECTION SYSTEM - FOIDS®

PART I – GENERAL

1.01 System Description

Furnish, install, test, and leave ready for operation the perimeter Intruder Detection and Monitoring System (IDMS). The system shall utilize single mode, Fiber Optic Fence Sensors. The entire system shall be managed by microprocessor controllers located in a rack assembly within the Central Control Center (CCC), which shall provide full color text and graphic displays that shall show clearly the status of all the individual sensing zones. The system shall be of proven design, and have the ability to readily integrate with access control and other types of intrusion detection and identification systems.

1.02 Related Work

None.

1.03 Reference Standards

1. SAES-0-115	Intruder Detection System
2. ISO 9001	

PART II – PRODUCTS

2.01 General

1. Provide a fully integrated Intrusion Detection and Monitoring System (IDMS).
2. The system is to be tamperproof and fail-safe and must contain line supervision to detect any attempt to spoof the system by cutting, climbing, lifting, bypassing or intercepting the data transmission. Any attempt to compromise sensors, trunk lines, junction boxes or the electronic units, shall result in an immediate alarm.
3. The system shall be fail safe in that failure of any part of the system, whether accidentally or deliberately induced, shall register an alarm state.
4. Transmission of IDMS data shall be via a single mode fiber optic cable. Sufficient fiber optic cores in these trunk cables shall be provided for 50% redundancy.
5. The fiber optic fence sensors shall be total passive and contain no active field components. All signal processing shall be carried out in the CCC.
6. The entire intrusion detection system shall continue to operate in the event of a main power failure utilizing Uninterruptible Power Supplies (UPS) and emergency generators or alternate power sources. In the event of a total power failure, including the emergency power sources, and the system goes down, it will

automatically reset to all previous settings that existed prior to the outage, upon restoration of power.

7. The security perimeter fence protected by the system shall be divided into the appropriate number of zones for the system proposed. Should there be a failure of an individual zone, the remainder of the system will continue to function. The status of these individual zones can be viewed on a computer video display unit (VDU). In addition, a printer will be used to record system status at the CCC.

8. All sensing zone detection parameters, including sensitivity thresholds, alarm signal discriminators and filtering shall be capable of being set and controlled from the CCC.

9. The normal lifetime of the sensors shall exceed ten (10) years and they shall be maintenance-free unless physically damaged. Repair of any damaged sensor cable shall easily be accomplished on site and shall not require replacement of the entire sensor cable.

10. The system shall be capable of detecting any intruder cutting, climbing, lifting or vaulting the fence.

2.02 Basic Operation

1. The IDMS shall continuously monitor the inputs from all fence sensor zones. Upon detection of an intruder, an audible alarm shall be sounded at the operator's console in the CCC, as well as at the Remote Control Center (RCC).

2. The alarmed zone will be highlighted on the computer monitor map display. If a second alarm occurs, the system should automatically display the alarm location on the computer monitor map display. The system will continue to operate in the alarm mode until the operator acknowledges and secures the alarms.

3. During an intrusion event, a highly excited atmosphere will exist. For this reason, it is imperative that the security system shall operate in an automatic mode requiring minimal response from the guard(s). Intelligence must be built into the control computers to display the proper images as they happen for assessment.

4. All actions taken by the operator plus alarm events shall be logged to the control computer's hard disk and printed out.

5. The system status will be clearly displayed at all times on the computer monitor. The status indications of display are divided by different types of annunciation for particular events. The IDMS should be designed so that specific system status is always related to an individual alarm zone. The various status indications are described below:

   Alarm - The status indication of an IDMS alarm shall be by both visual (through the monitor) and audible indicators in the event of IDMS sensor detection of an intrusion. A flashing red light plus an audible tone will indicate a security intrusion alarm. When the alarm is acknowledged, the red light will stop flashing and go steady and the audio tone will be canceled.

Access - A steady yellow light shall indicate zone access. The monitor display indicator of access refers to the condition where alarms are ignored due to an alarm event being expected. The system will maintain line supervision during the access period.

Secure - A steady green light shall indicate secure. Display of this indication shall be when communication is available on the signal transmission media and the sensors are “armed”.

Trouble - A flashing yellow indication for each zone shall be displayed when any condition exists which inhibits alarm detection (e.g., optical module or processor is lost).

Supervision - This indication will display a flashing red light when any tampering or bypassing of the system is attempted. Malfunctions and tampering are thus controlled by line supervision techniques.

