
USACE / NAVFAC / AFCEA UFGS-13720A (July 2003)

Preparing Activity: USACE Superseding
UFGS-13720A (May 1998)

UNIFIED FACILITIES GUIDE SPECIFICATIONS

References are in agreement with UMRL dated 25 June 2004

Latest Change indicate by CHG tags

SECTION TABLE OF CONTENTS

DIVISION 13 - SPECIAL CONSTRUCTION

SECTION 13720A

ELECTRONIC SECURITY SYSTEM

07/03

PART 1 GENERAL

- 1.1 REFERENCES
- 1.2 SYSTEM DESCRIPTION
 - 1.2.1 Central Station
 - 1.2.2 Systems Networks
 - 1.2.2.1 Console Network
 - 1.2.2.2 Field Device Network
 - 1.2.3 Field Equipment
 - 1.2.4 CCTV System Interface
 - 1.2.5 Overall System Reliability Requirements
 - 1.2.6 Error Detection and Retransmission
 - 1.2.7 System Definitions
 - 1.2.7.1 Intrusion Alarm
 - 1.2.7.2 Nuisance Alarm
 - 1.2.7.3 Environmental Alarm
 - 1.2.7.4 False Alarm
 - 1.2.7.5 Duress Alarm
 - 1.2.7.6 Guard Tour Alarm
 - 1.2.7.7 Fail-Safe Alarm
 - 1.2.7.8 Power Loss Alarm
 - 1.2.7.9 Entry Control Alarm
 - 1.2.7.10 Identifier
 - 1.2.7.11 Entry Control Devices
 - 1.2.7.12 Facility Interface Device
 - 1.2.8 Probability of Detection
 - 1.2.9 Standard Intruder
 - 1.2.9.1 Standard Intruder Movement
 - 1.2.10 False Alarm Rate
 - 1.2.10.1 Interior
 - 1.2.10.2 Exterior
 - 1.2.11 Error and Throughput Rates
 - 1.2.11.1 Type I Error Rate
 - 1.2.11.2 Type II Error Rate

- 1.2.12 System Throughput
- 1.2.13 Passage
- 1.2.14 Detection Resolution
- 1.2.15 Electrical Requirements
- 1.2.16 Power Line Surge Protection
- 1.2.17 Sensor and Device Wiring and Communication Circuit Surge Protection
- 1.2.18 Power Line Conditioners
- 1.2.19 System Reaction
 - 1.2.19.1 System Response
 - 1.2.19.2 System Heavy Load Definition
- 1.2.20 Environmental Conditions
 - 1.2.20.1 Interior, Controlled Environment
 - 1.2.20.2 Interior, Uncontrolled Environment
 - 1.2.20.3 Exterior Environment
 - 1.2.20.4 Hazardous Environment
 - 1.2.20.5 Console
- 1.2.21 System Capacity
- 1.3 DELIVERY OF TECHNICAL DATA AND COMPUTER SOFTWARE
 - 1.3.1 Group I Technical Data Package
 - 1.3.1.1 System Drawings
 - 1.3.1.2 Manufacturer's Data
 - 1.3.1.3 System Description and Analyses
 - 1.3.1.4 Software Data
 - 1.3.1.5 Overall System Reliability Calculations
 - 1.3.1.6 Certifications
 - 1.3.1.7 Key Control Plan
 - 1.3.2 Group II Technical Data Package
 - 1.3.3 Group III Technical Data Package
 - 1.3.4 Group IV Technical Data Package
 - 1.3.4.1 Operation and Maintenance Manuals
 - 1.3.4.2 Training Documentation
 - 1.3.4.3 Data Entry
 - 1.3.4.4 Graphics
 - 1.3.5 Group V Technical Data Package
 - 1.3.5.1 Functional Design Manual
 - 1.3.5.2 Hardware Manual
 - 1.3.5.3 Software Manual
 - 1.3.5.4 Operator's Manual
 - 1.3.5.5 Maintenance Manual
 - 1.3.5.6 Final System Drawings
- 1.4 TESTING
 - 1.4.1 General
 - 1.4.2 Test Procedures and Reports
- 1.5 TRAINING
 - 1.5.1 General
 - 1.5.2 Operator's Training I
 - 1.5.3 Operator's Training II
 - 1.5.4 Operator's Training III
 - 1.5.5 System Manager Training
 - 1.5.6 Maintenance Personnel Training
- 1.6 LINE SUPERVISION
 - 1.6.1 Signal and Data Transmission System (DTS) Line Supervision
 - 1.6.2 Data Encryption
- 1.7 DATA TRANSMISSION SYSTEM
- 1.8 MAINTENANCE AND SERVICE
 - 1.8.1 Warranty Period
 - 1.8.2 Description of Work
 - 1.8.3 Personnel

