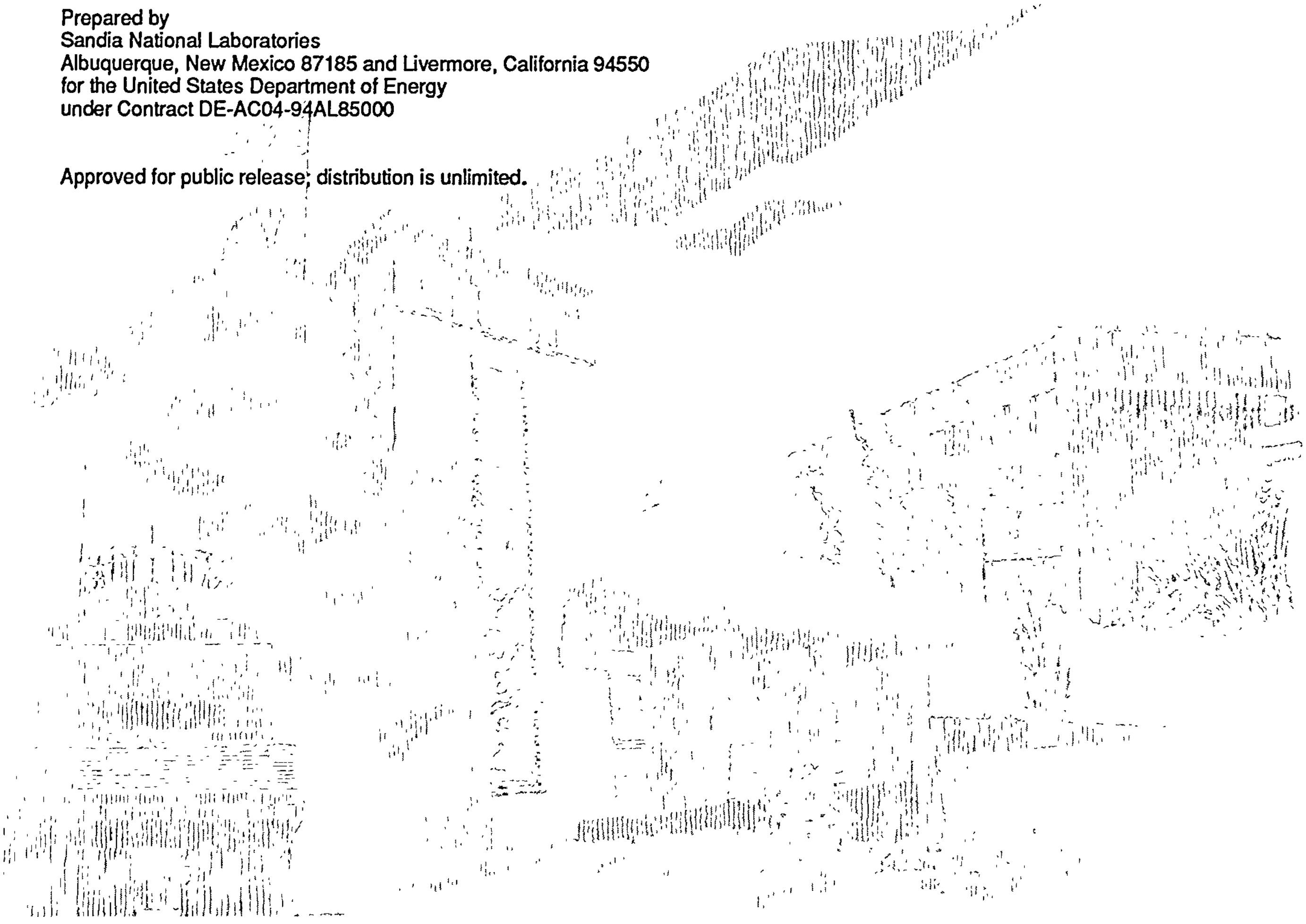
SANDIA REPORT
SAND95–1944 • UC–515
Unlimited Release
Printed September 1995

Functional Requirements with Survey Results for Integrated Intrusion Detection and Access Control Annunciator Systems

Lester H. Arakaki, Faye M. Monaco

Prepared by
Sandia National Laboratories
Albuquerque, New Mexico 87185 and Livermore, California 94550
for the United States Department of Energy
under Contract DE-AC04-94AL85000

Approved for public release; distribution is unlimited.



SF2900Q(8-81)

Issued by Sandia National Laboratories, operated for the United States Department of Energy by Sandia Corporation.

NOTICE: This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, nor any of their employees, nor any of their contractors, subcontractors, or their employees, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government, any agency thereof or any of their contractors or subcontractors. The views and opinions expressed herein do not necessarily state or reflect those of the United States Government, any agency thereof or any of their contractors.

Printed in the United States of America. This report has been reproduced directly from the best available copy.

Available to DOE and DOE contractors from
Office of Scientific and Technical Information
PO Box 62
Oak Ridge, TN 37831

Prices available from (615) 576-8401, FTS 626-8401

Available to the public from
National Technical Information Service
US Department of Commerce
5285 Port Royal Rd
Springfield, VA 22161

NTIS price codes
Printed copy: A05
Microfiche copy: A01

SAND95-1944
Unlimited Release
Printed September 1995

Distribution
Category UC-515

FUNCTIONAL REQUIREMENTS with SURVEY RESULTS

FOR

INTEGRATED INTRUSION DETECTION AND ACCESS CONTROL ANNUNCIATOR SYSTEMS

Lester H. Arakaki
Faye M. Monaco

Security Technology Department
Sandia National Laboratories
Albuquerque, New Mexico 87185-5800

Abstract

This report provides functional requirements and data obtained from a survey of producers of integrated intrusion detection and access control annunciator systems.

CONTENTS

1. MANAGEMENT OVERVIEW 1-1

1.1 INTRODUCTION 1-1

1.2 SURVEY BACKGROUND 1-1

1.3 ANNUNCIATOR DEFINITION 1-1

1.4 REPORT COMPOSITION 1-1

1.5 REPORT VALIDITY 1-2

1.6 SUGGESTED USE FOR REPORT DATA 1-2

2. SURVEYED FIRMS AND SYSTEMS 2-1

2.1 ADVANTOR CORPORATION 2-2

2.2 DSX ACCESS SYSTEMS INCORPORATED 2-3

2.3 INFOGRAPHIC SYSTEMS 2-4

2.4 LAWRENCE LIVERMORE NATIONAL LABORATORY 2-5

2.5 LOGIPLEX 2-6

2.6 MATRIX 2-7

2.7 MOSLER INCORPORATED 2-8

2.8 SMF SYSTEMS CORPORATION 2-9

2.9 VIKONICS INCORPORATED 2-10

2.10 VINDICATOR INCORPORATED 2-11

2.11 WESTINGHOUSE SECURITY ELECTRONICS 2-12

3. SURVEY DETAIL TABLES 3-1

3.1 FUNCTIONAL SPECIFICATIONS FOR THE INTEGRATED SYSTEM ANNUNCIATOR - GENERAL REQUIREMENTS 3-2

3.1.1 Central Alarm Stations shall display to the operator(s) all events which require a response 3-2

3.1.2 Facilities shall have a Secondary Alarm Station 3-2

3.1.3 The Secondary Alarm Station need not be fully redundant to the Central Alarm Station, but must be capable of providing effective control response to safeguards and security incidents 3-2

3.1.3.1 A duress alarm at the Central Alarm Station shall annunciate at the Secondary Alarm Station. This will not be annunciated at the Central Alarm Station. 3-3

3.1.3.2 A duress alarm at the Secondary Alarm Station shall annunciate at the Central Alarm Station. This will not be annunciated at the Secondary Alarm Station. 3-3

3.1.4 On-line functions shall be treated by the system with a higher priority than off-line functions. 3-3

3.1.5 The time from the moment a sensor is activated to the moment it is audibly and visibly annunciated shall be under two seconds. 3-3

3.1.6 The time from the moment a sensor is activated to the moment a video recording of the alarm scene is initiated shall be under one second. 3-3

3.1.7 User requests for the status of sensors or system components shall be satisfied in less than two seconds 3-4

3.1.8 The user shall receive instant feedback that the command was initiated. 3-4

3.1.9 Off-line functions must be able to be aborted by the operator at any time. 3-4

3.1.10 There must be sufficient internal and external redundancy and fail-over mechanisms to preclude the loss of any single component from causing catastrophic failure of the system. 3-5

3.1.11 If a system component(s) suffers a malfunction or failure, system functionality (if affected) must degrade gradually, maintaining higher priority on-line functions as long as possible. 3-6

3.1.12 Tools and equipment necessary for a system maintainer to properly diagnose and repair system failures shall be provided as part of the maintenance support system. 3-6

3.1.13 Maintenance procedures, training, menu-driven test programs and self diagnostics shall be provided as part of the maintenance support system. 3-6

3.1.14 Positive control and documentation of the product's development and changes are required. 3-7

3.1.14.1 Controls and audit trails for changes to the configuration are required. 3-7

3.1.14.2 The audit trail of all changes made to the stored data and code must be maintained in as automated fashion as possible. 3-7

3.1.14.3 The audit trail must be archived in non-volatile storage. 3-7

3.1.14.4 The audit trail must include but is not limited to the identification of the person(s) making the change, a description of the change made, and the date and time of the change. 3-7

3.1.15 Communications between system components must be protected from compromise or spoofing as required in the relevant DOE orders........ 3-8

3.1.16 If an exception reporting communications protocol is used, each data gathering panel (DGP) must be polled by an alarm annunciator at least once each hour. 3-9

3.1.17 The system must accurately display the correct state of every component of the system. 3-9

3.1.18 The system software shall have at least five levels of system access authorization to control: (1) access to operate functions, (2) read access to the data base, (3) read/write access to the data base, (4) read/write access to source code, and (5) read/write access to executable code. 3-10

3.1.19 Each access authorization level shall be protected by password or credential control. 3-11

3.1.20 The color scheme recommended for displaying events to the operator is: Red, Flashing Red, Yellow, and Green. 3-11

3.1.20.1 The system must be able to display system activity to the operator in graphic form........ 3-12

3.1.21 Interaction with the system must be possible, as a minimum, through a keyboard and/or by interfacing with a graphic screen. 3-15

3.2 FUNCTIONAL SPECIFICATIONS FOR THE INTEGRATED SYSTEM ANNUNCIATOR -SOFTWARE 3-16

3.2.1 The operating system may be from any proven commercial source. It must be a current, supported version. 3-16

3.2.2 Database, compilers, and other system software must also be current and supported. 3-16

3.2.3 The source code must either be provided by the supplier, or held in escrow by a third party. 3-16

3.2.4 The source code placed in escrow must be identical to the software supplied........ 3-16

3.2.5 As the software is revised, the source maintained in escrow must also be revised. 3-16

3.2.6 The integrity of the system hardware and software should be monitored in an automated fashion such that failures and tampering are detected and reported........ 3-17

3.2.6.1 Failures must be communicated to the operator. 3-17

3.2.7 The system must log all system known events/transactions........ 3-17

3.2.8 The system must allow the operator to archive data on command. 3-18

3.2.9 Archiving will be made to a nonvolatile media. 3-18

3.2.10 The software must allow the operator to produce both formatted and ad hoc reports of any data contained in the central database and the audit trail files. 3-18

3.2.11 The system must allow creation, queries, modifications, and deletions of database items. 3-20

3.2.12 The preceding functions shall be accomplished in a manner that isolates the user from the underlying structure. 3-21

3.2.13 When alarm processing determines that the status of a sensor and/or logical group has changed, it must be able to inform other systems. 3-22

3.2.14 Whenever event processing encounters an error condition, a message shall be printed to either a maintenance or console operator's log or display depending on the severity of the error. 3-22

3.3 FUNCTIONAL SPECIFICATIONS FOR THE INTEGRATED SYSTEM ANNUNCIATOR - HARDWARE 3-23

3.3.1 The system shall be capable of handling a 50% increase in system capacity and continue to meet the original performance requirements states in 2.1.1 without software or hardware modifications. 3-23

3.3.2 The system shall be designed to provide event reporting with no loss of data for a period of no less than eight hours after the loss of primary power. 3-23

3.3.3 The operator shall be notified within ten seconds upon the loss of primary power in any part of the system. 3-23

3.3.4 Switching to back-up power must be automatic upon the loss of primary power. 3-24

3.3.5 Back-up power must be applied in such a manner that no system component will be without power in the event of a loss of commercial power. 3-24

3.4 ALARM PROCESSING SYSTEM FUNCTIONAL SPECIFICATIONS FOR ANNUNCIATORS - GENERAL REQUIREMENTS 3-25

3.4.1 The alarm processing system must be capable of individually monitoring and annunciating the status of all sensors in the system. 3-25

3.4.2 The alarm processing system must be capable of visually and audibly annunciating to the operator a change in sensor status within 1 second of the change if less than 25% of the system's sensors alarm simultaneously, and within 3 seconds if 25% or more of the system's sensors alarm simultaneously. 3-25

3.4.3 The alarm processing system shall be capable of supervising the communications between the primary host processing computer and the sensors. 3-26

3.4.4 The alarm processing system shall be capable of ignoring intrusion sensor alarms if requested by an authorized operator. 3-26

3.4.5 The alarm processing system shall be capable of uniquely identifying, by both color and text, the following sensor and logical group states: Secure, Access, New Alarm, Alarm, Alarm Gone, New Tamper Alarm, Tamper Alarm, Tamper Alarm Gone, Off-line, and Failed. 3-26

3.4.6 The alarm processing system shall be capable of calculating a new status and displaying that status for any given sensor based on sensor input, environmental conditions, and user input. 3-27

3.4.7 The alarm processing system shall be capable of permitting the operator to place sensors "in access." 3-28

3.4.8 The alarm processing system shall be capable of prioritizing alarms from all sensors. 3-28

3.4.9 The alarm processing system shall be capable of changing the current priority of any given sensor or logical group based on input received from other components/systems. 3-28

3.4.10 The alarm processing system shall be capable of adding and deleting sensors in a logical group based on user input. 3-28

3.4.11 The alarm processing system shall be capable of adding and deleting a logical group. 3-28

3.5 ALARM PROCESSING SYSTEM FUNCTIONAL SPECIFICATIONS FOR ANNUNCIATORS - ALARM ASSESSMENT 3-29

3.5.1 The system must possess the capability to permit the operator to enter the assessment decision made by the operator into the database. 3-29

3.5.2 Alarms must be assessed as to their cause by either direct or indirect (CCTV) personnel observation or a combination of both. 3-29

3.5.2.1 CCTVs used for assessment must be able to be automatically switched (and aimed if PTZ) to display a preprogrammed camera image on the desired monitor. 3-29

3.6 ACCESS CONTROL SYSTEM FUNCTIONAL SPECIFICATIONS FOR ANNUNCIATORS - ACCESS CREDENTIAL 3-32

3.6.1 The badge must, at a minimum, interface with magnetic card readers. 3-32

3.6.2 The badge must be entered into or passed through a device that reads the embedded codes and passes that information to a database for comparison with existing data. 3-32

3.6.3 The badge shall be capable of being attached to an individual and displayed openly above the waist and below the shoulder. 3-32

3.7 ACCESS CONTROL SYSTEM FUNCTIONAL SPECIFICATIONS FOR ANNUNCIATORS - ACCESS PORTAL 3-33

3.7.1 Access portals shall provide for access control. 3-33
3.7.2 Access portals shall provide for alarm generation and assessment. 3-33
3.7.3 Access portals shall provide for assist access. 3-33
3.7.4 Access portals shall provide for emergency ingress/egress. 3-33
3.7.5 Access portals shall provide for degraded mode operation. 3-34
3.7.6 Access portals shall provide for positive single access. 3-34
3.7.7 Access portals shall provide for two-person rule. 3-34

3.8 ACCESS CONTROL SYSTEM FUNCTIONAL SPECIFICATIONS FOR ANNUNCIATORS - CONTROL SOFTWARE 3-35

3.8.1 The access control software must receive information from the installed access control devices, compare this information to data stored in a data base, and generate the appropriate signal to the portal locking device. 3-35
3.8.2 Unsuccessful access attempts must be logged in a transaction file. 3-35
3.8.3 Unsuccessful access attempts must be signaled to the appropriate portal access device . 3-35
3.8.4 The access control software must be capable of handling logical portal access requirements including individual access requirements for each portal. 3-36
3.8.4.1 The access control software must be capable of handling logical portal access requirements including two-person rule. 3-36
3.8.4.2 The access control software must be capable of handling logical portal access requirements including escorted visitors. 3-36
3.8.4.3 The access control software must be capable of handling logical portal access requirements including anti-passback. 3-37
3.8.4.4 The access control software must be capable of handling logical portal access requirements including invalid access attempts. 3-37
3.8.4.5 The access control software must be capable of handling logical portal access requirements including open portal time-out. 3-37
3.8.5 Authorized individuals must be able to place any portal "in access." 3-38
3.8.6 When a portal is placed "in access" the system will log the time of the event and the person taking the action. 3-38
3.8.7 When a portal is placed "in access" the system will provide constant notification that the portal is in access. 3-38
3.8.8 When an access portal is placed "in access," line supervision and tamper alarms will be reported. 3-38

3.8.8.1 When an access portal is placed "in access" by an authorized individual, notification of that action must be made to the operators in the primary alarm station. 3-39

3.8.8.2 When an access portal is placed "in access" by an authorized individual, notification of that action must be made to the operators in the secondary alarm station. 3-39

3.8.9 The access control software must be capable of enrolling and unenrolling entrants from one or more remote locations. 3-39

3.8.10 Enrollment of a potential entrant must be performed by authorized personnel. 3-39

3.8.11 Time of allowable access must be capable of being entered in thirty minute or less increments and will include a start and stop time of day. 3-39

3.8.12 Time of allowable access must be capable of being entered in thirty minute or less increments and will include a start and stop time of day. 3-40

3.8.13 Date of access must be capable of being entered as calendar dates, including the year. 3-40

3.8.14 Authorized portals may be entered as individual portal numbers or logical sets of portals. 3-40

3.8.15 The software will automatically update individual portals or devices that control one or more portals with data from the central data base. 3-40

3.8.16 When communications are lost between the intelligent field device and the "host" machine, the field device will internally log all transactions. 3-41

3.8.17 When communications are re-established between the intelligent field device and the "host" machine, the field device will up-load to the "host" all logged transactions that occurred while communications were lost. 3-41

3.8.18 The access control software will record all successful and unsuccessful access attempts in an audit trail file. 3-41

3.8.19 The minimum data to be recorded includes: name of entrant, personal identification number, event time, event date, portal number, and badge number if used. 3-41

3.8.20 The access control software will signal an alarm when the preset number of consecutive invalid access attempts has been exceeded from a single portal and for each subsequent consecutive invalid access attempt from that portal. 3-42

3.8.21 The access control software will signal an alarm when a tamper indication is received from protected portions of the portal. 3-42

3.8.22 The access control software will signal an alarm when any other monitored and unacceptable condition is detected. 3-42

4. GENERIC BLOCK DIAGRAM 4-1

5. GLOSSARY 5-1

1. MANAGEMENT OVERVIEW

1.1 INTRODUCTION

This report contains the guidance Functional Requirements for an Integrated Intrusion Detection and Access Control Annunciator System, and survey results of selected commercial systems. The survey questions were based upon the functional requirements; therefore, the results reflect which and sometimes how the guidance recommendations were met.