2.03 Basic Components and Functions

The purpose of the IDMS shall be to provide early detection and assessment of unauthorized intrusions to the facility so that on-site security personnel can react in a timely manner. In addition to local control and display of the system, it shall be possible for the system to be monitored and/or operated from a remote location.

1. Alarm Monitoring and Control System (AMCS)

The AMCS shall automatically monitor and control the operation of the IDMS. The system shall be designed to have remote monitoring capabilities.

a. Security Equipment Room

The system shall be comprised of a Control Console plus Equipment Racks located in the CCC. This area will house all control, communications, display and signal processing electronics with a hot backup computer that shares all database information.

b. Control Console in CCC

A monitor shall be used to present a site map and annunciate the intrusion status of all IDMS alarm points and view the availability status of all alarm gathering systems. The site map shall also display all fence zones, detection system zones and camera locations, along with their status.

The primary operational mode of the display is the security-monitoring screen (Operator’s Menu). This screen shall be used to annunciate the intrusion status of all IDMS alarm points and the availability status of all alarm gathering subsystems. Selection of each button or zone symbol shall appear to be instantaneous. An audible prompt shall be used to reinforce the user feedback acknowledging acceptance of the selection.

All operations involving the selection of an IDMS sensor zone shall be available to the user through the direct touching of or pointing at the zone symbol, without the need for scrolling through a list of options.

c. **Remote Alarm Monitor**

The Remote Control Center shall have two monitors capable of displaying freeze pictures from the alarmed zones on one of them and real-time pictures of the alarmed and adjacent zones on the other monitor together with text and graphics.

An audible alarm should give sound at the first indication that the system has detected an intrusion. This alarm should be loud enough to get the guard's attention without being so loud as to startle him. In the event the guard is not close enough to hear this more subtle alarm, a second level (at least 90 dB) alarm should then sound outside the Remote Control Center to ensure he hears the alert.

d. **Remote Display and Control**

It should be possible to have a supervisory and control console located in a remote location capable of supervisory control of the system and displaying all information.

2. **Equipment Racks**

Sufficient equipment racks shall be provided in the CCC equipment room to house:

1. Microprocessor-based master IDMS Control Computer.
2. "Hot" backup master IDMS Computer with automatic switch over.
3. Event and report logging printer interfaces.
4. Fiber Optic Fence Sensor electro-optics unit and alarm signal processing.
5. All fiber optic cable termination patch panels.
6. Detection Subsystem alarm interface.

3. **Fiber Optic Fence Sensor Subsystem**

The Fiber Optic Single Mode Fence Sensor is the primary intrusion sensor. The sensor should be a cable containing a single fiber optic core, attached to the fence fabric at mid-height by tie-wraps at regular intervals. By using Sagnac (reflectometric time division-multiplexed). Interferometry phenomenology, the sensor and associated electro-optics processing system shall be capable of detecting all attempts to climb, cut through or lift the fence.

Fence Sensors should:

1. Detect intrusion attempts associated with climbing, cutting or lifting the fence.
2. Attach directly to chain link fences with UV hardened cable ties.
3. Provide Immunity to EMI, RFI and other electro-static releases (lightning, generators, etc.).
4. Not be affected by moisture in any form (rain, fog, sleet, snow).
5. Provide flexible sensor lengths designed to meet a broad range of user requirements.

6. Provide digital processing allowing the fence sensor to be deployed in virtually any environment.
7. Hardware shall include a feedback loop to stabilize its reaction to fence activity regardless of the weather or time of day. This eliminates periods of insensitivity during the morning and evening when large temperature variations occur.
8. Detection algorithm shall search the fiber optic signal returned from the fence for two key features: one for climbs, and one for cuts. These features shall not exhibit by thermal variations small animals such as birds. The result is a system that is significantly less prone to false and nuisance alarms.
9. The system shall evaluate the background fence signal, which is a measure of wind. As the wind increases, alarm thresholds are raised to further reduce the false alarm rate.
10. A computer shall be used to store and trace data of events that occur. The events can be alarms, or higher signal levels that did not result in alarms. At a later time, the events can be reviewed on the attached computer, and a set of thresholds determined and tested for both cutting and climbing that properly annunciates intruders while avoiding annunciation of false alarms. By saving a large number of trace sets, a library of fence characteristics can be developed for turning purposes.
11. There shall be no active components in the field and all signal processing will be carried out in the CCC. This signal processing will distinguish between a cut and an object hitting the fence or between a climb and the action of the wind blowing the fence fabric.
12. The signal generated by the detection electronics connected to each zone shall be examined directly by the IDMS computer.
13. The contractor shall provide a suitable solution for covering the main gate and any emergency gates.