- 1.8.4 Schedule of Work
 - 1.8.4.1 Minor Inspections
 - 1.8.4.2 Major Inspections
 - 1.8.4.3 Scheduled Work
- 1.8.5 Emergency Service
- 1.8.6 Operation
- 1.8.7 Records and Logs
- 1.8.8 Work Requests
- 1.8.9 System Modifications
- 1.8.10 Software

PART 2 PRODUCTS

- 2.1 MATERIALS REQUIREMENTS
 - 2.1.1 Materials and Equipment
 - 2.1.2 Field Enclosures
 - 2.1.2.1 Interior Sensor
 - 2.1.2.2 Exterior Sensor
 - 2.1.2.3 Interior Electronics
 - 2.1.2.4 Exterior Electronics
 - 2.1.2.5 Corrosion Resistant
 - 2.1.2.6 Hazardous Environment Equipment
 - 2.1.3 Nameplates
 - 2.1.4 Fungus Treatment
 - 2.1.5 Tamper Provisions
 - 2.1.5.1 Tamper Switches
 - 2.1.5.2 Enclosure Covers
 - 2.1.6 Locks and Key-Lock Switches
 - 2.1.6.1 Locks
 - 2.1.6.2 Key-Lock-Operated Switches
 - 2.1.6.3 Construction Locks
 - 2.1.7 System Components
 - 2.1.7.1 Modularity
 - 2.1.7.2 Maintainability
 - 2.1.7.3 Interchangeability
 - 2.1.7.4 Product Safety
 - 2.1.8 Controls and Designations
 - 2.1.9 Special Test Equipment
 - 2.1.10 Alarm Output
- 2.2 CENTRAL STATION HARDWARE
 - 2.2.1 Memory
 - 2.2.2 Power Supply
 - 2.2.3 Real Time Clock (RTC)
 - 2.2.4 Serial Ports
 - 2.2.5 Parallel Port
 - 2.2.6 Color Monitor
 - 2.2.7 Keyboard A101
 - 2.2.8 Enhancement Hardware
 - 2.2.9 Disk Storage
 - 2.2.10 Floppy Disk Drives
 - 2.2.11 Magnetic Tape System
 - 2.2.12 Modem
 - 2.2.13 Audible Alarm
 - 2.2.14 Mouse
 - 2.2.15 CD-ROM Drive
 - 2.2.16 Dot Matrix Alarm Printer
 - 2.2.17 Report Printer
 - 2.2.18 Controllers
 - 2.2.19 Redundant Central Computer

- 2.2.20 Central Station Equipment Enclosures
- 2.2.21 Uninterruptible Power Supply (UPS)
- 2.2.22 Fixed Map Display
- 2.2.23 Enrollment Center Equipment
 - 2.2.23.1 Enrollment Center Accessories
- 2.2.24 Secondary Alarm Annunciation Site
- 2.3 CENTRAL STATION SOFTWARE
 - 2.3.1 System Software
 - 2.3.2 Real Time Clock Synchronization
 - 2.3.3 Database Definition Process
 - 2.3.4 Software Tamper
 - 2.3.5 Peer Computer Control Software
 - 2.3.6 Application Software
 - 2.3.6.1 Operator Commands
 - 2.3.6.2 Command Input
 - 2.3.6.3 Command Input Errors
 - 2.3.6.4 Enhancements
 - 2.3.6.5 System Access Control
 - 2.3.6.6 Alarm Monitoring Software
 - 2.3.6.7 Monitor Display Software
 - 2.3.6.8 Map Displays/Graphics Linked to Alarms
 - 2.3.6.9 User Defined Prompts/Messages Linked to Alarms
 - 2.3.6.10 System Test Software
 - 2.3.6.11 Report Generator
 - 2.3.6.12 Simulation (Training) Software
 - 2.3.6.13 Entry Control Enrollment Software
- 2.4 FIELD PROCESSING HARDWARE
 - 2.4.1 Alarm Annunciation Local Processor
 - 2.4.1.1 Processor Power Supply
 - 2.4.1.2 Auxiliary Equipment Power
 - 2.4.2 Entry Control Local Processor
 - 2.4.2.1 Processor Power Supply
 - 2.4.2.2 Auxiliary Equipment Power
- 2.5 FIELD PROCESSING SOFTWARE
 - 2.5.1 Operating System
 - 2.5.1.1 Startup
 - 2.5.1.2 Operating Mode
 - 2.5.1.3 Failure Mode
 - 2.5.2 Functions
- 2.6 INTERIOR SENSORS AND CONTROL DEVICES
 - 2.6.1 Balanced Magnetic Switch (BMS)
 - 2.6.1.1 BMS Subassemblies
 - 2.6.1.2 Housing
 - 2.6.1.3 Remote Test
 - 2.6.2 Glass Break Sensor, Piezoelectric
 - 2.6.2.1 Sensor Element, Piezoelectric
 - 2.6.2.2 Sensor Signal Processor, Piezoelectric
 - 2.6.2.3 Glass Break Simulator, Piezoelectric
 - 2.6.3 Glass Break Sensor, Acoustic
 - 2.6.3.1 Sensor Element, Acoustic
 - 2.6.3.2 Sensor Signal Processor, Acoustic
 - 2.6.3.3 Glass Break Simulator, Acoustic
 - 2.6.4 Duress Alarm Switches
 - 2.6.4.1 Footrail
 - 2.6.4.2 Push-button
 - 2.6.4.3 Wireless
 - 2.6.5 Security Screen
 - 2.6.6 Vibration Sensor
 - 2.6.7 Ultrasonic Motion Sensor