1.2 SURVEY BACKGROUND

The survey was conducted in the Summer of 1994, exploring the commercial sector to determine if commercial systems possess the capabilities necessary to wholly or partially meet U.S. Department of Energy needs. The majority of the questions reflect back upon specific Department of Energy requirements. Other questions were asked to clarify specific points. The surveys were conducted in person to avoid any misunderstanding of the questions and/or responses on the part of the vendor and/or Sandia National Laboratories.

Many systems appeared to be good candidates for this survey but logistical constraints permitted only a few of them to be surveyed. A selection process was used to determine which systems would be surveyed. This process ranked systems based upon their responses to selected questions from previous surveys. These questions identified specific needs which a system must meet for application within the Department of Energy. Based on the information available to us at the time, the ten best systems are represented in this survey.

1.3 ANNUNCIATOR DEFINITION

The guidance functional requirements and system survey in this report focus on the annunciator portion of a system. This report focuses on the annunciator functionality of a system. The actual end devices located in the field are not to be considered relevant to annunciator functionality. However, because annunciator functionality of an integrated system is tightly coupled to those same field devices, their interface to the annunciator and/or functionality is discussed.

1.4 REPORT COMPOSITION

This report consists of this management overview section and three other sections:

- Section 2 - Surveyed Firms and Systems. This section provides an overview of the firms participating in the survey, together with synopsis information on the systems they reported.
- Section 3 - Guidance and Survey Detail Tables. This section contains the guidance document and all the survey responses. The survey responses are in table form and accompany each element in the guidance.
- Section 4 - Glossary and Generic Block Diagram. This section contains a short glossary and a Generic Block Diagram of an integrated system.

1.5 REPORT VALIDITY

The data in this survey report have not been formally evaluated. Although every effort was made to encourage survey participants to be candid and truthful in their answers, the validity of individual responses has not been formally determined. This does not mean that the data cannot be used. However, it is suggested that direct comparisons among vendors be avoided.

1.6 SUGGESTED USE FOR REPORT DATA

Each guidance functional requirement in the report is immediately followed by the appropriate survey question and vendor responses. This report format allows users to quickly identify annunciator requirements and whether or not commercial systems may be able to meet them. As mentioned earlier, only a few systems are represented in this report. There may be several systems not included in this report which may meet a given site's needs. The commercial sector is at a point where there are few systems which possess truly unique capacities and/or functions. If systems represented in the survey have a particular capability, the probability is high that other systems also have that capability.

2. SURVEYED FIRMS AND SYSTEMS

This section provides narrative summaries concerning the products of firms that participated in this survey. Paragraph contents were extracted from vendor literature and survey replies. This information has *not* been independently verified by Sandia National Laboratories.

2.1 ADVANTOR CORPORATION

Advantor Corporation
6101 Lake Ellenor Drive
Orlando, Florida 32809

Advantor Corporation was founded in 1964 as Sonitrol Corporation. They utilized a sound activated intrusion detection system which allowed the central station operator to hear sounds emanating from the sensored area. In the fall of 1992, the company divested the Sonitrol franchise rights, and as of January 1993 Advantor Corporation concentrated on the technological development of customized, turn-key security networks.

Advantor's system is distributed, with intelligent field panels connected to the central station equipment. A single hardwired application of Advantor's AIMS Integrated Monitoring System will support a maximum of 768 collector/multiplexer panels, each with a maximum of 60 sensor points, for a total of 46,080 sensor points in the system. The access control portion of the system will support 320 doors with a maximum of 10,000 card holders per door. The intelligent field panels will function in a stand-alone-mode if communications between the host and itself is lost. During this time, it will store all transactions occurring locally, and will automatically upload that information upon the re-establishment of communications with the host. These panels will buffer up to 8,000 events internally.

System activity is displayed to the operator through text and graphic displays. The graphic display is for display only so the operator interfaces with the text screen. As system events occur they are automatically logged to a history file, as are any actions taken by the operator or other authorized user. All authorized users must log on and enter the correct password to gain access to the system. Passwords also determine what permissions any individual has while using the system.

The system supports several third party CCTV subsystems, allowing assessment through a CCTV subsystem.

The central station monitoring software runs on an 80486 based machine using the "Flex" operating system.

2.2 DSX ACCESS SYSTEMS INCORPORATED

DSX Access Systems Incorporated
12021 Plano Road
Suite 190
Dallas, Texas 75243

The DSX-1030 system is a PC based building/facility management and monitoring system used to control and monitor personnel and alarm activity. By making use of distributed processing, the DSX-1030 system integrates access control, alarm monitoring, CCTV, elevator and HVAC control, guard tour and video imaging into a single system.

This system provides three different control panels which can be combined to offer various combinations of card reader or keypad inputs, relay outputs, and alarm inputs. These field panels are intelligent, with a processor and memory on board. The normal mode of operation sees most event processing done in the field panels. This allows the panels to function when communications with the host is lost. Under these conditions, the panels will buffer up to 10,000 events, which will be uploaded to the host when communications is reestablished.

The first panel of every "location" is designated as the "Master." All subsequent panels are designated as "Slaves." These panels are identical except for switch settings. The Master is responsible for communications of all subsequent panels with the host. When the location is remote and operates by way of a modem, the remote Master buffers all "normal" transactions until its buffer is 80% full, at which time it initiates an upload to the host machine. All alarm events are immediately followed by a call to the host to annunciate the event. The host may be programmed to routinely poll each of the remote locations and collect the logs automatically.

A large configuration of this system will support 50,688 sensors points. Each panel will support a maximum of 16 end of line supervised alarm inputs.

The DSX-1030 system can be used in a networked configuration. This allows all functions to be executed at every workstation on the LAN. A maximum of 99 workstations are supported. Annunciation of system activities can be made at any of the workstations in addition to performing administrative functions such as generating reports and data base management. The actual annunciation of alarm events is made audibly and visually. If desired, the operator can bring up a graphic of the alarm area and has the option of zooming in to show more detail of the alarm area, or zooming out of the graphic to show more of the site. Up to 10,000 individual graphic screens are accommodated. These graphic images are for display only.

2.3 INFOGRAPHIC SYSTEMS

Infographic Systems
4462 Corporate Center Drive
Los Alamitos, California 90720

The Infographic Infoguard One-32 Plus system is a distributed system with a host computer, intelligent field panels, and field devices (sensors, card readers, etc.). The larger One-32 Plus-3 system will support monitoring of 8,192 alarm points, 512 card readers, and up to 50,000 card holders.

The distributed nature of the system allows access control functionality to remain if communications with the host should fail. In this event, the field panel would internally log all transactions taking place in that panel, and when communications are restored, that data would be uploaded to the host.

System activity is displayed to the operator in text and/or graphic form. In response to an intrusion alarm, the operator would be notified through a color coded text display. In addition, another monitor would display the appropriate graphic to give the operator a visual representation of the type and location of the alarm event. The operator does not interact with the graphic, it is used for display only. The operator interface at each terminal is completely menu driven through clear English language menus. Up to eight terminals are supported, and full functionality of the system is available from each terminal.

This system is available in an A-machine/B-machine redundant configuration. Memory in one machine is mirrored in the other. When some error condition occurs in the on-line machine, the system automatically switches to the stand-by machine and continues operating. During this time, no alarm data is lost, including alarm events coincident with a CPU failure.

A unique feature of the One-32 Plus system is the "monitor point verification." This feature allows the user to put an area into "test" mode and walk test an area without burdening the operator with the reporting of alarms. A summarized report can be generated later showing the walk test results.

A third party video subsystem is supported, and up to 512 discreet groups of cameras can be identified.

2.4 LAWRENCE LIVERMORE NATIONAL LABORATORY

Lawrence Livermore National Laboratory
7000 East Avenue
Livermore, California 94550

Argus is a security system developed at Lawrence Livermore National Laboratory. It is a security system with three integrated subsystems which are supported by a central computer system:

An automated access control system for personnel and equipment.

An electronic monitoring and alarm system to detect intruders and other unauthorized activities.

An information presentation system that integrates color map display, radio, and video systems.

Its redundant computers are designed for reliable operations 24 hours a day and through limited power outages. The number and size of Argus computers depends on site needs.

The access control subsystem is designed to monitor and control all access through selected entrances and exits. For maximum control and accountability, Argus permits security and program personnel to limit access to areas by clearance, group, individual, or by shift.

The monitoring and alarm system is designed to guard against unauthorized entry into high security areas, and to protect valuable equipment and information. Argus will monitor any sensor with a contact closure output. A collection of the monitoring equipment that protects a high-security area is grouped into an alarm station. A remote access panel (RAP) located outside each alarm station enables authorized access, local enrollment, and maintenance operations.

Argus presents alarms, problem reports, and the status of Argus monitored field equipment at ergonomically designed workstations for analysis by security personnel. Information is presented to the operator through combinations of color maps of the facility and a detailed text display. Radio and telephone lines are encrypted to make communications secure.

2.5 LOGIPLEX

Logiplex Corporation
5221 Southwest Corbett
PO Box 3428
Portland, Oregon 97208

The Logiplex system consists of the host machine, communications receivers, and intelligent field panels. The intelligent field panels are available in four types: Auditor Master and Remote, and Inquirer Master and Remote. The Auditor Master forms the first in a chain of up to 27 Auditor Remotes. Each chain has distance limitations beyond 3,000 feet, expandable to five miles by use of bus drivers. Each Auditor Remote, when fully loaded, will handle up to 96 individually annunciated sensor points, up to 8 entry control readers, and a total locally-stored data base of up to 12,000 card holders. The Inquirer is a smaller version of the Auditor, covering up to 24 sensor points, 4 readers, and up to 4,000 card holders.

The distributed nature of the system allows the field devices to operate when communications between the field panel and the host is lost. During this time, all transactions occurring at that panel are stored in internal memory. Up to 1,000 transactions may be stored. When communications between the field panel and the host is reestablished, the field panel will up-load its transaction log to the host machine. These field panels will also support the "printer-computer-interface." This device allows local annunciation of events through a real time printed report of all system activities.

The PC based systems operate on IBM AT compatible computers. They will communicate with the field panels directly, through the printer computer interface, or through modems. This system offers integration capabilities with expansion and convenient system design flexibility's in access control, intrusion monitoring, fire, intelligent CCTV switching interface, video image recording, guard tour, facilities management, industrial process control, and system wide map graphics.

The primary method of annunciation is made through a text screen. The system alerts the operator through a color coded text display to an alarm condition from a specific location and documents the operator's response. There is also a "Color Graphics" module which allows events to be displayed with color coded icons on maps. The graphic display may be viewed continuously, indicating all alarm events in real-time or as a single view of an alarm event.

2.6 MATRIX

Matrix Systems, Incorporated
7550 Paragon Road
P.O. Box 750038
Dayton, Ohio 45475

The Matrix R.9 is a "controlled access and security monitoring system". It is a distributed system, with intelligent components in the central station as well as in the field. In its large, networked configuration it will monitor up to 30,000 alarm points and 5,00 badge readers. This networked system contains a master data base in the host machine, and will support up to ten "node" systems. Each of these "node" subsystems are essentially stand alone smaller systems. Systems are available with a "hot" standby machine ready to automatically take control of the system if there is a fault in the on-line machine.

The intelligent alarm panels are available in a variety of configurations, providing various combinations of alarm monitoring, relay outputs, and intelligent badge readers. Up to 96 inputs, 48 outputs, and eight badge readers can be supported by a single intelligent alarm panel.

The intelligent field panels will store alarm activity in its internal memory, but access control events are buffered within the intelligent card readers themselves. In the event of a commercial power or communications failure, the card readers will continue to function normally, and the card reader will buffer a minimum of 1,24 transactions.

The primary operator interface is through a text terminal, but the Matrix "Color Graphic Alarm Display" displays the location, type and current status of alarm in graphic form. This package allows the user to create and edit floor plans, and display alarm points in the appropriate position on the floor plans. These alarm points are color coded to indicate status, and multiple levels of floor plans are possible.

This system will interface to fire and CCTV systems.

2.7 MOSLER INCORPORATED

Mosler Incorporated
One Security Place
Hamilton, Ohio 45012

Mosler's SmartLINX is a modular access control and alarm monitoring system that can integrate a variety of subsystems into a centrally controlled network. Each SmartLINX controller manages up to eight LINX plug-in modules that perform various functions. With the appropriate module, the SmartLINX controller processes information and makes access decisions at its local site.

Communications with the host computer can be made via dedicated dial-up or hard-wired lines, as well as optical fiber, broad band, or local area networks. Communications is need only when information changes or transactions need to be archived.

A listing of the modules which can be placed in SmartLINX will give an indication of the distributed functionality which exists in this system.

SmartRAM. This module turns a SmartLINX controller into a distributed processing field panel. Its on-board microprocessor and 1-4 MB of RAM provide full, independent processing at remote locations, even if communications with the host computer is lost.

SmartTALK. The SmartTALK modem lets SmartLINX communicate with the host computer over standard dial-up telephone lines.

SmartMUX. This multiplexer module connects SmartLINX controllers at any point in the system. Up to four levels of SmartLINX controllers are supported.

LINXREAD/SmartREAD. These reader interfaces are available for almost any type of card reader technology. Card reader technologies may be mixed within a system.

SmartMON. This alarm point monitor connects dry contact points to the SmartLINX system.

SmartCON. Sixteen high capacity relays let SmartLINX control external devices. These may be activated directly, by a time schedule, or in response to system events.

Annunciation and responses to system events can be made through text or graphic displays. This system also supports a video subsystem which may be used to help assess the cause of alarm events.

2.8 SMF SYSTEMS CORPORATION

SMF Systems Corporation
1 Embarcadero Center
Suite 4080
San Francisco, California 94111

The ACS-51 security system is a multitasking system operating with a data base management and report generating system. It will function with numerous card readers and is designed to offer a range of access control, alarm monitoring, and facility management features. Networking of the workstations allows flexibility in the configuration of terminals and data lines. Annunciation of system events can be made through a text display and/or a graphics display. Graphics may include color-coded maps of the site or building. These graphics may be drawn with the provided software, or can be imported from commercial CAD software. The graphics display may be configured with a touch screen, allowing the operator to interact with the graphic.

The ACS-51 system will interface to a CCTV subsystem permitting the operator to remotely assess alarm events. In response to an alarm, the appropriate CCTV camera view will be automatically displayed to the operator. The operator has the option of manually selecting camera views to display. This selection can be made from a keyboard or touch screen, eliminating the need for a separate control head.