The minimum acceptable performance specifications shall include:

1. Minimum Probability of Detection (PD): 98%
2. Temperature: -20 degrees Celcius to +65 degrees Celcius for external cable.
3. Temperature: 0 degrees Celcius to +50 degrees Celcius internal equipment.
4. Humidity: 0% to 100% for external cable sensor.
5. Humidity: 0% to 90% non-condensing for internal equipment.
6. The sensor cable shall have ultraviolet radiation resistant jacket.

2.04 Environmental Effects

1. The fiber optic IDMS (FOIDS) shall compensate for varying climate conditions automatically. In lieu of this capability, the system shall have the ability for programming, from the CCC each zone directly and separately to accommodate a wide variety of environmental conditions.
2. The FOIDS shall be capable of immediately reporting cut or broken sensors.
3. All communication cables shall operate within specifications at ambient temperatures between –20 degrees Celcius and +65 degrees Celcius and while immersed in water.
4. All sensor cables shall operate within specifications at ambient temperatures of between –20 degrees Celcius and +70 degrees Celcius continuously and also while subjected to incident solar flux of 1,040 Watts/m^2 and relative humidity of 99%.

2.05 Main Power Supply

All hardware supplied for this project shall use U.S. standard single phase, 120V, 60Hz power without the need for any external transformers or converters. The plug used on equipment power cords shall be NEMA reference 5-15P designed to plug in to a U.S. standard 15A receptacle designated NEMA 5-15R. Contractor shall clearly identify to the Company any deviations from this requirement and are subject to Company approval.

The Remote Control Center and CCC equipment shall be powered by uninterruptible power for at least one (1) hour in the event of normal power failure. Emergency power from an alternate source (e.g., backup generator) should be available within thirty (30) seconds. The input power to the UPS shall be provided by others from emergency main supply.

Fiber Optic transmission equipment shall be powered from supplies taken from the perimeter power cables. Unless an alternate power source is available, these devices shall be provided with backup batteries that will operate for twelve (12) hours in the event of power outage.

2.06 Equipment Specifications

1. Display and Assessment Workstation

The Display and Assessment computer in the CCC shall be based on Dell PCs or equivilent.

The stand-alone IDMS™ platform consists of a Pentium PC running on a Window 95/98 or Windows NT operating system. The operating system runs the Graphic User Interface (GUI), the Data Management System (DMS) and sensor specific utility interfacing software. All of the applications are COTS and run as a single integrated user-friendly system.

Hardware specifications:

- Processor
- 600 MHz with 32 KB L1 cache, 256 KB Advance Transfer L2 cache
- Memory
- 128 MB Non-ECC DIMM
- CD-ROM 48xmax. Variable Speed
- Diskette Drive 3.5, 1.44 MB
- Zip® Drive 100MB internal
- Sound Card Integrated
- Speakers PC
- Video Graphic Card
- Monitor 19” (17.9 viewable) 1600 x 1200 pixels
- 2 USB Ports
- Serial Port
- Parallel Port
- Keyboard
- Wheel Mouse
- Micro tower with access latch
- Dimensions: 6.4” width x 15.5” height x 13.4” depth
- Power 145 Watts
- Input Voltage: 30 to 135V at 60Hz
- Output Wattage: 145-Watts max. Continuous
- Output Voltage: 3.5V, 5V, and 12V
- Heat Dissipation: 180 BTU/hour (min. value)
- Power Management: APM 1.2 hard spin down and monitor control
- Backup Battery: 3.0VCR2032 Lithium Magnesium oxide coin cell

Software Specifications:

- Windows 95/98
- Microsoft Access Database
- ECSI Graphical User Interface

2. **Integration With Other Systems**

The system shall be capable of operating a stand-alone system with an ability to integrate with other types of security systems. A clearly defined documented and tested ability to connect to additional systems in the future shall be provided. Contractor shall supply documentation that shall describe all aspects of requirements for future connections.