- 2.6.7.1 Test Indicator, Ultrasonic System
 - 2.6.7.2 Remote Test, Ultrasonic System
- 2.6.8 Microwave Motion Sensor
 - 2.6.8.1 Test Indicator, Microwave System
 - 2.6.8.2 Remote Test, Microwave System
- 2.6.9 Passive Infrared Motion Sensor
 - 2.6.9.1 Test Indicator, Passive Infrared
 - 2.6.9.2 Remote Test, Passive Infrared
- 2.6.10 Microwave-Passive Infrared Dual Detection Motion Sensor
 - 2.6.10.1 Test Indicator
 - 2.6.10.2 Remote Test
- 2.6.11 Photo-Electric Sensor (Interior)
 - 2.6.11.1 Test Indicator, Photo-Electric
 - 2.6.11.2 Remote Test, Photo-Electric
- 2.6.12 Capacitance Proximity Sensor
 - 2.6.12.1 Test Indicator, Capacitance
 - 2.6.12.2 Remote Test, Capacitance
- 2.6.13 Video Motion Sensor (Interior)
- 2.6.14 Access/Secure Switches
- 2.7 EXTERIOR INTRUSION SENSORS
 - 2.7.1 Bistatic Microwave Sensor
 - 2.7.1.1 Test Indicator, Bistatic
 - 2.7.1.2 Remote Test, Bistatic
 - 2.7.2 Monostatic Microwave Sensor
 - 2.7.2.1 Test Indicator, Monostatic
 - 2.7.2.2 Remote Test, Monostatic
 - 2.7.3 Strain Sensitive Cable Sensor
 - 2.7.3.1 Test Indicator, Strain Sensitive
 - 2.7.3.2 Remote Test, Strain Sensitive
 - 2.7.4 Passive Infrared Motion Sensor (Exterior)
 - 2.7.4.1 Test Indicator, Passive Infrared Motion Sensor
 - 2.7.5 Tension Wire Fence Sensor
 - 2.7.6 Capacitance Fence Sensor
 - 2.7.7 Buried Ported Cable
 - 2.7.7.1 Test Indicator, Buried Ported Cable
 - 2.7.7.2 Remote Test, Buried Ported Cable
 - 2.7.8 Photo-Electric Sensor (Exterior)
 - 2.7.8.1 Test Indicator, Photo-Electric Exterior
 - 2.7.8.2 Remote Test, Photo-Electric Exterior
 - 2.7.9 Video Motion Sensor (Exterior)
- 2.8 ENTRY CONTROL DEVICES
 - 2.8.1 Card Readers and Credential Cards
 - 2.8.1.1 Magnetic Stripe
 - 2.8.1.2 Weigand Wire Effect
 - 2.8.1.3 Proximity
 - 2.8.1.4 Card Reader Display
 - 2.8.1.5 Card Reader Response Time
 - 2.8.1.6 Card Reader Power
 - 2.8.1.7 Card Reader Mounting Method
 - 2.8.1.8 Credential Card Modification
 - 2.8.1.9 Card Size and Dimensional Stability
 - 2.8.1.10 Card Materials and Physical Characteristics
 - 2.8.1.11 Card Construction
 - 2.8.1.12 Card Durability and Maintainability
 - 2.8.2 Keypads
 - 2.8.2.1 Keypad Display
 - 2.8.2.2 Keypad Response Time
 - 2.8.2.3 Keypad Power
 - 2.8.2.4 Keypad Mounting Method