Intelligent field panels with a local data base allow the system to continue to grant access if communications with the host machine is lost. Events occurring at that panel are buffered until communications with the host is reestablished. At that time, the activity log at the panel is uploaded to the host.

The 2110 field panels have multiple slots into which cards may be placed. The different cards lend different functionality to the 2110. The following types of cards are available: memory/microprocessor, communication multiplexer, alarm input, relay output, battery back-up, modem, and encryption.

The 3100 field panels can also perform access control in a "stand alone" mode, but its primary function is as a sensor interface panel. This panel will support eight sensor inputs and provides eight relays for outputs.

2.9 VIKONICS INCORPORATED

Vikonics Incorporated
370 North Street
Teterboro, New Jersey 07608

Vikonics markets several systems varying in capability and capacities. The system represented in this survey is the Visids 3500. The Visids 3500 is a distributed system, with intelligent field panels permitting local control for many functions. This system will interface to 8,196 uniquely identifiable alarm points in its standard configuration (Other large Vikonics systems will support 64,000 alarm points).

All events, whether authorized or not, can be displayed at one or more command center monitoring locations, sent to a printer for hard copy records, and logged to a disk for record keeping and future reporting. Intrusions and other unauthorized events are also audibly annunciated at the command centers, and locally if desired. All events are date and time stamped and reference the location and type of event, providing a complete audit trail of all activity.

The system informs security personnel of problems and automatically documents all security related events so that security personnel can quickly and effectively assess and respond to security problems.

Access control is performed with devices such as card readers, PIN keypads, and biometric identity verifiers. Card readers are available in various technologies including: magnetic stripe, weigand, barium ferrite, and proximity. The system will monitor for anti-passback and two person rule violations.

The intrusion detection portion of the system will monitor virtually any type of sensor. The alarm panels come in a variety of sizes and configurations and sizes, including units with local annunciation, local relay outputs to control response devices, or local secure/access capability. Local annunciation is accomplished both audibly and visually through status indicators affixed to the outside of an alarm panel. Sensors can be placed into access and back into secure mode locally using a secure/access device such as a keypad or keyswitch. The command center can also secure/access sensors, but can be restricted from doing so if required.

System events are annunciated through a text and/or graphics display. Color coded maps of the alarm site can be automatically displayed. Each status is represented with a different color.

The system will interface to several different CCTV systems. When an alarm occurs, the CCTV camera in that area can be automatically brought viewed on a specified CCTV monitor.

2.10 VINDICATOR INCORPORATED

Vindicator Incorporated
3001 Bee Caves Road
Austin, Texas 78746

Vindicator produces several security systems. The Vindicator Security Management and Reporting Terminal (S.M.A.R.T.) is their latest system. This system consists of the S.M.A.R.T. station linked with the Vindicator Ultra High Security (UHS) data gathering network. The S.M.A.R.T. station consists of a terminal, a multiplexer (CPU), and a printer. The UHS-Net Network comprises the UHS-8000 series gateways; the UHS-6800 series intrusion detection transponders, and the UHS-1401 entry control transaction processors. This is the system represented in this survey.

The S.M.A.R.T. multiplexer performs as the system CPU and the UHS-Net network system master. The UHS-Net network is a data gathering electronic distributed network designed specifically for a security system that requires the fast transmission of minimal bit alarm data packets. The entry control credential data is entered and maintained in a separate PC, however, each transaction processor locally controls and audits its associated portal without having to overload the alarm data bus.

The S.M.A.R.T. system will support a maximum of 10,000 alarm points. Up to eight annunciator stations (terminals) can be used, with full functionality from each. This is a distributed system, with intelligent components throughout the system. If communications between field panels and the host should be lost, the system will continue to function with little loss of performance. The communications between system components are encrypted with either a proprietary or DES encryption scheme.

Annunciation of system events is made through a text display, but a color graphics subsystem is available. At this time, the color graphics capability is for display only. The operator does not interface with the graphics.

If the application requires it, the S.M.A.R.T. system will interface with a CCTV subsystem to aid the operator in alarm assessment.

A second system, the Vindicator ECS-5000, was included in the survey although it was not the primary system of interest. Data on the ECS-5000 can be found in the survey detail table section.

2.11 WESTINGHOUSE SECURITY ELECTRONICS

Westinghouse Security Electronics
5452 Betsy Ross Drive
Santa Clara, California 95054

The Westinghouse SE6000 series security management system is represented in this survey. This stand alone SE6000 system will monitor 512 alarm points and 128 card readers. Up to 8,000 card holders can be enrolled into the system. Larger systems can be configured with multiple "local controllers" (host systems in a smaller configuration) reporting to a SE6000 host. This reporting can be made through a hardwired connection or over a modem.

The intelligent field panels contain a processor and a local data base which allows them to operate if communications with the host (or local controller) is lost. The field panels will interface to many types of devices. Door sensors, motion detectors, and temperature sensors can all be connected to field panels.

The SE6000 system will interface to several other systems. Among them are CCTV camera systems, elevator control, alarm monitoring interfaces, biometric devices, and video-badging systems.

The SE6000 has over 160 screens that may be viewed by a system user. The system administrator defines and determines access by limiting a system user to specific screens and functions. In addition to this, the system utilizes screen permissions. For each screen on the SE6000, the system administrator answers three yes/no questions to determine if the system user may add, delete, or change the information contained within each screen.

The SE6000 has the ability partition itself among several users. This partitioning allows each "tenant" access only to their own information. No tenant in the system is able to view or interact with another tenant's confidential information. To each tenant, it appears that they are the only user of the system. The one exception is "tenant 0," typically the system administrator. This person has global information access and is able to view everything that is entered and occurring within the system.

Alarms in the system can be displayed in graphic form on site maps. Icons on maps will change in color to annunciate the event. The position of the icon on the map will graphically indicate the location of the alarm event. The operator can acknowledge these events by interacting with the graphic screen.

3. SURVEY DETAIL TABLES

This report section provides detail tables of the integrated intrusion detection and access control annunciator systems survey results. The survey addresses eight major parameter areas:

- **Integrated System Annunciator - General Requirements.** This area deals with considerations involving general requirements for facility architecture, system performance, high availability, gradual degradation, maintenance, configuration management, system communication, and system access and accuracy.
- **Integrated System Annunciator - Software.** This area deals with considerations involving system software, software integrity, archiving, reports, database and reports structure, process control and exception handling.
- **Integrated System Annunicator - Hardware.** This area deals with considerations involving computer hardware and uninterruptible power sources.
- **Annunciator Alarm Processing - General Requirements.** This area deals with considerations involving alarm processing system communications with a sensor system which includes intrusion, duress, line supervision, and enclosure tamper sensors.
- **Annunciator Alarm Processing - Alarm Assessment.** This area deals with considerations involving direct and indirect assessment of alarms and assessment decision capabilities.
- **Access Control Annunciator - Access Credential.** This area deals with considerations involving badge types and badge interface capabilities.
- **Access Control Annunciator - Access Portal.** This area deals with considerations involving access authorizations and access portal functions.
- **Access Control Annunciator - Control Software.** This area deals with considerations involving access control software concerning access control logic and requirements.

3.1 FUNCTIONAL SPECIFICATIONS FOR THE INTEGRATED SYSTEM ANNUNCIATOR - GENERAL REQUIREMENTS

Requirements/Questions:

3.1.1 Central Alarm Stations shall display to the operator(s) all events which require a response.

3.1.1 Does your system display to the operator all events which require a response?

3.1.2 Facilities shall have a Secondary Alarm Station.

3.1.2a Does your system support multiple concurrent installations of itself?
3.1.2b What is the maximum number of annunciator stations (terminals) supported for your security system?
3.1.2c Does your system support master-master level annunciators (two or more annunciators able to act to control the entire network)?

3.1.3 The Secondary Alarm Station need not be fully redundant to the Central Alarm Station, but must be capable of providing effective control response to safeguards and security incidents.

3.1.3 Does your system support interaction with one annunciator while another is "display only?"

Firm Short Name	System Name	3.1.1	3.1.2a	3.1.2b	3.1.2c	3.1.3
Advantor	AIMS	Yes	Yes	7	Yes	Yes
DSX	DSX-1030 Series	Yes	Yes	99	Yes	No
Infographic	Infogard One-32 Plus	Yes	Yes	16	Yes	Yes
LLNL	Argus	Yes	Yes	Unlimited	Yes	Yes
Logiplex	Logiplex System	Yes	Yes	96	Yes	Yes
Matrix	R9.X System	Yes	Yes	75	Yes	Yes
Mosler	SmartLINX	Yes	Yes	256	Yes	Yes
SMF	ACS 51	Yes	Yes	64	Yes	Yes
Vikonics	Visids 4000	Yes	Yes	64	Yes	Yes
Vindicator	S.M.A.R.T.	Yes	Yes	8	Yes	Yes
	ECS-5000	Yes	Yes	2	Yes	Yes
Westinghouse	SE6000	Yes	Yes	12	Yes	No

Requirements/Questions:

3.1.3.1 A duress alarm at the Central Alarm Station shall annunciate at the Secondary Alarm Station. This will not be annunciated at the Central Alarm Station.

3.1.3.1 Will a duress alarm generated at the Central Alarm Station be annunciated at the Secondary Alarm Station without being annunciated at the Central Alarm Station?

3.1.3.2 A duress alarm at the Secondary Alarm Station shall annunciate at the Central Alarm Station. This will not be annunciated at the Secondary Alarm Station.

3.1.3.2 Will a duress alarm generated at the Secondary Alarm Station be annunciated at the Central Alarm Station without being annunciated at the Secondary Alarm Station?

3.1.4 On-line functions shall be treated by the system with a higher priority than off-line functions.

3.1.4 Are on-line functions treated by the system with a higher priority than off-line functions?

3.1.5 The time from the moment a sensor is activated to the moment it is audibly and visibly annunciated shall be under two seconds.

3.1.5 Is the time from the moment a sensor is activated to the moment that event is audibly and visibly annunciated less than two seconds?

3.1.6 The time from the moment a sensor is activated to the moment a video recording of the alarm scene is initiated shall be under one second.

3.1.6 Is the time from the moment a sensor is activated to the moment recording of that event has started less than one second?

Firm Short Name	System Name	3.1.3.1	3.1.3.2	3.1.4	3.1.5	3.1.6
Advantor	AIMS	Yes	Yes	Yes	Yes	Yes
DSX	DSX-1030 Series	No	No	Yes	Yes	No
Infographic	Infogard One-32 Plus	Yes	Yes	Yes	Yes	Yes
LLNL	Argus	Yes	Yes	Yes	Yes	Yes
Logiplex	Logiplex System	Yes	Yes	Yes	Yes	Yes
Matrix	R9.X System	Yes	Yes	Yes	Yes	Yes
Mosler	SmartLINX	Yes	Yes	Yes	Yes	Yes
SMF	ACS 51	Yes	Yes	Yes	Yes	Yes
Vikonics	Visids 4000	Yes	Yes	Yes	Yes	Yes
Vindicator	S.M.A.R.T.	Yes	Yes	Yes	Yes	Yes
	ECS-5000	Yes	Yes	Yes	Yes	No
Westinghouse	SE6000	Yes	Yes	Yes	Yes	Unknown

Requirements/Questions:

3.1.7 User requests for the status of sensors or system components shall be satisfied in less than two seconds.

3.1.7 Are user requests for the status of sensors or system components satisfied in less than two seconds?

3.1.8 The user shall receive instant feedback that the command was initiated.

3.1.8 Does the user receive instant (no perceptible delay) feedback that the command was initiated?

3.1.9 Off-line functions must be able to be aborted by the operator at any time.

3.1.9 Can off-line functions be aborted by the operator at any time?

Firm Short Name	System Name	3.1.7	3.1.8	3.1.9
Advantor	AIMS	Yes	Yes	Yes
DSX	DSX-1030 Series	Yes	Yes	Yes
Infographic	Infogard One-32 Plus	Yes	Yes	Yes
LLNL	Argus	Yes	Yes	Yes
Logiplex	Logiplex System	Yes	Yes	Yes
Matrix	R9.X System	Yes	N/A	Yes
Mosler	SmartLINX	Yes	Yes	Yes
SMF	ACS 51	Yes	Yes	Yes
Vikonics	Visids 4000	N/A	Yes	Yes
Vindicator	S.M.A.R.T.	Yes	Yes	Yes
	ECS-5000	Yes	Yes	Yes
Westinghouse	SE6000	No	Yes	Yes

Requirements/Questions:

3.1.10 There must be sufficient internal and external redundancy and fail-over mechanisms to preclude the loss of any single component from causing catastrophic failure of the system.

3.1.10a Does your system reside on a hardware/software platform which is fully fault tolerant?

3.1.10b Was your security application software engineered for fault tolerant operation on its platform?

3.1.10c Does your system possess the capability to operate on a multiprocessor hardware platform (one with more than a single CPU collocated in the same physical enclosure)?

3.1.10d Can your system operate if it loses one of the CPUs?

3.1.10e Does your system possess the capability to operate with mirrored rigid disks?

3.1.10f Was your system engineered to provide enhanced power supply reliability?

Firm Short Name	System Name	3.1.10a	3.1.10b	3.1.10c	3.1.10d	3.1.10e	3.1.10f
Advantor	AIMS	No	N/A	No	N/A	No	Yes-Built in UPS
DSX	DSX-1030 Series	Yes	N/A	No	N/A	Yes	Yes-Built in UPS
Infographic	Infogard One-32 Plus	Yes	Yes	No	N/A	Yes	Other-External UPS
LLNL	Argus	No	N/A	Yes	Yes-CPU in place, CPU removed	Yes	Yes-Built in UPS
Logiplex	Logiplex System	Yes	Yes	No	N/A	Yes	Yes-Built in UPS
Matrix	R9.X System	No	Yes	No	N/A	No	Yes-Built in UPS
Mosler	SmartLINX	Yes	Yes	Yes	Yes-CPU in place, CPU removed	Yes	Yes-Built in UPS
SMF	ACS 51	Yes	Yes	Yes	Yes-CPU in place	Yes	Yes-Built in UPS
Vikonics	Visids 4000	Yes	Yes	Yes	N/A	Yes	Yes-Built in UPS
Vindicator	S.M.A.R.T.	Yes	Yes	Yes	Yes- CPU in place, CPU removed	No	Yes-Multiple internal power supplies
	ECS-5000	Yes	No	Yes	Unknown	No	Yes-Multiple internal power supplies, External battery
Westinghouse	SE6000	No	No	No	N/A	Yes	Yes-Built in UPS

Requirements/Questions:

3.1.11 If a system component(s) suffers a malfunction or failure, system functionality (if affected) must degrade gradually, maintaining higher priority on-line functions as long as possible.

3.1.11 If the system suffers a degradation in performance of some component(s), is it able to maintain the function of higher-priority on-line functions as long as possible?

3.1.12 Tools and equipment necessary for a system maintainer to properly diagnose and repair system failures shall be provided as part of the maintenance support system.

3.1.12 Are tools (software and hardware) necessary for a system maintainer to properly diagnose and repair system failures provided as part of the maintenance support system?

3.1.13 Maintenance procedures, training, menu-driven test programs and self diagnostics shall be provided as part of the maintenance support system.

3.1.13 Are maintenance procedures, training, menu-driven test programs and self diagnostics provided as part of the maintenance support system?

Firm Short Name	System Name	3.1.11	3.1.12	3.1.13
Advantor	AIMS	Yes	Yes	Yes
DSX	DSX-1030 Series	Yes	Yes	Yes
Infographic	Infogard One-32 Plus	Yes	No	Yes
LLNL	Argus	Yes	Yes	Yes
Logiplex	Logiplex System	Yes	No	Yes
Matrix	R9.X System	Yes	Yes	Yes
Mosler	SmartLINX	Yes	Yes	Yes
SMF	ACS 51	Yes	Yes	Yes
Vikonics	Visids 4000	Yes	Yes	Yes
Vindicator	S.M.A.R.T.	Yes	Yes	Yes
	ECS-5000	Yes	Yes	Yes
Westinghouse	SE6000	No	Yes	Yes

Requirements/Questions:

3.1.14 Positive control and documentation of the product's development and changes are required.

3.1.14 Does the vendor maintain positive control and documentation of the development of their product?

3.1.14.1 Controls and audit trails for changes to the configuration are required.

3.1.14.1 Does the system maintain an audit trail of changes to its configuration?

3.1.14.2 The audit trail of all changes made to the stored data and code must be maintained in as automated fashion as possible.

3.1.14.2 Is the audit trail of all changes made to stored data and code maintained in an automated fashion?

3.1.14.3 The audit trail must be archived in non-volatile storage.

3.1.14.3 Is the audit trail maintained in non-volatile storage?

3.1.14.4 The audit trail must include but is not limited to the identification of the person(s) making the change, a description of the change made, and the date and time of the change.

3.1.14.4 Does the audit trail include, as a minimum, the identification of the person(s) making the change, a description of the change made, and the date and time of the change?