2.07 – System Control Criteria

1. The system shall have the capability to perform extensive control commands and review of previous activity related to the perimeter system and other integrated systems.
2. The primary operation mode of the Display and Assessment Workstation is the security-monitoring screen (Operator's Menu). This screen shall be used to annunciate the intrusion status of all IDMS alarm points, the availability status of all alarm gathering subsystems and to control review of recorded images. Selection of each button or zone symbol shall appear to be instantaneous. An audible prompt shall be used to reinforce the user feedback acknowledging acceptance of the selection.
3. All operations involving the selection of an IDMS zone camera shall be available to the user through the operator keypad or touch screen.
4. All alarms shall be capable of being masked on a zone-by-zone selectable basis so as to avoid a high false response rate during periods of legitimate activity. In order to keep the IDMS at optimum performance, the IMDS shall also allow the supervisor, under password protection, to access and adjust the detection parameters of the video intrusion detection and fence sensors.
5. The supervisor shall have a switch function under password control allowing a sensor to be masked. Once in the masked state, a function shall exist to re-activate the sensor. If the particular sensor was predetermined to be a sensor which the supervisor cannot mask, the button to perform the function will be removed from the keypad.
6. A context sensitive help screen shall be available with on-screen text to describe each of the button choices available on the screen. Alarm processing shall override the help screen and present the alarm information immediately upon receipt of the alarm signal.
7. A separate set of operational functions shall be available for supervisory and system administration use. There functions shall be capable of password protection, requiring a user password for entry to the menu. Simultaneously, Operations and Supervisory Control shall be possible through the use of a separate workstation monitor. There shall be no reduction in any of the performance specifications for alarm processing during any parallel supervisory activity.
8. IDMS shall be controlled by an operator keypad or touch screen with restricted functions which allow operation of the Security Control and Monitoring capabilities of the system, but not the programming or Configuring Operations. This keypad or touch screen should have a set of built-in commands. Also, this keypad or touch screen should work in conjunction with and does not replace the system keyboard.

9. The IDMS shall provide a function to allow the System Manager to generate simulated alarm activity. Simulations shall be limited to display alarm activity. All operator console presentations shall appear as though an actual incoming sensor point caused the alarm. The operator shall have all of the normal processing facilities available. Data logging reports shall be annotated to identify each occurrence as a simulated event. All output drive points associated with the simulated alarm sensor will respond as though the alarm was caused by an actual incoming sensor point. Any alarm entering the system from an outside source or from internal diagnostics will cause the simulation to terminate and return the system to the normal operating condition with the alarm presented and ready for acknowledgment. The simulation system shall not automatically re-engage following the interruption. The simulation system shall have the capability to allow the alarm simulation routine to be pre-programmed and run according to the recorded script once started. The pre-programmed alarm simulation sequence shall be started manually by user command. It shall not be possible to pre-program the starting time of the simulation.

2.08 Software

1. Operating System

The Operating System (OS) environment for all computers shall be a recognized industry standard operating system available off-the-shelf. All commercial off the shelf (COTS) software shall be the most current version at the time of installation. The preferred operating system shall be the latest version of Windows NT.

Technical Support and Documentation

The contractor shall supply unlimited license for any application software developed specifically for this system installation. (This does not apply to COTS). The application software shall require no modification to run with the delivered operating system. All software interfaces with the operating system shall be via OS interface standards. The use of software emulators to execute applications shall not be acceptable.

2. System Support for Software Development and Testing

The contractor shall provide all system software, programming aids, compilers, libraries, etc. necessary to support comprehensive application program development and testing.

All software development and initial testing shall be done without interfering with normal operation of the system.

All application software to readily support the following functions shall be provided:

a. Modification of any software specifically developed for the IDMS, database and displays.

b. Development of new software in the programming language utilized within the system.

c. Debugging and testing of modified or new software.

d. Integration of modified or new software, databases and displays into the system.

e. Software configuration management.

3. **Maintenance Utilities**

   The processor system shall have a full complement of maintenance utilities. These utilities shall allow its maintenance role to be carried out with little or no understanding of or experience with the operating system. The utilities, themselves, shall be user friendly and require little training to use them effectively.

   The IDMS shall utilize COTS software to the maximum extent possible. However, all software that is developed will be in a single high level language (such as C) regardless of the platform.

4. **Software Quality Factors**

   Contractor shall design the IDMS to meet the requirements presented herein. The contractor shall identify all subsystems to be used throughout the IDMS and categorize them.

   The categories will be COTS (non-developed items), modified COTS or IDMS developed software. The contractor shall establish and maintain an efficient system quality program for all modified COTS and developed software.

5. **Field Proven Software**

   Contractor shall provide a field-proven system. Where integrated or other software packages are required, contractor shall utilize COTS software to the maximum extent possible.