- 2.8.2.5 Keypad Duress Codes
- 2.8.3 Card Readers With Integral Keypad
 - 2.8.3.1 Magnetic Stripe
 - 2.8.3.2 Proximity
- 2.8.4 Personal Identity Verification Equipment
 - 2.8.4.1 Eye Retina Scanner
 - 2.8.4.2 Hand Geometry
 - 2.8.4.3 Fingerprint Analysis Scanner
 - 2.8.4.4 Iris Scan Device
- 2.8.5 Portal Control Devices
 - 2.8.5.1 Push-button Switches
 - 2.8.5.2 Panic Bar Emergency Exit With Alarm
 - 2.8.5.3 Electric Door Strikes/Bolts
 - 2.8.5.4 Electromagnetic Lock
 - 2.8.5.5 Entry Booth
 - 2.8.5.6 Booth Security and Operational Enhancements
 - 2.8.5.7 Entry Booth Electrical Requirements
 - 2.8.5.8 Vehicle Gate Opener
- 2.9 SURVEILLANCE AND DETECTION EQUIPMENT
 - 2.9.1 Article Surveillance/X-Ray
 - 2.9.1.1 Size and Weight
 - 2.9.1.2 Local Audible Alarms
 - 2.9.1.3 Maximum Package Size
 - 2.9.1.4 X-Ray Tube
 - 2.9.1.5 Electrical
 - 2.9.1.6 Safety
 - 2.9.1.7 Display
 - 2.9.1.8 Conveyor
 - 2.9.1.9 Material Identification and Resolution
 - 2.9.2 Metal Detector
 - 2.9.2.1 Size and Weight
 - 2.9.2.2 Local Alarms
 - 2.9.2.3 Material Identification and Sensitivity
 - 2.9.2.4 Traffic Counter
 - 2.9.2.5 Electrical
- 2.10 ENTRY CONTROL SOFTWARE
 - 2.10.1 Interface Device
 - 2.10.2 Operator Interface
 - 2.10.3 Entry Control Functions
 - 2.10.3.1 Multiple Security Levels
 - 2.10.3.2 Two person rule
 - 2.10.3.3 Anti-Passback
 - 2.10.3.4 Immediate Access Change
 - 2.10.3.5 Multiple Time Zones
 - 2.10.3.6 Guard Tour
 - 2.10.3.7 Elevator Control
 - 2.10.4 Electronic Entry Control System Capacities
 - 2.10.4.1 Enrollees
 - 2.10.4.2 Transaction History File Size
 - 2.10.5 Entry Control System Alarms
 - 2.10.5.1 Duress
 - 2.10.5.2 Guard Tour
 - 2.10.5.3 Entry Denial
 - 2.10.5.4 Portal Open
 - 2.10.5.5 Bolt Not Engaged
 - 2.10.5.6 Strike Not Secured
 - 2.10.5.7 Alarm Shunting/System Bypass
- 2.11 WIRE AND CABLE
 - 2.11.1 Above Ground Sensor Wiring

- 2.11.2 Direct Burial Sensor Wiring
- 2.11.3 Local Area Network (LAN) Cabling

PART 3 EXECUTION

- 3.1 GENERAL REQUIREMENTS
 - 3.1.1 Installation
 - 3.1.2 Enclosure Penetrations
 - 3.1.3 Cold Galvanizing
 - 3.1.4 Current Site Conditions
 - 3.1.5 Existing Equipment
 - 3.1.6 Installation Software
- 3.2 SYSTEM STARTUP
- 3.3 SUPPLEMENTAL CONTRACTOR QUALITY CONTROL
- 3.4 TESTING
 - 3.4.1 General Requirements for Testing
 - 3.4.2 Predelivery Testing
 - 3.4.2.1 Test Setup
 - 3.4.3 Contractor's Field Testing
 - 3.4.4 Performance Verification Test
 - 3.4.5 Endurance Test
- 3.5 RELIABILITY CALCULATION
 - 3.5.1 Definition of Reliability
 - 3.5.2 Series and Parallel Components
 - 3.5.3 Calculation Procedure
 - 3.5.4 Sample Calculations

-- End of Section Table of Contents --

USACE / NAVFAC / AFCESA UFGS-13720A (July 2003)

Preparing Activity: USACE Superseding
UFGS-13720A (May 1998)

UNIFIED FACILITIES GUIDE SPECIFICATIONS

References are in agreement with UMRL dated 25 June 2004

Latest Change indicate by CHG tags

SECTION 13720A

ELECTRONIC SECURITY SYSTEM 07/03

NOTE: This guide specification covers the requirements for an intrusion detection and electronic entry control system.