Firm Short Name	System Name	3.1.14	3.1.14.1	3.1.14.2	3.1.14.3	3.1.14.4
Advantor	AIMS	Yes	Yes	Yes	Yes	Yes
DSX	DSX-1030 Series	Yes	Yes	Yes	Yes	Yes
Infographic	Infogard One-32 Plus	Yes	Yes	Yes	Yes	Yes
LLNL	Argus	Yes	Yes	Yes	Yes	Yes
Logiplex	Logiplex System	Yes	Yes	Yes	Yes	Yes
Matrix	R9.X System	Yes	Yes	Yes	Yes	Yes
Mosler	SmartLINX	Yes	Yes	Yes	Yes	Yes
SMF	ACS 51	Yes	Yes	Yes	Yes	Yes
Vikonics	Visids 4000	Yes	Yes	Yes	Yes	Yes
Vindicator	S.M.A.R.T.	Yes	Yes	Yes	Yes	Yes
	ECS-5000	Yes	Yes	Yes	Yes	Yes
Westinghouse	SE6000	Yes	Yes	Yes	Yes	Yes

Requirements/Questions:

3.1.15 Communications between system components must be protected from compromise or spoofing as required in the relevant DOE orders.

3.1.15a Does your system use some form of data authentication between system components?
3.1.15b Does your system support some form of encryption between system components?
3.1.15c Does your system support network interface to other computers?
3.1.15d Are serial communications used to interface to other computers?
3.1.15e Can fiber optic media be used to interface to other computers?

Firm Short Name	System Name	3.1.15a	3.1.15b	3.1.15c	3.1.15d	3.1.15e
Advantor	AIMS	Yes	Yes, Proprietary/DES	Yes	Yes	Yes
DSX	DSX-1030 Series	Yes	Yes, DES	Yes	Yes	Yes
Infographic	Infogard One-32 Plus	Yes	Yes, DES	Yes	Yes	Yes
LLNL	Argus	Yes	Yes, Proprietary/DES	Yes	Yes	Yes
Logiplex	Logiplex System	Yes	Yes, Proprietary/DES	Yes	Yes	Yes
Matrix	R9.X System	Yes	Yes, Proprietary/DES	Yes	Yes	Yes
Mosler	SmartLINX	Yes	Yes, DES	Yes	Yes	Yes
SMF	ACS 51	Yes	Yes, DES	Yes	Yes	Yes
Vikonics	Visids 4000	Yes	Yes, Proprietary/DES	Yes	Yes	Yes
Vindicator	S.M.A.R.T.	No	Yes, Proprietary/DES	Yes	Yes	Yes
	ECS-5000	Yes	Yes, Proprietary/DES	Yes	Yes	Yes
Westinghouse	SE6000	Yes	No	Yes	Yes	Yes

Requirements/Questions:

3.1.15 Communications between system components must be protected from compromise or spoofing as required in the relevant DOE orders.

3.1.15f What other methodology can be used to interface to other computers?

3.1.16 If an exception reporting communications protocol is used, each data gathering panel (DGP) must be polled by an alarm annunciator at least once each hour.

3.1.16 Does your system have the capability to interrogate sensors and/or collectors/multiplexers for their current status?

3.1.17 The system must accurately display the correct state of every component of the system.

3.1.17 Can your system accurately display the correct state of every component of the system?

Firm Short Name	System Name	3.1.15f	3.1.16	3.1.17
Advantor	AIMS	TCP/IP	Yes	Yes
DSX	DSX-1030 Series	RF Modems	Yes	Yes
Infographic	Infogard One-32 Plus	Wireless RF Modems, Dedicated Telephone Lines	Yes	Yes
LLNL	Argus	TCP/IP	Yes	Yes
Logiplex	Logiplex System	TCP/IP	Yes	Yes
Matrix	R9.X System	RF Modems	Yes	Yes
Mosler	SmartLINX	TCP/IP	Yes	Yes
SMF	ACS 51	IBM Token Ring	Yes	Yes
Vikonics	Visids 4000	RF Microwave	Yes	Yes
Vindicator	S.M.A.R.T.	TTL	Yes	Yes
	ECS-5000	None	Yes	Yes
Westinghouse	SE6000	None	Yes	Yes

Requirements/Questions:

3.1.18 The system software shall have at least five levels of system access authorization to control: (1) access to operate functions, (2) read access to the data base, (3) read/write access to the data base, (4) read/write access to source code, and (5) read/write access to executable code.

3.1.18a Does your system have at least five levels of system access authorization which corresponds to access to operator functions?
3.1.18b Does your system have at least five levels of system access authorization which corresponds to read access to the data base?
3.1.18c Does your system have at least five levels of system access authorization which corresponds to read/write access to the data base?
3.1.18d Does your system have at least five levels of system access authorization which corresponds to read write access to source code?
3.1.18e Does your system have at least five levels of system access authorization which corresponds to read/write access to executable code?

Firm Short Name	System Name	3.1.18a	3.1.18b	3.1.18c	3.1.18d	3.1.18e
Advantor	AIMS	Yes	Yes	Yes	No	No
DSX	DSX-1030 Series	Yes	Yes	Yes	No	No
Infographic	Infogard One-32 Plus	Yes	Yes	Yes	No	No
LLNL	Argus	Yes	Yes	Yes	No	Yes
Logiplex	Logiplex System	Yes	Yes	Yes	No	No
Matrix	R9.X System	Yes	Yes	Yes	Yes	Yes
Mosler	SmartLINX	Yes	Yes	Yes	No	No
SMF	ACS 51	Yes	Yes	Yes	No	No
Vikonics	Visids 4000	Yes	Yes	Yes	No	No
Vindicator	S.M.A.R.T.	No	No	No	No	No
	ECS-5000	Yes	Yes	Yes	Yes	Yes
Westinghouse	SE6000	Yes	Yes	Yes	No	No

Requirements/Questions:

3.1.19 Each access authorization level shall be protected by password or credential control.

3.1.19a Is each access authorization level protected by a password or credential control?

3.1.19b Does your security system implement a two-person rule for any of the following operator actions?

3.1.20 The color scheme recommended for displaying events to the operator is: Red, Flashing Red, Yellow, and Green.

3.1.20 What color scheme is used to display events to the operator?

Firm Short Name	System Name	3.1.19a	3.1.19b	3.1.20
Advantor	AIMS	Yes	None	Red, Flashing Red, Yellow, Green, Blue, White, Magenta
DSX	DSX-1030 Series	Yes	None	Red, Black, Blue, Purple, Gray
Infographic	Infogard One-32 Plus	Yes	Database Modification	Red, Flashing Red, Yellow, Green
LLNL	Argus	Yes	Sensor State Change, Database Modification, Control Change	Red, Yellow, Green, Blue, White
Logiplex	Logiplex System	Yes	Sensor State Change, Database Modification, Control Change	Red, Flashing Red, Yellow, Green, Blue, Magenta
Matrix	R9.X System	Yes	Sensor State Change, Database Modification, Control Change	Red, Flashing Red, Green, Flashing Yellow
Mosler	SmartLINX	Yes	Sensor State Change, Database Modification, Control Change	Red, Flashing Red, Yellow, Green, Flashing Yellow
SMF	ACS 51	Yes	Sensor State Change, Database Modification, Control Change	Red, Flashing Red, Yellow, Green, Flashing Yellow
Vikonics	Visids 4000	Yes	None	Red, Flashing Red, Yellow, Green, Grey
Vindicator	S.M.A.R.T.	Yes	Sensor State Change	Red, Flashing Red, Yellow, Green, Blue
	ECS-5000	Yes	None	Red, Flashing Red, Yellow, Green
Westinghouse	SE6000	Yes	None	Red, Flashing Red, Yellow, Green

Requirements/Questions:

3.1.20.1 The system must be able to display system activity to the operator in graphic form.

3.1.20.1a Does your system have the ability to display system activity to the operator in graphic form which shows the location and type of event?

3.1.20.1b Does your system have the capability to represent field devices with icons on a graphic image?

3.1.20.1c Does your system support end-user modification of maps/graphics (size, scale, color shape, etc.)?

3.1.20.1d Does your system have the capability to create/draw maps, graphics, and icons?

3.1.20.1e Does your system support positioning of icons via "point and drag?"

Firm Short Name	System Name	3.1.20.1a	2.1.20.1b	3.1.20.1c	3.1.20.1d	3.1.20.1e
Advantor	AIMS	Yes	Yes	Yes	Yes	Yes
DSX	DSX-1030 Series	Yes	No	Yes	Yes	Yes
Infographic	Infogard One-32 Plus	Yes	Yes	Yes	Yes	Yes
LLNL	Argus	Yes	Yes	Yes	Yes	Yes
Logiplex	Logiplex System	Yes	Yes	Yes	Yes	Yes
Matrix	R9.X System	Yes	Yes	Yes	Yes	Yes
Mosler	SmartLINX	Yes	Yes	Yes	Yes	Yes
SMF	ACS 51	Yes	Yes	Yes	Yes	Yes
Vikonics	Visids 4000	Yes	Yes	Yes	Yes	Yes
Vindicator	S.M.A.R.T.	Yes	Yes	Yes	Yes	Yes
	ECS-5000	Yes	Yes	Yes	Yes	Yes
Westinghouse	SE6000	Yes	Yes	Yes	Yes	Yes

Requirements/Questions:

3.1.20.1 The system must be able to display system activity to the operator in graphic form.

3.1.20.1f Does your system support blinking icons?
3.1.20.1g Does your system support "shadow density icons?"
3.1.20.1h What is the maximum number of icons supported by your system?
3.1.20.1I What is the maximum number of icons which can be displayed simultaneously on a single graphic image?

Firm Short Name	System Name	3.1.20.1f	3.1.20.1g	3.1.20.1h	3.1.20.1i
Advantor	AIMS	Yes	No	18	1,000
DSX	DSX-1030 Series	Yes	No	2	Unknown
Infographic	Infogard One-32 Plus	Yes	No	16	Unlimited
LLNL	Argus	Yes	No	Unlimited	Unlimited
Logiplex	Logiplex System	Yes	No	37,000	Unknown
Matrix	R9.X System	Yes	No	124	Unknown
Mosler	SmartLINX	Yes	No	Disk Space Dependent	Screen Space Dependent
SMF	ACS 51	Yes	Yes	70	Screen Space Dependent
Vikonics	Visids 4000	Yes	No	Disk Space Dependent	Screen Space Dependent
Vindicator	S.M.A.R.T.	Yes	No	10,000	50
	ECS-5000	Yes	No	Unlimited	200+
Westinghouse	SE6000	Yes	No	Unknown	Unknown

Requirements/Questions:

3.1.20.1 The system must be able to display system activity to the operator in graphic form.

3.1.20.1j Does your system support a change in icon attributes in response to a system event?

3.1.20.1k Does your system have the capability to import existing hard copy/paper maps and graphics via scanning?

3.1.20.1l What graphic file formats are supported by your system?

Firm Short Name	System Name	3.1.20.1j	3.1.20.1k	3.1.20.1l
Advantor	AIMS	Yes	Yes	BMP
DSX	DSX-1030 Series	Yes	No	PCX
Infographic	Infogard One-32 Plus	Yes	No	PIC
LLNL	Argus	Yes	Yes	World Data Bank, Tiger, Dime, Autocad, DXF, Teknikad
Logiplex	Logiplex System	Yes	Yes	TIFF, DXF
Matrix	R9.X System	Yes	No	TIFF
Mosler	SmartLINX	Yes	Yes	DXF, BMP, TIFF
SMF	ACS 51	Yes	Yes	DXF
Vikonics	Visids 4000	Yes	Yes	PCX
Vindicator	S.M.A.R.T.	Yes	No	None
	ECS-5000	Yes	Yes	RSTR, TIFF, VMF
Westinghouse	SE6000	Yes	No	None

Requirements/Questions:

3.1.21 Interaction with the system must be possible, as a minimum, through a keyboard and/or by interfacing with a graphic screen.

3.1.21a If the operator interacts with the system through the graphic screen with a pointing device, can alarm events be acknowledged?

3.1.21b If the operator interacts with the system through the graphic screen with a pointing device, can individual alarms be activated and deactivated?

3.1.21c If the operator interacts with the system through the graphic screen with a pointing device, can alarms be activated and deactivated by groups?

3.1.21d If the operator interacts with the system through the graphic screen with a pointing device, can other system devices be controlled?

Firm Short Name	System Name	3.1.21a	3.1.21b	3.1.21c	3.1.21d
Advantor	AIMS	No	No	No	No
DSX	DSX-1030 Series	N/A	N/A	N/A	N/A
Infographic	Infogard One-32 Plus	No	No	No	No
LLNL	Argus	Yes	Yes	Yes	Yes
Logiplex	Logiplex System	Yes	Yes	Yes	No
Matrix	R9.X System	No	No	No	No
Mosler	SmartLINX	Yes	Yes	Yes	Yes
SMF	ACS 51	Yes	Yes	Yes	Yes
Vikonics	Visids 4000	No	No	No	No
Vindicator	S.M.A.R.T.	Yes	Yes	Yes	Yes
	ECS-5000	Yes	Yes	Yes	Yes
Westinghouse	SE6000	Yes	Yes	Yes	Yes

3.2 FUNCTIONAL SPECIFICATIONS FOR THE INTEGRATED SYSTEM ANNUNCIATOR -SOFTWARE

Requirements/Questions:

3.2.1 The operating system may be from any proven commercial source. It must be a current, supported version.

3.2.1 Is your operating system a current supported version from a proven, commercial source?

3.2.2 Database, compilers, and other system software must also be current and supported.

3.2.2 Is all other system software current and supported?

3.2.3 The source code must either be provided by the supplier, or held in escrow by a third party.

3.2.3 Is the source code provided by the vendor or held in escrow by a third party?

3.2.4 The source code placed in escrow must be identical to the software supplied.

3.2.4 Are procedures in place to insure that the source code placed in escrow is identical to the software supplied?

3.2.5 As the software is revised, the source maintained in escrow must also be revised.

3.2.5 Are procedures in place to insure that when software is revised the source maintained in escrow is also revised?

Firm Short Name	System Name	3.2.1	3.2.2	3.2.3	3.2.4	3.2.5
Advantor	AIMS	Yes	Yes	Escrow	Yes	Yes
DSX	DSX-1030 Series	Yes	Yes	Escrow	Yes	Yes
Infographic	Infogard One-32 Plus	Yes	Yes	Escrow	Yes	Yes
LLNL	Argus	Yes	Yes	Provided	Yes	Yes
Logiplex	Logiplex System	Yes	Yes	Provided, Escrow	Yes	Yes
Matrix	R9.X System	Yes	Yes	Provided, Escrow	Yes	Yes
Mosler	SmartLINX	Yes	Yes	Escrow	Yes	Yes
SMF	ACS 51	Yes	Yes	Escrow	Yes	Yes
Vikonics	Visids 4000	Yes	Yes	Escrow	Yes	Yes
Vindicator	S.M.A.R.T.	Yes	Yes	Escrow	Yes	Yes
	ECS-5000	Yes	Yes	Escrow	Yes	Yes
Westinghouse	SE6000	Yes	Yes	Escrow	Yes	Yes

Requirements/Questions:

3.2.6 The integrity of the system hardware and software should be monitored in an automated fashion such that failures and tampering are detected and reported.

3.2.6 Is the integrity of the system hardware and software monitored in an automated fashion such that failures and tampering are detected and reported?

3.2.6.1 Failures must be communicated to the operator.

3.2.6.1 Are all system know failures annunciated to the operator?

3.2.7 The system must log all system known events/transactions.

3.2.7a Does your system possess some form of activity audit trail, records, logs, or other similar storage and reporting capability which records all system activity?
3.2.7b Which database architecture is supported by your security system?
3.2.7c Does your system support the capability to accomplish ad hoc queries?

Firm Short Name	System Name	3.2.6	3.2.6.1	3.2.7a	3.2.7b	3.2.7c
Advantor	AIMS	Yes	Yes	Yes	Relational, Network	No
DSX	DSX-1030 Series	Yes	Yes	Yes	Relational	Yes
Infographic	Infogard One-32 Plus	Yes	Yes	Yes	Hierarchical	Yes
LLNL	Argus	Yes	Yes	Yes	Relational	Yes
Logiplex	Logiplex System	Yes	Yes	Yes	Relational	Yes
Matrix	R9.X System	Yes	Yes	Yes	Index, Proprietary	Yes
Mosler	SmartLINX	Yes	Yes	Yes	Index, Proprietary	No
SMF	ACS 51	Yes	Yes	Yes	Relational	Yes
Vikonics	Visids 4000	Yes	Yes	Yes	Hierarchical, Relational, Network	Yes
Vindicator	S.M.A.R.T.	Yes	Yes	Yes	Relational	Yes
	ECS-5000	Yes	Yes	Yes	Relational	Yes
Westinghouse	SE6000	Yes	Yes	Yes	Relational	Yes

Requirements/Questions:

3.2.8 The system must allow the operator to archive data on command.

3.2.8 Does the system allow the operator to archive data on command?

3.2.9 Archiving will be made to a nonvolatile media.

3.2.9 Is all archiving made to a nonvolatile media?

3.2.10 The software must allow the operator to produce both formatted and ad hoc reports of any data contained in the central database and the audit trail files.