6. **Authorization System**

   a. IDMS shall incorporate a comprehensive log-on control capability to limit and control users and administrators logging into the system. The system shall permit designated individuals to set up authorization levels to the field level for users. An audit trail of all system activities shall be maintained. Changes to the authorization system shall be restricted to designated individuals.

   b. ***User log-on control*** – the system shall use passwords and log-on IDMS to control log-on, of all users to workstations. System password security shall be designed to ensure that only Company authorized users have access to the system and then only for specific functions. Access to the system shall be secured using a user name and password system. The system shall require a definable length (minimum of six [6] characters) for the password and shall allow users to assign their own passwords. The system manager shall have the capability to extend the minimum length of the password and transmit this globally to both workstations.

   c. ***User access level definition*** **–** the system shall have the ability to restrict user access to specific field and function levels. Each user shall have a predetermined set of authority in terms of access to the data and programs in the system. Through the security/access control system, each user may be assigned so that certain system commands and instructions cannot be executed without specific levels of authority. In addition, access to data and program files may be individually assigned by the system.

d. ***Audit trail*** – a detailed audit trail of all system activities shall be maintained by the system. This shall include log-ins; invalid log-in attempts and changes made to data.

e. All log-ins and attempted log-ins to the system will be logged to the audit trail, date, time, badge number and workstation ID will be logged to the audit trail showing whether the log-in was successful. Unsuccessful log-in attempts will be logged showing date, time, and user ID used, workstation ID and reason log-in was unsuccessful.

f. All activities on the IDMS will be logged to the audit trail. The audit file will be sized to contain at least one (1) month's activities. Data from the audit trail shall be deleted after it has been copied to tape. If the audit trail is full and has not been backed up, the contractor shall develop procedures and software to deal with the contingency.

g. ***Authorization levels*** – three (3) levels (at least) of authorization are required.

PART III – EXECUTION

3.01 Coordination

1. Fiber Optic Trunk Cable

The Single Mode Fiber Optic Cable trunk cables shall be installed in minimum four (4) inch PVC direct burial conduit.

2. Fence Sensor

a. The sensor cable should be tie-wrapped to the fence fabric. The cable shall be fastened to the fence fabric at 36 cm maximum intervals. The fastening shall not be over tightened.

b. All fiber optic splices shall be made weatherproof and enclosed in NEMA termination boxes.

c. The hand holes and junction boxes shall act as environmental protection for the fiber optic splice, since they provide protection against potential hazards, including extreme forms of heat.

d. Termination of fiber optic cables in the equipment room of the CCC shall be accomplished by installing fiber optic patch panels with pre-connectorized assemblies.

e. During installation of the sensor cables, accurate records of conduit and cables shall be prepared and maintained. These records shall be required for maintenance and future troubleshooting purposes.

3. Splicing Procedure

All fiber optic splices shall be performed in accordance with acceptable industry procedures.

4. Patch Panel

A patch panel, containing interconnection sleeves, shall be provided in the control room. The cables entering the building from various zones shall be terminated on the patch panel to minimize accidental damage to the cables. Patch cords shall be used to connect equipment with the patch panel wherever required. The patch panel shall be rack mounted.

3.02 Availability

1. Definitions

The system shall have an availability of at least 99.95% to the operator, without degradation of performance and system response. The availability requirement refers to functional availability, and encompasses not only hardware, but also software availability. The standby or redundant half of the system shall have an availability of at least 99.8%.

The availability of the system shall be defined as follows:

$$\frac{\text{Total Test Time Unavailable Time}}{\text{Total Test Time}}$$

System unavailable time is defined as the time from the loss of the first on-line operator function to the restoration of all operator functions. These functions include, but are not limited to, applications, display update and other MMI functions and logging.

The availability requirements stated in the section shall be subject to the following constraints and assumptions:

a. Non-availability due to failure of equipment outside the system shall not be considered.

b. Non-availability due to accidents, fires or other acts of God shall not be considered.

c. The system must be maintained and operated in accordance with the documentation supplied with the system.

2. Availability and Repair Time

These requirements are on a functional, rather than equipment, basis. All items of equipment necessary to provide a given function shall be included in determining the availability of that function. Failure of equipment for which redundant equipment is provided shall not be considered to the extent that switch over to the redundant equipment is performed automatically and the data involved is continuously available during the failure and switch over.

3.03 – Safety

All equipment shall comply with the latest electrical current leakage requirements of IEC-990 and 1010-1.

3.04 – Acoustics

The acoustic noise level in all areas shall not exceed 65 dB (A) with all equipment operating.

3.05 – Grounding

All equipment shall use a three-wire plug with a third wire connected to the receptacle ground pin.

3.06 – Hardware Reliability Testing

Hardware reliability testing shall be in accordance with 23-SAMSS-010.

END OF SPECIFICATION