Comments and suggestions on this guide specification are welcome and should be directed to the technical proponent of the specification. A listing of technical proponents, including their organization designation and telephone number, is on the Internet.

Recommended changes to a UFGS should be submitted as a Criteria Change Request (CCR).

Use of electronic communication is encouraged.

Brackets are used in the text to indicate designer choices or locations where text must be supplied by the designer.

PART 1 GENERAL

NOTE: The section number should be inserted in the specification heading and prefixed to each page number in the project specifications. This section will be used in conjunction with Section 16415A ELECTRICAL WORK, INTERIOR; Section 16370A ELECTRICAL DISTRIBUTION SYSTEM, AERIAL; Section 16375A ELECTRICAL DISTRIBUTION SYSTEM, UNDERGROUND; Section 16792A WIRE LINE DATA TRANSMISSION SYSTEMS; Section 16768A FIBER OPTIC DATA TRANSMISSION SYSTEM; Section 16751A CLOSED CIRCUIT TELEVISION SYSTEMS; and any other guide specification sections required by the design.

1.1 REFERENCES

NOTE: Issue (date) of references included in
project specifications need not be more current than
provided by the latest guide specification. Use of
SpecsIntact automated reference checking is
recommended for projects based on older guide
specifications.

The publications listed below form a part of this specification to the extent referenced. The publications are referred to within the text by the basic designation only.

AMERICAN CONFERENCE OF GOVERNMENTAL INDUSTRIAL HYGIENISTS (ACGIH)

ACGIH 0100Doc (2001) Documentation of the Threshold
Limit Values and Biological Exposure
Indices

AMERICAN NATIONAL STANDARDS INSTITUTE (ANSI)

ANSI INCITS 154 (1988; R 1999) Office Machines and
Supplies - Alphanumeric Machines-Keyboards
Arrangement

ANSI INCITS 92 (1981; R 1998) Data Encryption Algorithm

ASTM INTERNATIONAL (ASTM)

ASTM E 84 (2003) Surface Burning Characteristics of
Building Materials

ELECTRONIC INDUSTRIES ALLIANCE (EIA)

EIA 170 (1957) Electrical Performance Standards -
Monochrome Television Studio Facilities

EIA ANSI/EIA-310-D (1992) Racks, Panels, and Associated
Equipment

EIA ANSI/EIA/TIA-232-F (2002) Interface Between Data Terminal
Equipment and Data Circuit-Terminating
Equipment Employing Serial Binary Data
Interchange

EIA ANSI/TIA/EIA-568-A (1995; Addendum 3 1998) Commercial
Building Telecommunications Cabling
Standard - 3 Parts

INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS (IEEE)

IEEE C2 (2002) National Electrical Safety Code

IEEE C62.41 (1991) Recommended Practice for Surge
Voltages in Low-Voltage AC Power Circuits

IEEE Std 142 (1992) Recommended Practice for Grounding

of Industrial and Commercial Power Systems
- Green Book

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION (ISO)

ISO 7810	(2003) Identification Cards - Physical Characteristics
ISO 7811-1	(2002) Identification Cards - Recording Technique - Part 1: Embossing
ISO 7811-2	(2001) Identification Cards - Recording Technique - Part 2: Magnetic Stripe - Low Coercivity
ISO 7811-3	(1995) Identification Cards - Recording Technique - Part 3: Location of Embossed Characters on ID-1 Cards
ISO 7811-4	(1995) Identification Cards - Recording Technique - Part 4: Location of Read-Only Magnetic Tracks - Tracks 1 and 2
ISO 7811-5	(1995) Identification Cards - Recording Technique - Part 5: Location of Read-Write Magnetic Track - Track 3

INTERNATIONAL TELECOMMUNICATION UNION (ITU)

ITU V.34	(1998) Data Communication Over the Telephone Network: A Modem Operating at Data Signaling Rates of up to 33,600 bits for use on the General Switched Telephone Network and on Leased Point-to-Point Two-Wire Telephone Type Circuits
ITU V.42	(2002) Data Communications Over the Telephone Network: Error-Correcting Procedures for DCEs Using Asynchronous-to-Synchronous Conversion

NATIONAL ELECTRICAL MANUFACTURERS ASSOCIATION (NEMA)