3.2.10a Does your system possess the capability to generate reports?
3.2.10b Does your system support the capability to accomplish ad hoc queries by use of a single query for multiple tables with logical qualifications?
3.2.10c Are logs individually namable within the total number of logs supported?

Firm Short Name	System Name	3.2.8	3.2.9	3.2.10a	3.2.10b	3.2.10c
Advantor	AIMS	Yes	Yes	Paper, File, CRT/Display	No	No
DSX	DSX-1030 Series	Yes	Yes	Paper, File, CRT/Display	Yes	Yes
Infographic	Infogard One-32 Plus	Yes	Yes	Paper, CRT/Display	Yes	Yes
LLNL	Argus	Yes	Yes	Paper, CRT/Display	Yes	Yes
Logiplex	Logiplex System	Yes	Yes	Paper, File, CRT/Display	Yes	No
Matrix	R9.X System	Yes	Yes	Paper, File, CRT/Display	Yes	Yes
Mosler	SmartLINX	Yes	Yes	Paper, File, CRT/Display, Tape Media	N/A	N/A
SMF	ACS 51	Yes	Yes	Paper, File, CRT/Display	Unknown	Unknown
Vikonics	Visids 4000	Yes	Yes	Paper, File, CRT/Display, Other Computers	Yes	Yes
Vindicator	S.M.A.R.T.	Yes	Yes	Paper, CRT/Display	Yes	Yes
	ECS-5000	Yes	Yes	Paper, CRT/Display	Yes	Yes
Westinghouse	SE6000	Yes	Yes	Paper, CRT/Display	Yes	Yes

Requirements/Questions:

3.2.10 **The software must allow the operator to produce both formatted and ad hoc reports of any data contained in the central database and the audit trail files.**

3.2.10d Which of the indicated forms of report generation are supported by your system?

3.2.10e Does your system support a screen print capability where any alphanumeric log display is also capable of a hard copy generation on a printer?

3.2.10f Does your system support a variable screen report format where on-screen alphanumeric data can be displayed in variable formats?

3.2.10g Does your system support variable hard-copy report formats where hard-copy alphanumeric data can be displayed in variable formats?

Firm Short Name	System Name	3.2.10d	3.2.10e	3.2.10f	3.2.10g
Advantor	AIMS	Preprogrammed, Preformatted, Ad Hoc	Yes	No	No
DSX	DSX-1030 Series	Preprogrammed, Preformatted, Ad Hoc	Yes	No	No
Infographic	Infogard One-32 Plus	Preprogrammed, Preformatted, Ad Hoc	Yes	Yes	Yes
LLNL	Argus	Preprogrammed, Preformatted, Ad Hoc	Yes	Yes	Yes
Logiplex	Logiplex System	Preprogrammed, Preformatted, Ad Hoc	Yes	Yes	Yes
Matrix	R9.X System	Preprogrammed, Preformatted, Ad Hoc	No	No	No
Mosler	SmartLINX	Preprogrammed, Preformatted, Ad Hoc	Yes	Yes	Yes
SMF	ACS 51	Preprogrammed, Preformatted, Ad Hoc, External Device	Yes	Yes	Yes
Vikonics	Visids 4000	Preprogrammed, Preformatted, Ad Hoc	Yes	Yes	Yes
Vindicator	S.M.A.R.T.	Preprogrammed, Preformatted	No	No	No
	ECS-5000	Preprogrammed, Preformatted	Yes	No	No
Westinghouse	SE6000	Preprogrammed, Preformatted, Ad Hoc	Yes	Yes	Yes

Requirements/Questions:

3.2.11 The system must allow creation, queries, modifications, and deletions of database items.

3.2.11a Does your system permit an authorized operator to modify database items?
3.2.11b Does your system permit an authorized operator to delete database items?
3.2.11c Does your system permit an authorized operator to examine/extract a data subset on any attribute?
3.2.11d Does your system permit an authorized operator to examine/extract a data subset by time?
3.2.11e Does your system permit an authorized operator to examine/extract a data subset by event type?

Firm Short Name	System Name	3.2.11a	3.2.11b	3.2.11c	3.2.11d	3.2.11e
Advantor	AIMS	Yes	Yes	No	Yes	Yes
DSX	DSX-1030 Series	Yes	Yes	Yes	Yes	Yes
Infographic	Infogard One-32 Plus	Yes	Yes	Yes	Yes	Yes
LLNL	Argus	Yes	Yes	Yes	Yes	Yes
Logiplex	Logiplex System	Yes	Yes	Yes	Yes	Yes
Matrix	R9.X System	Yes	Yes	No	No	No
Mosler	SmartLINX	Yes	Yes	Yes	Yes	Yes
SMF	ACS 51	Yes	Yes	Yes	Yes	Unknown
Vikonics	Visids 4000	Yes	Yes	Yes	Yes	Yes
Vindicator	S.M.A.R.T.	Yes	Yes	No	Yes	Yes
	ECS-5000	Yes	Yes	Yes	Yes	Yes
Westinghouse	SE6000	Yes	Yes	Yes	Yes	Yes

Requirements/Questions:

3.2.11 The system must allow creation, queries, modifications, and deletions of database items.

3.2.11f Does your system permit an authorized operator to do logical comparisons within attributes?

3.2.11g Does your system permit an authorized operator to do arithmetic operations (count, sum, average) within attributes?

3.2.12 The preceding functions shall be accomplished in a manner that isolates the user from the underlying structure.

3.2.12 Are operator's creations, queries, modifications, and deletions of database items performed in a manner which isolated the operator from the underlying structure?

Firm Short Name	System Name	3.2.11f	3.2.11g	3.2.12
Advantor	AIMS	No	Yes	Yes
DSX	DSX-1030 Series	No	Yes	Yes
Infographic	Infogard One-32 Plus	No	Yes	Yes
LLNL	Argus	Yes	Yes	Yes
Logiplex	Logiplex System	No	No	Yes
Matrix	R9.X System	No	No	No
Mosler	SmartLINX	Yes	No	Yes
SMF	ACS 51	Unknown	Yes	Yes
Vikonics	Visids 4000	Yes	No	No
Vindicator	S.M.A.R.T.	No	No	Yes
	ECS-5000	No	No	Yes
Westinghouse	SE6000	Yes	Yes	Yes

Requirements/Questions:

3.2.13 When alarm processing determines that the status of a sensor and/or logical group has changed, it must be able to inform other systems.

3.2.13 When the system determiries that there has been a change of status within the system, which subsystems can it inform?

3.2.14 Whenever event processing encounters an error condition, a message shall be printed to either a maintenance or console operator's log or display depending on the severity of the error.

3.2.14 Are system error conditions reported either to a maintenance or console operator's log?

Firm Short Name	System Name	3.2.13	3.2.14
Advantor	AIMS	CCTV. Text Display, Map Display, Horn, Log, Remote Annunciator	Yes
DSX	DSX-1030 Series	CCTV, Text Display, Map Display, Horn, Log, Remote Annunciator	Yes
Infographic	Infogard One-32 Plus	CCTV, Text Display, Map Display, Horn, Log, Remote Annunciator, Printer, External Lights	Yes
LLNL	Argus	CCTV, Text Display, Map Display, Horn, Log, Remote Annunciator	Yes
Logiplex	Logiplex System	CCTV, Text Display, Map Display, Horn, Log, Remote Annunciator	Yes
Matrix	R9.X System	CCTV, Text Display, Map Display, Horn, Log, Remote Annunciator	Yes
Mosler	SmartLINX	CCTV, Text Display, Map Display, Horn, Log, Remote Annunciator	Yes
SMF	ACS 51	CCTV, Text Display, Map Display, Horn, Log, Remote Annunciator	Yes
Vikonics	Visids 4000	CCTV, Text Display, Map Display, Horn, Log, Remote Annunciator	Yes
Vindicator	S.M.A.R.T.	CCTV, Text Display, Map Display, Horn, Log, Remote Annunciator	Yes
	ECS-5000	CCTV, Text Display, Map Display, Horn, Log, Remote Annunciator	Yes
Westinghouse	SE6000	CCTV, Text Display, Map Display, Horn, Log, Remote Annunciator	Yes

3.3 FUNCTIONAL SPECIFICATIONS FOR THE INTEGRATED SYSTEM ANNUNCIATOR - HARDWARE

Requirements/Questions:

3.3.1 The system shall be capable of handling a 50% increase in system capacity and continue to meet the original performance requirements states in 2.1.1 without software or hardware modifications.

3.3.1a What is the maximum number of alarms controlled by a single annunciator?

3.3.1b What is the maximum number of sensors the collector/multiplexer can interface with and individually identify?

3.3.1c What is the maximum number of collectors/multiplexers the annunciator may interface to?

3.3.2 he system shall be designed to provide event reporting with no loss of data for a period of no less than eight hours after the loss of primary power.

3.3.2 Can the system be configured to provide transaction reporting and control with no loss of data for a period of no less than eight hours after the loss of primary power?

3.3.3 he operator shall be notified within ten seconds upon the loss of primary power in any part of the system.

3.3.3 Is the operator notified of the loss of power within ten seconds upon the loss of primary power to any component of the system?

Firm Short Name	System Name	3.3.1a	3.3.1b	3.3.1c	3.3.2	3.3.3
Advantor	AIMS	4,6080	60	768	Yes	Yes
DSX	DSX-1030 Series	50,688	16	4,950	Yes	No
Infographic	Infogard One-32 Plus	8,192	196	512	Yes	Yes
LLNL	Argus	Unlimited	400	10,000	Yes	Yes
Logiplex	Logiplex System	37,000	128	10	Yes	Yes
Matrix	R9.X System	7,500	96	78	Yes	Yes
Mosler	SmartLINX	9,999	128	128	Yes	Yes
SMF	ACS 51	20,000	112	1,024	Yes	Yes
Vikonics	Visids 4000	8,196	64	1,000	Yes	Yes
Vindicator	S.M.A.R.T.	10,000	16	250	Yes	Yes
	ECS-5000	2,016	8	252	Yes	Yes
Westinghouse	SE6000	8,064	63	128	Yes	Yes

Requirements/Questions:

3.3.4 Switching to back-up power must be automatic upon the loss of primary power.

3.3.4 Is the switching to back-up power automatic upon the loss of primary power?

3.3.5 Back-up power must be applied in such a manner that no system component will be without power in the event of a loss of commercial power.

3.3.5 Is back-up power applied in such a manner that no system component will be without power in the event of the loss of commercial power?

Firm Short Name	System Name	3.3.4	3.3.5
Advantor	AIMS	Yes	Yes
DSX	DSX-1030 Series	Yes	N/A
Infographic	Infogard One-32 Plus	Yes	Yes
LLNL	Argus	Yes	Yes
Logiplex	Logiplex System	Yes	Yes
Matrix	R9.X System	Yes	Yes
Mosler	SmartLINX	Yes	Yes
SMF	ACS 51	Yes	Yes
Vikonics	Visids 4000	Yes	Yes
Vindicator	S.M.A.R.T.	Yes	Yes
	ECS-5000	Yes	Yes
Westinghouse	SE6000	Yes	Yes

3.4 ALARM PROCESSING SYSTEM FUNCTIONAL SPECIFICATIONS FOR ANNUNCIATORS - GENERAL REQUIREMENTS

Requirements/Questions:

3.4.1 The alarm processing system must be capable of individually monitoring and annunciating the status of all sensors in the system.

3.4.1a Does your system have the capability to interface to sensors with two state outputs?
3.4.1b Does your system have the capability to interface to sensors with analog outputs?
3.4.1c Does your system have some methodology for handling of "simultaneous" alarms?

3.4.2 The alarm processing system must be capable of visually and audibly annunciating to the operator a change in sensor status within 1 second of the change if less than 25% of the system's sensors alarm simultaneously, and within 3 seconds if 25% or more of the system's sensors alarm simultaneously.

3.4.2a Which audio outputs are provided with and routinely supported by your security system?
3.4.2b Does your system support presentation of data via some combination of maps/drawings, icons, character data, other, or none?

Firm Short Name	System Name	3.4.1a	3.4.1b	3.4.1c	3.4.2a	3.4.2b
Advantor	AIMS	Yes	No	Yes	Internal Speaker, Separate Horn, External Speaker	Maps/Drawings, Icons, Character Data
DSX	DSX-1030 Series	Yes	No	Yes	Internal Speaker	Maps/Drawings, Icons, Character Data
Infographic	Infogard One-32 Plus	Yes	No	Yes	Internal Speaker	Maps/Drawings, Character Data
LLNL	Argus	Yes	Yes	Yes	Internal Speaker	Maps/Drawings, Icons, Character Data
Logiplex	Logiplex System	Yes	Yes	Yes	Internal Speaker, Separate Horn	Maps/Drawings, Icons, Character Data, LEDs
Matrix	R9.X System	Yes	No	Yes	Internal Speaker	Maps/Drawings, Icons, Character Data
Mosler	SmartLINX	Yes	No	Yes	Internal Speaker, Separate Horn	Maps/Drawings, Icons, Character Data
SMF	ACS 51	Yes	No	Yes	Internal Speaker, Sound Board, MIDI Board, Separate Horn	Maps/Drawings, Icons, Character Data
Vikonics	Visids 4000	Yes	No	Yes	Internal Speaker, Sound Board, Separate Horn	Maps/Drawings, Icons, Character Data
Vindicator	S.M.A.R.T.	Yes	Yes	Yes	Internal Speaker, Separate Horn	Maps/Drawings, Character Data
	ECS-5000	Yes	Yes	Yes	Internal Speaker, Separate Horn	Maps/Drawings, Icons, Character Data
Westinghouse	SE6000	Yes	No	Yes	Internal Speaker	Maps/Drawings, Icons, Character Data

Requirements/Questions:

3.4.3 The alarm processing system shall be capable of supervising the communications between the primary host processing computer and the sensors.

3.4.3 Does your system supervise the communications between the primary host processing computer and the sensors?

3.4.4 The alarm processing system shall be capable of ignoring intrusion sensor alarms if requested by an authorized operator.

3.4.4 Is your system able to ignore intrusion alarms if requested by an authorized operator?

3.4.5 The alarm processing system shall be capable of uniquely identifying, by both color and text, the following sensor and logical group states: Secure, Access, New Alarm, Alarm, Alarm Gone, New Tamper Alarm, Tamper Alarm, Tamper Alarm Gone, Off-line, and Failed.

3.4.5a Which sensor and logical group states is your system able to identify, by both color and text?

Firm Short Name	System Name	3.4.3	3.4.4	3.4.5a
Advantor	AIMS	Yes	Yes	Secure, Access, New Alarm, Alarm, New Tamper Alarm, Tamper Alarm, Off-line, Restore
DSX	DSX-1030 Series	Yes	Yes	Secure, Access, New Alarm, Alarm, New Tamper, Tamper Alarm, Failed, Bypass
Infographic	Infogard One-32 Plus	Yes	Yes	Secure, Access, New Alarm, Alarm, Alarm Gone, New Tamper Alarm, Tamper Alarm, Tamper Alarm Gone, Deactivate
LLNL	Argus	Yes	No	Secure, Access, New Alarm, Alarm, Alarm Gone, New Tamper Alarm, Tamper Alarm, Tamper Alarm Gone, Off-line, Failed
Logiplex	Logiplex System	Yes	Yes	Secure, Access, New Alarm, Alarm, Alarm Gone, New Tamper Alarm, Tamper Alarm, Tamper Alarm Gone, Disabled, Failed
Matrix	R9.X System	Yes	Yes	Secure, Access, New Alarm, Tamper Alarm
Mosler	SmartLINX	Yes	Yes	Secure, Access, New Alarm, Alarm, New Tamper Alarm, Tamper Alarm, Off-line
SMF	ACS 51	Yes	Yes	Secure, Access, New Alarm, Alarm, Alarm Gone, New Tamper Alarm, Tamper Alarm Gone, Off-line, Trouble
Vikonics	Visids 4000	Yes	Yes	Secure, Access, New Alarm, Alarm, New Tamper Alarm, Tamper Alarm, Maintenance
Vindicator	S.M.A.R.T.	Yes	Yes	Secure, Access, New Alarm, Alarm, Alarm Gone, New Tamper Alarm, Tamper Alarm, Tamper Alarm Gone, Off-line, Failed
	ECS-5000	Yes	Yes	Secure, Access, New Alarm, Alarm, Alarm Gone, New Tamper Alarm, Tamper Alarm, Tamper Alarm Gone, Failed
Westinghouse	SE6000	Yes	Yes	Secure, Access, New Alarm, Alarm, New Tamper Alarm, Tamper Alarm, Failed

Requirements/Questions:

3.4.5 The alarm processing system shall be capable of uniquely identifying, by both color and text, the following sensor and logical group states: Secure, Access, New Alarm, Alarm, Alarm Gone, New Tamper Alarm, Tamper Alarm, Tamper Alarm Gone, Off-line, and Failed.