NEMA 250	(2003) Enclosures for Electrical Equipment (1000 Volts Maximum)
NEMA ICS 1	(2000) Industrial Control and Systems: General Requirements

NATIONAL FIRE PROTECTION ASSOCIATION (NFPA)

NFPA 70	(2002) National Electrical Code
---------	---------------------------------

U.S. NATIONAL ARCHIVES AND RECORDS ADMINISTRATION (NARA)

21 CFR 1020	Performance Standards for Ionizing Radiation Emitting Products
47 CFR 15	Radio Frequency Devices

47 CFR 68

Connection of Terminal Equipment to the
Telephone Network

UNDERWRITERS LABORATORIES (UL)

UL 1037	(1999; Rev thru Sep 1999) Antitheft Alarms and Devices
UL 1076	(1995; Rev thru Feb 1999) Proprietary Burglar Alarm Units and Systems
UL 294	(1999; Rev thru Oct 2001) Access Control System Units
UL 639	(1997; Rev thru Sep 2002) Intrusion Detection Units
UL 681	(1999; Rev thru Jan 2001) Installation and Classification of Burglar and Holdup Alarm Systems
UL 796	(1999; Rev thru Dec 2003) Printed-Wiring Boards
UL 972	(2002) Burglary Resisting Glazing Material

1.2 SYSTEM DESCRIPTION

NOTE: The designer must show sensor detection patterns, entry control terminal devices, portal control, facility interface, personnel identity verification, surveillance and detection equipment locations, and quantities and installation details on drawings. Add requirements for additional site specific conditions such as furniture/equipment layout within protected areas, and hazard location areas, type of hazard, class, and group.

The Contractor shall provide an Electronic Security System (ESS) as described and shown including installation of any Government Furnished Equipment. All computing devices, as defined in 47 CFR 15, shall be certified to comply with the requirements for Class A computing devices and labeled as set forth in 47 CFR 15. Electronic equipment shall comply with 47 CFR 15.

1.2.1 Central Station

The central station shall be configured to provide operator interface, interaction, dynamic and real time monitoring, display, and control. The central station shall control system networks to interconnect all system components including subordinate or separate control stations, enrollment stations and field equipment. The system shall be able to manage up to 16,000 uniquely identifiable inputs and outputs.

1.2.2 Systems Networks

System networks shall interconnect all components of the system. These networks shall include communications between a central station and any subordinate or separate station, enrollment stations, local annunciation stations, portal control stations or redundant central stations. The systems network shall provide totally automatic communication of status changes, commands, field initiated interrupts and any other communications required for proper system operation. System communication shall not require operator initiation or response. System communication shall return to normal after any partial or total network interruption such as power loss or transient upset. The system shall automatically annunciate communication failures to the operator with identification of the communication link that has experienced a partial or total failure. A communications controller may be used as an interface between the central station display systems and the field device network. The communications controller shall provide those functions needed to attain the specified network communications performance.

1.2.2.1 Console Network

A console network, if required, shall provide communication between a central station and any subordinate or separate stations of the system. Where redundant central or parallel stations are required, the console network shall allow the configuration of stations as master and slave. The console network may be a part of the field device network or may be separate depending upon the manufacturer's system configuration.

1.2.2.2 Field Device Network

The field device network shall provide communication between a central control station and field devices of the system. The field device network shall be configured as shown in the drawings. Field devices shall consist of alarm annunciation local processors and entry control local processors. Each field device shall be interrogated during each interrogation cycle. The field device network shall provide line supervision that detects and annunciates communications interruptions or compromised communications between any field device and the central station.

1.2.3 Field Equipment

Field equipment shall include local processors, sensors and controls. Local processors shall serve as an interface between the central station and sensors and controls. Data exchange between the central station and the local processors shall include down-line transmission of commands, software and databases to local processors. The up line data exchange from the local processor to the central station shall include status data such as intrusion alarms, status reports and entry control records. Local processors are categorized as alarm annunciation or entry control.

1.2.4 CCTV System Interface

**NOTE: This interface is required only if a CCTV
system is part of the design.**

An interface shall be provided for connection of the central station to the CCTV system as specified in Section 16751A CLOSED CIRCUIT TELEVISION

SYSTEMS and as shown. This shall not be accomplished by using an electro-mechanical relay assembly.

1.2.5 Overall System Reliability Requirements

The system, including all components and appurtenances, shall be configured and installed to yield a mean time between failure (MTBF) of at least 10,000 hours.

1.2.6 Error Detection and Retransmission

A cyclic code error detection method shall be used between local processors and the central station, which shall detect single and double bit errors, burst errors of 8 bits or less, and at least 99 percent of all other multibit and burst error conditions. Interactive or product error detection codes alone will not be acceptable. A message shall be in error if 1 bit is received incorrectly. The system shall retransmit messages with detected errors. A 2-digit decimal number shall be operator assignable to each communication link representing the number of retransmission attempts. When the number of consecutive retransmission attempts equals the assigned quantity, the central station shall print a communication failure alarm message. The system shall monitor the frequency of data transmission failure for display and logging.

1.2.7 System Definitions

1.2.7.1 Intrusion Alarm

An alarm resulting from the detection of a specified target, caused by an attempt to intrude into the protected area, or when entry into an entry controlled area is attempted without successfully using entry control procedures.

1.2.7.2 Nuisance Alarm

An alarm resulting from the detection of an appropriate alarm stimulus, but which does not represent an attempt to intrude into the protected area.

1.2.7.3 Environmental Alarm

An alarm during environmental conditions which exceed those specified.

1.2.7.4 False Alarm

An alarm when there is no alarm stimulus.

1.2.7.5 Duress Alarm

An alarm condition which results from a set of pre-established conditions such as entering a special code into a keypad or by activating a switch. This alarm category shall take precedence over other alarm categories.

1.2.7.6 Guard Tour Alarm

An alarm resulting from a guard being either early or late at a specified check-in location.

1.2.7.7 Fail-Safe Alarm

An alarm resulting from detection of diminished functional capabilities.

1.2.7.8 Power Loss Alarm

An alarm resulting from a loss of primary power.

1.2.7.9 Entry Control Alarm

An alarm resulting from improper use of entry control procedures or equipment.

1.2.7.10 Identifier

A card credential, keypad personal identification number or code, biometric characteristic or any other unique identification entered as data into the entry control database for the purpose of identifying an individual. Identifiers shall be used by the electronic security system for the purpose of validating passage requests for areas equipped with entry control equipment.

1.2.7.11 Entry Control Devices

Any equipment which gives a user the means to input identifier data into the entry control system for verification.

1.2.7.12 Facility Interface Device

A facility interface device shall be any type of mechanism which is controlled in response to passage requests and allows passage through a portal.

1.2.8 Probability of Detection

Each zone shall have a continuous probability of detection greater than 90 percent and shall be demonstrated with a confidence level of 95 percent. This probability of detection is defined as 49 successful detections out of 50 tests or 96 successful detections out of 100 tests.

1.2.9 Standard Intruder

The system shall be able to detect an intruder that weighs 100 pounds or less and is 5 feet tall or less. The intruder shall be dressed in a long-sleeved shirt, slacks and shoes unless environmental conditions at the site require protective clothing.

1.2.9.1 Standard Intruder Movement

Standard intruder movement is defined as any movement such as walking, running, crawling, rolling, or jumping through a protected zone in the most advantageous manner for the intruder.

1.2.10 False Alarm Rate

1.2.10.1 Interior

A false alarm rate of no more than 1 false alarm per sensor per 30 days at the specified probability of detection shall be provided.

1.2.10.2 Exterior

A false alarm rate of no more than 1 false alarm per sensor per 5 days at the specified probability of detection shall be provided.

1.2.11 Error and Throughput Rates

Error and throughput rates shall be single portal performance rates obtained when processing individuals 1 at a time.

1.2.11.1 Type I Error Rate

Type I error rate is defined as an error where the system denies entry to an authorized, enrolled individual. The rate shall be less than 1 percent.

1.2.11.2 Type II Error Rate

NOTE: The designer will decide what level of security is appropriate for the project. An error rate of 0.1 percent should be used for medium security projects, 0.01 percent for high security projects, and 0.001 percent should be selected for extremely high security projects. The smaller number will be more difficult to meet and therefore more costly. The designer should carefully consider the needs of the site when making this choice.

Type II error rate is defined as an error where the system grants entry to an unauthorized individual. The entry control Type II error rate shall be less than [0.1] [0.01] [0.001] percent.

1.2.12 System Throughput

NOTE: To support this paragraph the designer will show the throughput rates needed at each portal on the drawings or in a table. The designer will calculate the number of people entering through each portal at peak traffic periods with system response and processing times for each passage request taken into account.

At the specified error rates, the system throughput rate through a single portal shall be as shown.

1.2.13 Passage

NOTE: The designer will show on the drawings whether entry control is used for ingress or for egress at each portal.

Passage is defined as ingress and/or egress past an entry control device, or through a portal. Entry control procedures and equipment shall be implemented for passage through each portal as shown.