3.4.5b What is the maximum number of intrusion detection alarm states supported by your system?

3.4.5c How many of these states may be uniquely identified on your display?

3.4.5d How many of these states may be uniquely identified in a log/database entry?

3.4.5e How many intrusion detection alarm states are automatically defined on your system?

3.4.6 The alarm processing system shall be capable of calculating a new status and displaying that status for any given sensor based on sensor input, environmental conditions, and user input.

3.4.6 Is your system capable of calculating a new status and displaying that status for any given sensor based on sensor input, environmental conditions, and user input?

Firm Short Name	System Name	3.4.5b	3.4.5c	3.4.5d	3.4.5e	3.4.6
Advantor	AIMS	16	16	16	16	No
DSX	DSX-1030 Series	7	7	7	7	Yes
Infographic	Infogard One-32 Plus	8	8	8	8	Yes
LLNL	Argus	6	6	6	6	Yes
Logiplex	Logiplex System	6	6	6	6	No
Matrix	R9.X System	4	4	4	4	No
Mosler	SmartLINX	5	5	5	5	Yes
SMF	ACS 51	6	6	6	6	Yes
Vikonics	Visids 4000	7	7	7	7	No
Vindicator	S.M.A.R.T.	710	22	22	22	Yes
	ECS-5000	5	2	2	2	Yes
Westinghouse	SE6000	7	7	7	7	Yes

Requirements/Questions:

3.4.7 The alarm processing system shall be capable of permitting the operator to place sensors "in access."

3.4.7 Is your system capable of permitting the operator to place sensors "in access?"

3.4.8 The alarm processing system shall be capable of prioritizing alarms from all sensors.

3.4.8a Does your system support assignment of priorities to events (state changes)?
3.4.8b Does your system support end-user assignment of priorities to events (state changes)?

3.4.9 The alarm processing system shall be capable of changing the current priority of any given sensor or logical group based on input received from other components/systems.

3.4.9 Is your system capable of changing the current priority of any given sensor or logical group based on input received from other components/systems?

3.4.10 The alarm processing system shall be capable of adding and deleting sensors in a logical group based on user input.

3.4.10 Is your system capable of adding and deleting sensors in a logical group based on user input?

3.4.11 The alarm processing system shall be capable of adding and deleting a logical group.

3.4.11 Is your system capable of adding and deleting a logical group?

Firm Short Name	System Name	3.4.7	3.4.8a	3.4.8b	3.4.9	3.4.10	3.4.11
Advantor	AIMS	Yes	Yes	Yes	No	Yes	Yes
DSX	DSX-1030 Series	Yes	Yes	Yes	Yes	No	N/A
Infographic	Infogard One-32 Plus	Yes	Yes	Yes	No	Yes	No
LLNL	Argus	Yes	Yes	Yes	Yes	Yes	Yes
Logiplex	Logiplex System	Yes	Yes	Yes	No	Yes	No
Matrix	R9.X System	Yes	Yes	Yes	No	No	No
Mosler	SmartLINX	Yes	Yes	Yes	No	Yes	Yes
SMF	ACS 51	Yes	Yes	Yes	No	Yes	Yes
Vikonics	Visids 4000	Yes	Yes	Yes	No	Yes	Yes
Vindicator	S.M.A.R.T.	Yes	Yes	No	Yes	No	No
	ECS-5000	Yes	Yes	Yes	Yes	Yes	Yes
Westinghouse	SE6000	Yes	Yes	Yes	No	Yes	Yes

3.5 ALARM PROCESSING SYSTEM FUNCTIONAL SPECIFICATIONS FOR ANNUNCIATORS - ALARM ASSESSMENT

Requirements/Questions:

3.5.1 The system must possess the capability to permit the operator to enter the assessment decision made by the operator into the database.

3.5.1 Does your system support an operator on-screen detailed entry capability to indicate results of event responses?

3.5.2 Alarms must be assessed as to their cause by either direct or indirect (CCTV) personnel observation or a combination of both.

3.5.2 Does your system facilitate the assessment of alarms by direct personnel observation, CCTV, or both?

3.5.2.1 CCTVs used for assessment must be able to be automatically switched (and aimed if PTZ) to display a preprogrammed camera image on the desired monitor.

3.5.2.1a Does your system have the capability to interface to fixed position CCTV cameras?
3.5.2.1b How many CCTV cameras can your system identify?
3.5.2.1c Does your system have the capability to interface to PTZ CCTV cameras?

Firm Short Name	System Name	3.5.1	3.5.2	3.5.2.1a	3.5.2.1b	3.5.2.1c
Advantor	AIMS	Yes	Yes	Yes	Unknown	Unknown
DSX	DSX-1030 Series	Yes	Yes	Yes	50	Yes
Infographic	Infogard One-32 Plus	Yes	Yes	Yes	Unknown	Yes
LLNL	Argus	Yes	Yes	Yes	1,024	Yes
Logiplex	Logiplex System	Yes	Yes	Yes	Unknown	Yes
Matrix	R9.X System	Yes	Yes	Yes	Unknown	Unknown
Mosler	SmartLINX	Yes	Yes	Yes	9,999	Yes
SMF	ACS 51	Yes	Yes	Yes	2,000	Yes
Vikonics	Visids 4000	Yes	Yes	Yes	999	Yes
Vindicator	S.M.A.R.T.	No	Yes	Yes	64	No
	ECS-5000	Yes	Yes	Yes	256+	Yes
Westinghouse	SE6000	Yes	Yes	Yes	1	Yes

Requirements/Questions:

3.5.2.1 CCTVs used for assessment must be able to be automatically switched (and aimed if PTZ) to display a preprogrammed camera image on the desired monitor.

3.5.2.1d How many PTZ systems can your system identify and control?
3.5.2.1e How is the interface to the video switcher made?
3.5.2.1f Does your system support a video tape recorder?
3.5.2.1g Does your system support a video frame grabber?
3.5.2.1h Does your system support a video printer?

Firm Short Name	System Name	3.5.2.1d	3.5.2.1e	3.5.2.1f	3.5.2.1g	3.5.2.1h
Advantor	AIMS	Unknown	Serial, Relay	Unknown	Unknown	Unknown
DSX	DSX-1030 Series	Unknown	Serial, Relay	Yes	Yes	Yes
Infographic	Infogard One-32 Plus	Unknown	Serial, Relay	Unknown	Unknown	Unknown
LLNL	Argus	64	Serial	Yes	Yes	No
Logiplex	Logiplex System	Unknown	Serial, Relay	Yes	Yes	Yes
Matrix	R9.X System	Unknown	Serial	Unknown	No	Unknown
Mosler	SmartLINX	9,999	Serial, Relay	Yes	Yes	Yes
SMF	ACS 51	1,000	Serial	Yes	Yes	Yes
Vikonics	Visids 4000	999	Serial	Yes	Yes	No
Vindicator	S.M.A.R.T.	Unknown	Serial	Yes	Yes	Yes
	ECS-5000	256+	Serial	Yes	Yes	Yes
Westinghouse	SE6000	Unknown	Serial, Relay	Yes	Yes	Yes

Requirements/Questions:

3.5.2.1 CCTVs used for assessment must be able to be automatically switched (and aimed if PTZ) to display a preprogrammed camera image on the desired monitor.

3.5.2.1l Can camera inputs be selected for sequenced display to a video monitor?
3.5.2.1j Can video images be annotated with alphanumeric data?
3.5.2.1k Can video images be displayed directly on the annunciator screen?

Firm Short Name	System Name	3.5.2.1i	3.5.2.1j	3.5.2.1k
Advantor	AIMS	Unknown	Unknown	No
DSX	DSX-1030 Series	Yes	Yes	No
Infographic	Infogard One-32 Plus	Unknown	Unknown	No
LLNL	Argus	Yes	Yes	No
Logiplex	Logiplex System	Unknown	Yes	No
Matrix	R9.X System	Unknown	Unknown	No
Mosler	SmartLINX	Yes	Yes	No
SMF	ACS 51	Yes	Yes	Yes
Vikonics	Visids 4000	Yes	Yes	No
Vindicator	S.M.A.R.T.	Yes	Yes	No
	ECS-5000	Yes	Yes	No
Westinghouse	SE6000	Yes	Yes	Yes

3.6 ACCESS CONTROL SYSTEM FUNCTIONAL SPECIFICATIONS FOR ANNUNCIATORS - ACCESS CREDENTIAL

Requirements/Questions:

3.6.1 The badge must, at a minimum, interface with magnetic card readers.

3.6.1a Does your system support a magnetically or optically coded card reader?
3.6.1b Does your system support a smart card reader?
3.6.1c Does your system support a proximity card reader?
3.6.1d Does your system support a numeric keypad?

3.6.2 The badge must be entered into or passed through a device that reads the embedded codes and passes that information to a database for comparison with existing data.

3.6.2 Does your system support a badge which must be entered into or passed through a device that reads the embedded codes and passes that information to a database for comparison with existing data?

3.6.3 The badge shall be capable of being attached to an individual and displayed openly above the waist and below the shoulder.

3.6.3 Does your system support a bade that is capable of being attached to an individual and displayed openly above the waist and below the shoulder?

Firm Short Name	System Name	3.6.1a	3.6.1b	3.6.1.c	3.1.6.d	3.6.2	3.6.3
Advantor	AIMS	Yes	No	No	Yes	Yes	Yes
DSX	DSX-1030 Series	Yes	Yes	Yes	Yes	Yes	Yes
Infographic	Infogard One-32 Plus	Yes	No	Yes	Yes	Yes	Yes
LLNL	Argus	Yes	No	No	Yes	Yes	Yes
Logiplex	Logiplex System	Yes	Yes	Yes	Yes	Yes	Yes
Matrix	R9.X System	Yes	No	Yes	Yes	Yes	Yes
Mosler	SmartLINX	Yes	Yes	Yes	Yes	Yes	Yes
SMF	ACS 51	Yes	Yes	Yes	Yes	Yes	Yes
Vikonics	Visids 4000	Yes	No	Yes	Yes	Yes	Yes
Vindicator	S.M.A.R.T.	Yes	Yes	Yes	Yes	Yes	Yes
	ECS-5000	Yes	Yes	Yes	Yes	Yes	Yes
Westinghouse	SE6000	Yes	Yes	Yes	Yes	Yes	Yes

3.7 ACCESS CONTROL SYSTEM FUNCTIONAL SPECIFICATIONS FOR ANNUNCIATORS - ACCESS PORTAL

Requirements/Questions:

3.7.1 Access portals shall provide for access control.

3.7.1 Does your system support portals which provide for access control?

3.7.2 Access portals shall provide for alarm generation and assessment.

3.7.2 Does your system support portal devices capable of alarm generation and assessment?

3.7.3 Access portals shall provide for assist access.

3.7.3 Does your system support portal devices which assist access (ADA)?

3.7.4 Access portals shall provide for emergency ingress/egress.

3.7.4 In the event of emergency ingress/egress, will the operator be automatically notified of this activity?

Firm Short Name	System Name	3.7.1	3.7.2	3.7.3	3.7.4
Advantor	AIMS	Yes	Yes	Yes	Yes
DSX	DSX-1030 Series	Yes	Yes	Yes	Yes
Infographic	Infogard One-32 Plus	Yes	Yes	Yes	Yes
LLNL	Argus	Yes	Yes	Yes	Yes
Logiplex	Logiplex System	Yes	Yes	Yes	Yes
Matrix	R9.X System	Yes	Yes	Yes	Yes
Mosler	SmartLINX	Yes	Yes	Yes	Yes
SMF	ACS 51	Yes	Yes	Yes	Yes
Vikonics	Visids 4000	Yes	Yes	Yes	Yes
Vindicator	S.M.A.R.T.	Yes	Yes	Yes	Yes
	ECS-5000	Yes	Yes	Yes	Yes
Westinghouse	SE6000	Yes	Yes	Yes	Yes

Requirements/Questions:

3.7.5 Access portals shall provide for degraded mode operation.

3.7.5 Does your system support portal devices which are capable of degraded mode operation?

3.7.6 Access portals shall provide for positive single access.

3.7.6 Does your system support portals which are capable of positive single access?

3.7.7 Access portals shall provide for two-person rule.

3.7.7 Does your system support a two-person access rule?

Firm Short Name	System Name	3.7.5	3.7.6	3.7.7
Advantor	AIMS	No	Yes	Yes
DSX	DSX-1030 Series	Yes	Yes	Yes
Infographic	Infogard One-32 Plus	Yes	Yes	Yes
LLNL	Argus	Yes	Yes	Yes
Logiplex	Logiplex System	Yes	Yes	Yes
Matrix	R9.X System	Yes	Yes	Yes
Mosler	SmartLINX	Yes	Yes	Yes
SMF	ACS 51	Yes	Yes	Yes
Vikonics	Visids 4000	Yes	Yes	Yes
Vindicator	S.M.A.R.T.	Yes	Yes	Yes
	ECS-5000	Yes	No	Yes
Westinghouse	SE6000	Yes	Yes	Yes

3.8 ACCESS CONTROL SYSTEM FUNCTIONAL SPECIFICATIONS FOR ANNUNCIATORS - CONTROL SOFTWARE

Requirements/Questions:

3.8.1 The access control software must receive information from the installed access control devices, compare this information to data stored in a data base, and generate the appropriate signal to the portal locking device.

3.8.1 Does your system receive information from the installed access control devices, compare this information to data stored in a database, and generate the appropriate signal to the portal locking device?

3.8.2 Unsuccessful access attempts must be logged in a transaction file.

3.8.2 Are unsuccessful access attempts logged in a transaction file?

3.8.3 Unsuccessful access attempts must be signaled to the appropriate portal access device

.

3.8.3 Are unsuccessful access attempts signaled to the appropriate portal access device?

Firm Short Name	System Name	3.8.1	3.8.2	3.8.3
Advantor	AIMS	Yes	Yes	Yes
DSX	DSX-1030 Series	Yes	Yes	Yes
Infographic	Infogard One-32 Plus	Yes	Yes	Yes
LLNL	Argus	Yes	Yes	Yes
Logiplex	Logiplex System	Yes	Yes	Yes
Matrix	R9.X System	Yes	Yes	Yes
Mosler	SmartLINX	Yes	Yes	Yes
SMF	ACS 51	Yes	Yes	Yes
Vikonics	Visids 4000	Yes	Yes	Yes
Vindicator	S.M.A.R.T.	Yes	Yes	Yes
	ECS-5000	Yes	Yes	Yes
Westinghouse	SE6000	Yes	Yes	Yes

Requirements/Questions:

3.8.4 The access control software must be capable of handling logical portal access requirements including individual access requirements for each portal.

3.8.4 Does the system software support individual portal access requirements?

3.8.4.1 The access control software must be capable of handling logical portal access requirements including two-person rule.

3.8.4.1 Does the system software support a two-person access rule?

3.8.4.2 The access control software must be capable of handling logical portal access requirements including escorted visitors.

3.8.4.2 Does the system software support some visitor/escort logic?

Firm Short Name	System Name	3.8.4	3.8.4.1	3.8.4.2
Advantor	AIMS	Yes	Yes	No
DSX	DSX-1030 Series	Yes	N/A	Yes
Infographic	Infogard One-32 Plus	Yes	Yes	No
LLNL	Argus	Yes	Yes	Yes
Logiplex	Logiplex System	Yes	Yes	Yes
Matrix	R9.X System	Yes	Yes	Yes
Mosler	SmartLINX	Yes	Yes	Yes
SMF	ACS 51	Yes	Yes	Yes
Vikonics	Visids 4000	Yes	Yes	Yes
Vindicator	S.M.A.R.T.	Yes	Yes	Yes
	ECS-5000	Yes	Yes	Yes
Westinghouse	SE6000	Yes	Yes	Yes

Requirements/Questions:

3.8.4.3 The access control software must be capable of handling logical portal access requirements including anti-passback.

3.8.4.3a Does the system software support anti-passback logic?

3.8.4.3b Is the anti-passback check made at the host machine or at the local controller?

3.8.4.4 The access control software must be capable of handling logical portal access requirements including invalid access attempts.

3.8.4.4 What number of consecutive unsuccessful access attempts is the requester allowed by your system?

3.8.4.5 The access control software must be capable of handling logical portal access requirements including open portal time-out.

3.8.4.5 Will the entry control subsystem support a door unlocked alarm under circumstances when the door does not close and/or lock within some specified period of time?

Firm Short Name	System Name	3.8.4.3a	3.8.4.3b	3.8.4.4	3.8.4.5
Advantor	AIMS	Yes	Host, Local Controller	Variable between 2 and 4	Yes-Variable
DSX	DSX-1030 Series	Yes	Local Controller	Variable between 0 and 5	Yes-Variable
Infographic	Infogard One-32 Plus	Yes	Host, Local Controller	Fixed at 1	Yes-Variable
LLNL	Argus	Yes	Local Controller	Configurable	Yes-Variable
Logiplex	Logiplex System	Yes	Local Controller, Global	Variable between 1 and 15	Yes-Variable
Matrix	R9.X System	Yes	Host, Global, Local Controller	Unlimited	Yes-Variable
Mosler	SmartLINX	Yes	Host, Local Controller	Fixed at 1	Yes-Variable
SMF	ACS 51	Yes	Host, Local Controller	Unknown	Yes-Variable
Vikonics	Visids 4000	Yes	Local Controller, Global	Fixed at 3	Yes-Variable
Vindicator	S.M.A.R.T.	Yes	Local Controller	Variable between 1 and 255	Yes-Variable
	ECS-5000	Yes	Local Controller	Variable between 1 and 255	Yes-Variable
Westinghouse	SE6000	Yes	Host, Local Controller	Fixed at 3	Yes-Variable

Requirements/Questions:

3.8.5 Authorized individuals must be able to place any portal "in access."

3.8.5a Does your system permit an authorized operator to place any portal "in access?"
3.8.5b Does your system permit an authorized operator to remotely release locks?

3.8.6 When a portal is placed "in access" the system will log the time of the event and the person taking the action.

3.8.6 Does your system permit an authorized operator to place any portal "in access?"

3.8.7 When a portal is placed "in access" the system will provide constant notification that the portal is in access.

3.8.7 When a portal is placed "in access" does the system provide constant notification that the portal is in access?

3.8.8 When an access portal is placed "in access," line supervision and tamper alarms will be reported.

3.8.8 When an access portal is placed "in access", do line supervision and tamper alarms continue to be reported?

Firm Short Name	System Name	3.8.5a	3.8.5b	3.8.6	3.8.7	3.8.8
Advantor	AIMS	Yes	Yes	Yes	Yes	Yes
DSX	DSX-1030 Series	Yes	Yes	Yes	No	No
Infographic	Infogard One-32 Plus	Yes	Yes	Yes	Yes	Yes
LLNL	Argus	Yes	Yes	Yes	Yes	Yes
Logiplex	Logiplex System	Yes	Yes	Yes	Yes	Yes
Matrix	R9.X System	Yes	Yes	Yes	Yes	Yes
Mosler	SmartLINX	Yes	Yes	Yes	Yes	Yes
SMF	ACS 51	Yes	Yes	Yes	Yes	Yes
Vikonics	Visids 4000	Yes	Yes	Yes	No	Yes
Vindicator	S.M.A.R.T.	Yes	Yes	No	Yes	Yes
	ECS-5000	Yes	Yes	Yes	Yes	Yes
Westinghouse	SE6000	Yes	Yes	Yes	Yes	Yes

Requirements/Questions:

3.8.8.1 When an access portal is placed "in access" by an authorized individual, notification of that action must be made to the operators in the primary alarm station.

3.8.8.1 When an access portal is placed "in access" from the central alarm station, can notification of that action be made to the operators in the secondary alarm station?

3.8.8.2 When an access portal is placed "in access" by an authorized individual, notification of that action must be made to the operators in the secondary alarm station.

3.8.8.2 When an access portal is placed "in access" from the secondary alarm station, can notification of that action be made to the operators in the central alarm station?

3.8.9 The access control software must be capable of enrolling and unenrolling entrants from one or more remote locations.

3.8.9 Does the system software permit enrolling and unenrolling entrants from one or more remote locations?

3.8.10 Enrollment of a potential entrant must be performed by authorized personnel.

3.8.10 Must potential entrants be enrolled only by authorized personnel?

3.8.11 Time of allowable access must be capable of being entered in thirty minute or less increments and will include a start and stop time of day.

3.8.11 What is the highest resolution of date/time supported by your security system?

Firm Short Name	System Name	3.8.8.1	3.8.8.2	3.8.9	3.8.10	3.8.11
Advantor	AIMS	Yes	Yes	Yes	Yes	1 Minute
DSX	DSX-1030 Series	Yes	Yes	Yes	Yes	1 Minute
Infographic	Infogard One-32 Plus	Yes	Yes	Yes	Yes	1 Minute
LLNL	Argus	Yes	Yes	No	Yes	1 Minute
Logiplex	Logiplex System	Yes	Yes	Yes	Yes	1 Second
Matrix	R9.X System	Yes	Yes	Yes	Yes	2 Seconds
Mosler	SmartLINX	Yes	Yes	Yes	Yes	1 Minute
SMF	ACS 51	Yes	Yes	Yes	Yes	1 Second
Vikonics	Visids 4000	Yes	No	Yes	Yes	1 Minute
Vindicator	S.M.A.R.T.	Yes	Yes	Yes	Yes	1 Minute
	ECS-5000	No	No	Yes	Yes	1 Second
Westinghouse	SE6000	Yes	Yes	Yes	Yes	1 Minute

Requirements/Questions:

3.8.12 Time of allowable access must be capable of being entered in thirty minute or less increments and will include a start and stop time of day.

3.8.12 Does the entry control subsystem provide for various categories of access, delimited as shown?

3.8.13 Date of access must be capable of being entered as calendar dates, including the year.

3.8.13 Does yours system require the dates of access be entered as calendar dates, including the year?

3.8.14 Authorized portals may be entered as individual portal numbers or logical sets of portals.

3.8.14 Does your system allow portals to be entered as individual portals or logical sets of portals?

3.8.15 The software will automatically update individual portals or devices that control one or more portals with data from the central data base.

3.8.15 Does the system automatically update individual portals or devices that control one or more portals with data from the central database when changes are made to the central database?

Firm Short Name	System Name	3.8.12	3.8.13	3.8.14	3.8.15
Advantor	AIMS	Date/Day, Time, Location	No	Yes	Yes
DSX	DSX-1030 Series	Date/Day, Time, Location	Yes	Yes	Yes
Infographic	Infogard One-32 Plus	Date/Day, Time, Location	Yes	Yes	Yes
LLNL	Argus	Date/Day, Time, Location	Yes	Yes	Yes
Logiplex	Logiplex System	Date/Day, Time, Location, Device Card Sensor	Yes	Yes	Yes
Matrix	R9.X System	Date/Day, Time, Location	Yes	Yes	Yes
Mosler	SmartLINX	Date/Day, Time, Location, Person	Yes	Yes	Yes
SMF	ACS 51	Date/Day, Time, Location	Yes	Yes	Yes
Vikonics	Visids 4000	Date/Day, Time, Location	Yes	Yes	Yes
Vindicator	S.M.A.R.T.	Date/Day, Time, Location, Credential, Rule	Yes	Yes	Yes
	ECS-5000	Date/Day, Time, Location, Groups, Individuals, Access Authorities	Yes	Yes	Yes
Westinghouse	SE6000	Date, Time, Location	Yes	Yes	Yes

Requirements/Questions:

3.8.16 When communications are lost between the intelligent field device and the "host" machine, the field device will internally log all transactions.

3.8.16a When communications is lost between the intelligent field device and the "host" machine, does the field device internally log all transactions?
3.8.16b What is the total number of transactions which can be stored in a field panel?

3.8.17 When communications are re-established between the intelligent field device and the "host" machine, the field device will up-load to the "host" all logged transactions that occurred while communications were lost.

3.8.17 When communications are re-established between the intelligent field device and the "host" machine, does the field device automatically will up-load to the "host" all logged transactions that occurred while communications were lost?

3.8.18 The access control software will record all successful and unsuccessful access attempts in an audit trail file.

3.8.18 Does your system automatically record all successful and unsuccessful access attempts in an audit trail file?

3.8.19 The minimum data to be recorded includes: name of entrant, personal identification number, event time, event date, portal number, and badge number if used.

3.8.19 Does all recorded access activity include as a minimum the: name of entrant, personal identification number (if used, may also be encrypted), event time, event date, portal number, and badge number if used.

Firm Short Name	System Name	3.8.16a	3.8.16b	3.8.17	3.8.18	3.8.19
Advantor	AIMS	Yes	8,000	Yes	Yes	Yes
DSX	DSX-1030 Series	Yes	10,000	Yes	Yes	Yes
Infographic	Infogard One-32 Plus	Yes	10,000+	Yes	Yes	Yes
LLNL	Argus	Yes	Unknown	Yes	Yes	Yes
Logiplex	Logiplex System	Yes	1,000	Yes	Yes	Yes
Matrix	R9.X System	Yes	1,000	Yes	Yes	Yes
Mosler	SmartLINX	Yes	10,000	Yes	Yes	Yes
SMF	ACS 51	Yes	3,000	Yes	Yes	Yes
Vikonics	Visids 4000	Yes	4,000	Yes	Yes	No
Vindicator	S.M.A.R.T.	Yes	Unknown	Yes	Yes	Yes
	ECS-5000	Yes	10,000+	Yes	Yes	Yes
Westinghouse	SE6000	Yes	4,000	Yes	Yes	Yes

Requirements/Questions:

3.8.20 The access control software will signal an alarm when the preset number of consecutive invalid access attempts has been exceeded from a single portal and for each subsequent consecutive invalid access attempt from that portal.

3.8.20 Will your system generate an alarm when the preset number of consecutive invalid access attempts has been exceeded from a single portal and for each subsequent consecutive invalid access attempt from that portal?

3.8.21 The access control software will signal an alarm when a tamper indication is received from protected portions of the portal.

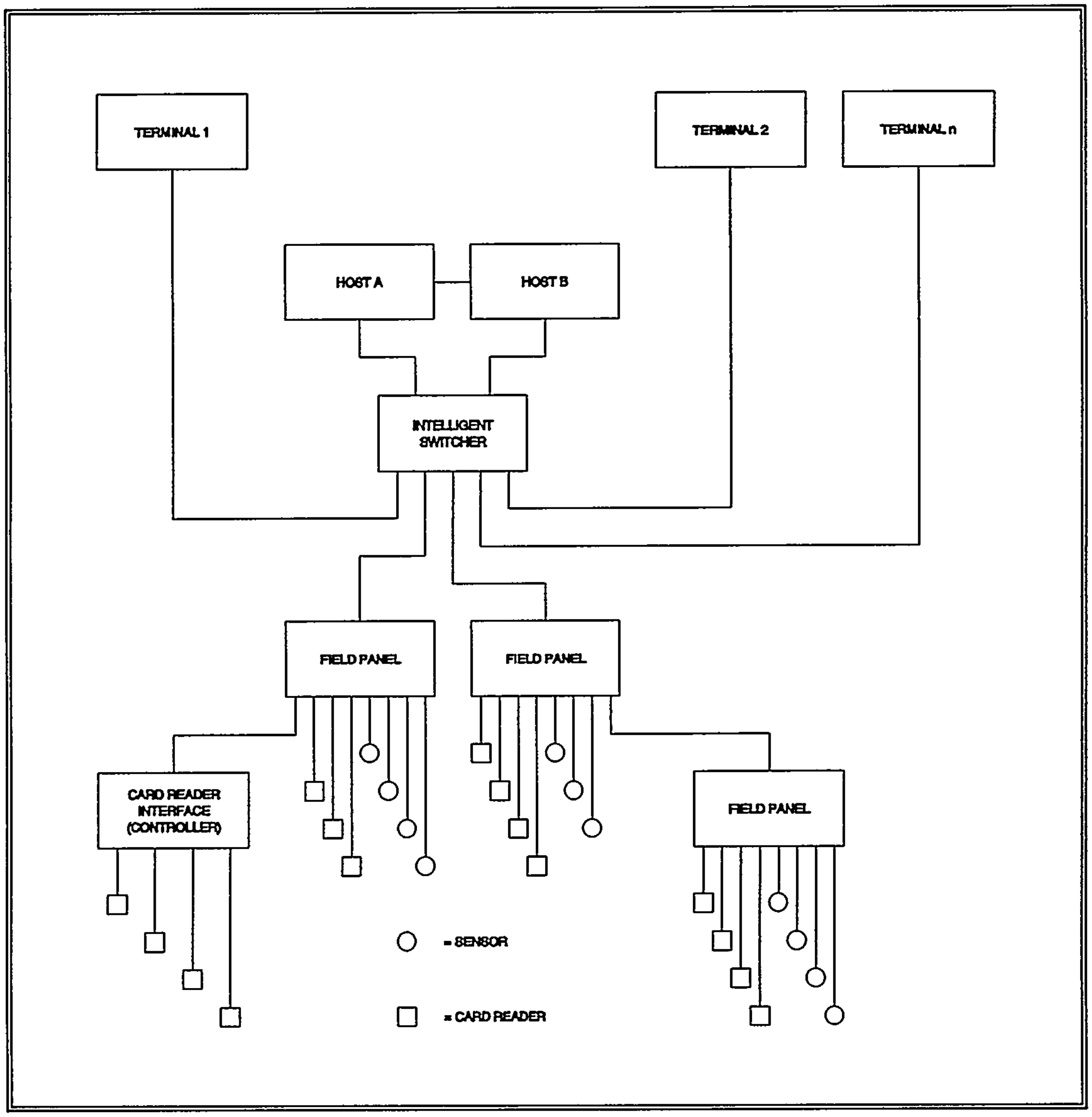
3.8.21 Will your system generate an alarm when a tamper indication is received from protected portions of the portal?

3.8.22 The access control software will signal an alarm when any other monitored and unacceptable condition is detected.

3.8.22 Will your system generate an alarm when any other monitored and unacceptable condition is detected?

Firm Short Name	System Name	3.8.20	3.8.21	3.8.22
Advantor	AIMS	Yes	Yes	Yes
DSX	DSX-1030 Series	Yes	Yes	Yes
Infographic	Infogard One-32 Plus	Yes	Yes	Yes
LLNL	Argus	Yes	Yes	Yes
Logiplex	Logiplex System	Yes	Yes	Yes
Matrix	R9.X System	Yes	Yes	Yes
Mosler	SmartLINX	Yes	Yes	Yes
SMF	ACS 51	Yes	Yes	Yes
Vikonics	Visids 4000	Yes	Yes	Yes
Vindicator	S.M.A.R.T.	Yes	Yes	Yes
	ECS-5000	Yes	Yes	Yes
Westinghouse	SE6000	No	Yes	Yes

4. GENERIC BLOCK DIAGRAM



The block diagram shown above is typical of most Integrated Intrusion Detection and Access Control Annunciator Systems as configured for a small site. Specific features or combinations of features may not be representative of a particular system.

This page intentionally left blank.

5. GLOSSARY

Access. When a device is placed in "Access" its primary function is bypassed. A detection by an intrusion sensor may not be annunciated, or an access portal may not limit access but will allow free passage. Similar to "Mask" and "Shunt."

Alarm. An alarm is any event occurring within the system which requires a response by an operator.

Annunciator. The part or parts of a system with which the operator interacts (as opposed to the parts of the system which reside in the field).

Archive. To back-up and/or off-load data from the system to some media which can be physically removed from the system.

Assessment. Attributing a cause to an alarm event.

Audit Trail. A record of all activity taking place within the system. This includes changes to the system's configuration as well as activity resulting from daily use of the system.

Central Alarm Station. The primary area at which system events are annunciated.

Event. Any activity occurring within the system may be termed an "Event." Identical to a "Transaction."

Field Panel. Any of a number of types of devices which are usually (but not restricted to) not physically near the host. Three examples of these are Card Reader Controllers, Modems, and Multiplexers.

Host. The processor(s) which possesses primary responsibility for operation of the system.

Mask. When a device is placed in "Access" its primary function is bypassed. An intrusion sensor may not signal a detection, or an access portal may not limit access but will allow free passage. Similar to "Access" and "Shunt."

Off-Line Functions. Functions which do not require immediate response by the operator. Two examples of this are report generation and transaction log archiving.

On-Line Functions. Functions which require immediate response by the operator. Two examples of this are alarm annunciation and portal access requests.

Portal. A portal is an opening through which passage is controlled. Portals may be either single or double door (man-trap)types.

Secondary Alarm Station. The alternate area at which system events are annunciated.

Sensor State. Any of a number of logical combinations of status' a sensor can report and user input. As an example, if a sensor detects an intrusion and signals an alarm, that is a "new alarm" state. If the sensor *remains* in alarm and the operator acknowledges it, that is an "acknowledged alarm" state.

Shunt. When a device is placed in "Access" its primary function is bypassed. An intrusion sensor may not signal a detection, or an access portal may not limit access but will allow free passage. Similar to "Access" and "Mask."

Tamper. A Tamper alarm is an alarm which signals an intrusion *not* into a monitored area, but an intrusion into the system itself. This includes system hardware components such as sensors, card readers, and field panels as well as system software such as unauthorized attempts to view and/or modify system data bases and/or functions.

Transaction. Any activity occurring within the system may be termed a "Transaction." Identical to an "Event."

External Distribution:

1 General George L. McFadden, Director
Office of Security Affairs, NN-50
U.S. Department of Energy
Washington, DC 20585

1 Edward J. McCallum, Director
Office of Safeguards and Security, NN-51
U.S. Department of Energy
Washington, DC 20585

1 David A. Jones, Director
Policy, Standards, and Analysis Division,
NN-512
U.S. Department of Energy
Washington, DC 20585

2 William J. Desmond, Program Manager
Darryl Toms
Physical Security Branch, NN-512.1
U.S. Department of Energy
Washington, DC 20585

1 Lynne Gebrowsky, Program Manager
Personnel Security Policy, Procedures,
Analysis Branch, NN-512.2
U.S. Department of Energy
Washington, DC 20585

1 Larry D. Wilcher, Program Manager
Technical and Operations Security
Branch, NN-512.3
U.S. Department of Energy
Washington, DC 20585

1 David W. Crawford, Program Manager
Materials Control and Accounting
Branch, NN-512.4
U.S. Department of Energy
Washington, DC 20585

1 G. Bowser, Program Manager
Assessment and Integration Branch,
NN-513.1
U.S. Department of Energy
Washington, DC 20585

1 Donald J. Solich, Program Manager
Weapons Safeguards and Security
Operations Branch, NN-513.2
U.S. Department of Energy
Washington, DC 20585

1 G. Griffin, Program Manager, Actg
Production/Energy Safeguards/Security
Operations Branch, NN-513.3
U.S. Department of Energy
Washington, DC 20585

2 G. Dan Smith, Program Manager
Carl A. Pocratsky
Planning and Technology Development
Branch, NN-513.4
U.S. Department of Energy
Washington, DC 20585

1 Marshall O. Combs, Director
Headquarters Operations Division, NN-514
U.S. Department of Energy
Washington, DC 20585

1 Charles C. Coker, Program Manager
Physical Protection Branch, NN-514.1
U.S. Department of Energy
Washington, DC 20585

1 Floyd McCloud, Program Manager
Technical/Information Security Branch,
NN-514.2
U.S. Department of Energy
Washington, DC 20585

1 Kenneth Sanders, Director
International Safeguards Division, NN-44
U.S. Department of Energy
Washington, DC 20585

1 Bryan Siebert, Jr., Director
Office of Declassification, NN-52
U.S. Department of Energy
Washington, DC 20585

1 William Hensley, Director
Office of Engineering, Operations, Security,
and Transition Support, DP-31
U.S. Department of Energy
Washington, DC 20585

1 R. Crow, Director
Office of RD&T Facilities, DP-65
U.S. Department of Energy
Washington, DC 20585

1 Glen S. Podonsky, Deputy Assistant
Secretary
Office of Oversight, EH-2
U.S. Department of Energy
Washington, DC 20585

1 Vincent J. Moskaitis
Office of Plans, Technology, and
Certification, EH-4.3
U.S. Department of Energy
Washington, DC 20585

1 HEADQUARTERS, USAFE
Attn: Director, Plans and Programs
Unit 3050, Box 135
APO-AE 09094-5000

1 U.S. Army Military Police School
ATZN-MP-TS (Capt. Sanders)
Fort McClellan, AL 36205-5030

1 Commander
U.S. Army Engineering Division
Attn: HNDED-ME, Electronic Technology
PO Box 1600
Huntsville, AL 35806

1 Naval Civil Engineering Laboratory
Attn: G. Cook, L-56
Port Hueneme, CA 93043

1 Donald Wentz, Director
Safeguards and Security
Lawrence Livermore National Laboratory
PO Box 808
Livermore, CA 94550

1 K. J. Heidemann, Director
U.S. Department of Energy/RF
Safeguards and Security Division
PO Box 928
Golden, CO 80402-0928

1 G. P. Morgan, Director
U.S. Department of Energy
Western Area Power Administration
Division of Energy Services and Security
Affairs, A0410
1667 Cole Boulevard, Bldg 18
Golden, CO 80401-0456

1 James Hartman, Assistant Manager
Site Support and Security
U.S. Department of Energy/RF
PO Box 958, Bldg 115
Golden, CO 80402-0464

1 Chief of Security Police
Air Force Space Command
Peterson Air Force Base
Colorado 80914-5001

1 James W. Atherton, SA
Federal Bureau of Investigation
Washington Field Office
10th Street and Pennsylvania Avenue NW
Washington, DC 20537

1 Raymond Brady, Director
U.S. Nuclear Regulatory Commission
Division of Security
Washington, DC 20555

1 Fred Branch, Chief
Physical Security Branch
U.S. Department of State
DS/PSD Room 804, SA6
Washington, DC 20520

1 Robert Burnett, Director
U.S. Nuclear Regulatory Commission
Division of Fuel Cycle, Safety, and
Safeguards, NMSS
Mail Stop 8-A-33 TWFN
Washington, DC 20555

1 Director, Systems Protection
OASD (C3I), DASD (I&S), CI&SP, 3C260
6000 Defense Pentagon
Washington, DC 20301-6000

1 Central Intelligence Agency
Director, Office of Security
202 Jefferson
Washington, DC 20505

1 Priscilla A. Dwyer
U.S. Nuclear Regulatory Commission
Division of Fuel Cycle, Safety, and
Safeguards, NMSS
Washington, DC 20555

1 Tom Fey
U.S. Department of State
DS/PI/PRD, State Annex 1
2201 C Street NW
Washington, DC 20520

1 John C. Hagan
National Aeronautics and Space
Administration
Security Office (NIS)
Washington, DC 20546

1 U.S. Department of Justice
Federal Bureau of Prisons
Attn: Jim Mahan, Room 300
320 First Street NW
Washington, DC 20534

1 J. Partlow, Director
U.S. Nuclear Regulatory Commission
Division of Inspection Programs
Washington, DC 20555

1 HEADQUARTERS, USAF/SPX
Attn: LtCol Mike Pasquin
1340 Air Force
The Pentagon
Washington, DC 20330-1340

1 HEADQUARTERS, USAF/SPO
Attn: Maj John M. Reis
1340 Air Force
The Pentagon
Washington, DC 20330-1340

1 C. C. Slagle, Manager
Technical Division
U.S. Bureau of Engraving & Printing
Room 303M
14th and C Street NW
Washington, DC 20228

1 Richard J. Solan, Chief
U.S. Secret Service
Security Division/Planning and Development
1800 G Street NW, Room 941
Washington, DC 20223

1 Department of the Navy (CNO N-O9N)
Attn: Leo L. Targosz, Jr.
Washington, DC 20388-5024

1 Michael Toscano, Chairman
DoD Physical Security Equipment
Advisory Group
OUSD (A&T)
The Pentagon, Room 3B1060
Washington, DC 20301

1 Stanley W. Zack, Jr.
Federal Bureau of Investigation
Washington Field Office
10th Street and Pennsylvania Avenue NW
Washington, DC 20537

1 HEADQUARTERS, PACAF/SPPA
Attn: Director, Plans and Programs
Hickam Air Force Base
Hawaii 96853

1 Richard L. Green, Director
U.S. Department of Energy/ID
Safeguards and Security Division
785 DOE Place
Idaho Falls, ID 83402

1 Lockheed Idaho Technologies Company
Attn: John J. Noon, Director
Safeguards and Security
PO Box 1624
Idaho Falls, ID 83415

1 Bruce Meppen, Manager
Safeguards and Security
U.S. Department of Energy
Argonne National Laboratory, Idaho Site
PO Box 2528
Idaho Falls, ID 83403-2528

1 Charleton Bingham, Director
U.S. Department of Energy/CH
New Brunswick Laboratory
Safeguards and Security Division
Argonne, IL 60439

1 Thomas Gradle, Director
U.S. Department of Energy/CH
Safeguards and Security Division
Argonne, IL 60439

2 Argonne National Laboratory
Attn: K. W. Poupa
Attn: D. G. Erick
970 South Cass Avenue
Argonne, IL 60439

1 Rudy Dorner
Fermi National Accelerator Laboratory
MS 102
Batavia, IL 60150

1 J. Dollinger, Security Department
Boeing Petroleum Services
850 South Clearview
New Orleans, LA 70123

1 Donald J. Ornick, Director
Security Division
U.S. Department of Energy/OR
900 Commerce Road East
New Orleans, LA 70123

1 Wackenhut Services, Inc.
800 West Commerce Road, Suite 100
New Orleans, LA 70123

1 A. L. Lavery
Transportation Systems Center
Kendall Square
Cambridge, MA 02142

4 HEADQUARTERS, ESC
Attn: Doug Dalessio, AVJ
Attn: Don Carr, AVJF
Attn: Morry Outwater, AVJR
Attn: Capt. Jamie Thurber, AVJG TASS
20 Schilling Circle
Hanscom Air Force Base
Massachusetts 01731-2816

1 Michael Kraynick
National Security Agency
Mail Stop 51
Fort Meade, MD 20755

2 AlliedSignal, Inc.
Attn: S. J. Baker, Manager
Attn: S. V. Zvacek, Supervisor
Security and Emergency Management
Kansas City, MO 64141-6159

1 Commanding General
USAJFKSWCS
SOTIC
Fort Bragg, NC 28307-5000

1 Commanding General
1st SOCOM
ODCOPS-Special Projects
Fort Bragg, NC 28307

1 Col. William F. Garrison
Department of the Army
1st Special Forces Operational, Det-Delta
Fort Bragg, NC 28307-5000

1 John Trout
U.S. Army Corps of Engineers, MROED-S
215 North 17th Street
Omaha, NE 68102

1 U.S. Department of Energy/Safeguards
and Security
Central Training Academy
Attn: Stan Laktasic
PO Box 18041
Albuquerque, NM 87185

1 U.S. Department of Energy, SNSD/AL
Attn: Ms. Linda L. Mueller, Acting Director
Security and Nuclear Safeguards Directorate
PO Box 5400
Albuquerque, NM 87185

1 HEADQUARTERS, AFSPA/SPS
Attn: Col David M. Taylor, USAF
Director, Physical Security
8201 H Avenue SE
Kirtland Air Force Base
New Mexico 87117-5664

1 Director of Operations (SPO)
Air Force Agency Security Police
Kirtland Air Force Base
New Mexico 87117-5000

1 D. B. Smith, N-DO/SG
Los Alamos National Laboratory
Mail Stop: E550
PO Box 1663
Los Alamos, NM 87545

1 E. Wayne Adams, Director
Safeguards and Security Division
U.S. Department of Energy/NV
PO Box 98518
Las Vegas, NV 89193-8518

1 Raytheon Services, Inc.
Attn: Electronics Department
PO Box 93838
Las Vegas, NV 89193-3838

1 George G. Stefani, Jr., Director
Safeguards and Security Division
U.S. Department of Energy
Schenectady Naval Reactors Office
PO Box 1069
Schenectady, NY 12301

2 U.S. Department of Energy
Brookhaven Area Office
Attn: Joseph Indusi, Bldg 197C
Attn: Kris Dahms, Bldg 703
53 Bell Avenue
Upton, NY 11973

1 485th EIG/EICI
Griffiss Air Force Base
New York 13441-6348

1 Daniel Baker, Security Manager
EG&G Mound
PO Box 3000
Building 99
Miamisburg, OH 45342

1 J. M. Miller, Manager
Westinghouse Materials Company of Ohio
Safeguards and Security
PO Box 898704
Cincinnati, OH 45239

1 Robert L. Windus, Security Manager
U.S. Department of Energy/BP
PO Box 3621
Portland, OR 97208

1 J. A. Bullian, Director
U.S. Department of Energy/PNR
Safeguards and Security Division
PO Box 109
West Mifflin, PA 15122

1 A. H. Hopfinger, Manager
Laboratory Operational Safeguards, 62M
Bettis Atomic Power Laboratory
Westinghouse Electric Corporation
Box 79
West Mifflin, PA 15122-0079

2 Westinghouse Savannah River Company
Attn: J. W. Dorrycott, Division Manager
Safeguards, Security, & Emergency Preparedness
Attn: R. E. Gmitter, Manager
Safeguards and Security Programs
PO Box 616
Aiken, SC 29802

4 U.S. Department of Energy/SR
Office of Safeguards and Security
Attn: Larry Brown, Director
Attn: Larry Ogletree, Director
Safeguards Engineering and Projects Branch
Attn: Tom Williams, Branch Chief
Safeguards and Classification
Attn: Steve Shelt
Information and Protection Branch
PO Box A
Aiken, SC 29802

3 Martin Marietta Energy Systems
Y-12 Safeguards and Security
Attn: W. L. Clements, Division Manager
Attn: M. Fuller
Attn: Cathy Key
Bldg 9706-1, MS 8212
Oak Ridge, TN 37831-8213

1 William G. Phelps, Director
U.S. Department of Energy/OR
Safeguards and Security Division
PO Box 2001
Oak Ridge, TN 37831-8570

1 James J. Hallihan, Director
Mason and Hanger-Silas Mason Company, Inc.
Pantex Plant
Safeguards and Security
PO Box 30020
Amarillo, TX 79177-001

1 Chief of Security Police
Air Force Intelligence Command
Kelly Air Force Base
Texas 78243-5000

1 Belvoir Research, Development, and Engineering Center
Product Manager
Physical Security Equipment
Attn: AMCPM-PSE
Fort Belvoir, VA 22060-5606

1 Commander
U.S. Army Troop Support Command
Attn: STRBE-1-POLIC (M. Jennings)
Fort Belvoir, VA 22060

1 Jerry Edwards
U.S. Army PSEMO
Attn: AMSAT-W-TP
BRDEC
Fort Belvoir, VA 22060-5606

1 William J. Witter
Defense Nuclear Agency (NOSA)
6801 Telegraph Road
Alexandria, VA 22310-3398

1 W. R. Brooksher, Manager
Westinghouse Hanford Company
Safeguards and Security Division
PO Box 1970, Mail Stop L4-01
Richland, WA 99352

1 J. L. Spracklen, Director
U.S. Department of Energy/RL
Safeguards and Security Division
PO Box 550, Mail Stop A6-35
Richland, WA 99352

1 Oak Ridge National Laboratory
Attn: M. H. Ehinger
P. O. Box 2008
Oak Ridge, TN 37831

Internal Distribution:

1	MS 0173	F. Gallegos (7400)
1	MS 0175	B. D. Green (13214)
1	MS 0181	R. K. McIntire (7401)
1	MS 0322	P. J. Eicker (2100)
1	MS 0329	J. G. Harlan (2512)
1	MS 0427	W. R. Reynolds (5103)
1	MS 0458	L. R. Gilliom (5603)
1	MS 0469	J. M. Taylor (5006)
1	MS 0490	P. E. D'Antonio (12324)
1	MS 0490	S. D. Spray (12331)
1	MS 0537	D. R. Weiss (2314)
1	MS 0560	P. A. Longmire (5407)
1	MS 0567	R. D. Horton (9208)
1	MS 0570	C. W. Childers (5900)
1	MS 0611	R. M. Workhoven (7433)
1	MS 0627	G. C. Novotny (12334)
1	MS 0632	R. G. Easterling (12303)
1	MS 0656	J. C. Matter (9249)
1	MS 0761	R. F. Davis (5800)
1	MS 0761	F. O. Luetters (5822)
1	MS 0762	G. Smith (5807)
3	MS 0762	Safeguards & Security Library
1	MS 0765	D. E. McGovern (5808)
1	MS 0765	J. D. Williams (5821)
1	MS 0766	J. R. Kelsey (9600)
1	MS 0767	E. R. Hoover (9603)
1	MS 0767	S. C. Roehrig (9604)
1	MS 0768	R. W. Moya (5804)
1	MS 0768	J. W. Kane (5806)
1	MS 0769	D. S. Miyoshi (5800)
1	MS 0775	M. L. Christiansen (9615)
1	MS 0775	S. L. K. Rountree (9617)
1	MS 0776	I. G. Waddoups (5845)
1	MS 0780	S. Ortiz (5838)
20	MS 0780	D. S. Fitzgerald (5838)
1	MS 0780	F. M. Monaco (5838)
1	MS 0781	D. J. Gangel (5831)
1	MS 0781	L. W. Kruse (5833)
1	MS 0782	J. F. Chapek (5848)
1	MS 0782	L. H. Arakaki (5848)
1	MS 0783	S. H. Scott (9611)
1	MS 0790	H. J. Abeyta (9612)
1	MS 0877	J. R. Gosler (5903)
1	MS 0985	J. H. Stichman (2600)
1	MS 0987	R. J. Longoria (2611)
1	MS 9004	M. John (8100)
1	MS 9105	L. Hiles (8400)
1	MS 1070	R. Bair (2200)
1	MS 1114	J. Giachino (7402)
1	MS 1115	A. J. Villareal (7432)
1	MS 1125	K. M. Jensen (9616)
1	MS 1131	B. J. Steele (5849)
1	MS 9020	S. C. Gray (8632)
1	MS 9018	Central Technical Files (8523-2)
5	MS 0899	Technical Library (13414)
1	MS 0619	Print Media (12615)
2	MS 0100	Document Processing (7613-2) For DOE/OSTI

Org.	Bldg.	Name	Rec'd by	Org.	Bldg.	Name	Rec'd by

Sandia National Laboratories