1.2.14 Detection Resolution

The system shall have detection resolution sufficient to locate intrusions at each device and zone; and tampering at individual devices.

1.2.15 Electrical Requirements

NOTE: The designer will select the correct line frequency and voltage and show on the drawings the characteristics of each voltage source.

Electrically powered ESS equipment shall operate on [120] [240] volt [60] [50] Hz ac sources as shown. Equipment shall be able to tolerate variations in the voltage source of plus or minus 10 percent, and variations in the line frequency of plus or minus 2 percent with no degradation of performance.

1.2.16 Power Line Surge Protection

Equipment connected to alternating current circuits shall be protected from power line surges. Equipment protection shall withstand surge test waveforms described in IEEE C62.41. Fuses shall not be used for surge protection.

1.2.17 Sensor and Device Wiring and Communication Circuit Surge Protection

Inputs shall be protected against surges induced on device wiring. Outputs shall be protected against surges induced on control and device wiring installed outdoors and as shown. Communications equipment shall be protected against surges induced on any communications circuit. Cables and conductors, except fiber optics, which serve as communications circuits from console to field equipment, and between field equipment, shall have surge protection circuits installed at each end. Protection shall be furnished at equipment, and additional triple electrode gas surge protectors rated for the application on each wireline circuit shall be installed within 1 m 3 feet of the building cable entrance. Fuses shall not be used for surge protection. The inputs and outputs shall be tested in both normal mode and common mode using the following two waveforms:

- a. A 10 microsecond rise time by 1000 microsecond pulse width waveform with a peak voltage of 1500 Volts and a peak current of 60 amperes.
- b. An 8 microsecond rise time by 20 microsecond pulse width waveform with a peak voltage of 1000 Volts and a peak current of 500 amperes.

1.2.18 Power Line Conditioners

A power line conditioner shall be furnished for the console equipment and each local processor. The power line conditioners shall be of the ferro-resonant design, with no moving parts and no tap switching, while electrically isolating the secondary from the power line side. The power line conditioners shall be sized for 125 percent of the actual connected kVA load. Characteristics of the power line conditioners shall be as follows:

- a. At 85 percent load, the output voltage shall not deviate by more

than plus or minus 1 percent of nominal when the input voltage fluctuates between minus 20 percent to plus 10 percent of nominal.

b. During load changes of zero to full load, the output voltage shall not deviate by more than plus or minus 3 percent of nominal. Full correction of load switching disturbances shall be accomplished within 5 cycles, and 95 percent correction shall be accomplished within 2 cycles of the onset of the disturbance.

c. Total harmonic distortion shall not exceed 3-1/2 percent at full load.

1.2.19 System Reaction

NOTE: The designer must determine the required system end-to-end response. Short response times such as 1 second, are only required for systems where alarm actuated CCTV assessment will be applied. In other situations, response times as high as 3 or 4 seconds are acceptable. Large systems with many entry control devices may be unable to achieve short response times.

1.2.19.1 System Response

The field device network shall provide a system end-to-end response time of [1 second] [_____] or less for every device connected to the system. Alarms shall be annunciated at the central station within 1 second of the alarm occurring at a local processor or device controlled by a local processor, and within 100 milliseconds if the alarm occurs at the central station. Alarm and status changes shall be displayed within 100 milliseconds after receipt of data by the central station. All graphics shall be displayed, including graphics generated map displays, on the console monitor within 5 seconds of alarm receipt at the security console. This response time shall be maintained during system heavy load.

1.2.19.2 System Heavy Load Definition

For the purpose of system heavy load definition, the system shall consist of central station equipment, communication controller and required local processors. System heavy load conditions are defined as the occurrence of alarms at the rate of 10 alarms per second distributed evenly among all local processors in the system. The alarm printer shall continue to print out all occurrences, including time of occurrence, to the nearest second.

1.2.20 Environmental Conditions

1.2.20.1 Interior, Controlled Environment

System components, except the console equipment installed in interior locations, having controlled environments shall be rated for continuous operation under ambient environmental conditions of 2 to 50 degrees C 36 to 122 degrees F dry bulb and 20 to 90 percent relative humidity, non-condensing.

1.2.20.2 Interior, Uncontrolled Environment

System components installed in interior locations having uncontrolled environments shall be rated for continuous operation under ambient environmental conditions of minus 18 to plus 50 degrees C 0 to 122 degrees F dry bulb and 10 to 95 percent relative humidity, non-condensing.

1.2.20.3 Exterior Environment

System components that are installed in locations exposed to weather shall be rated for continuous operation under ambient environmental conditions of minus 34 degrees C to 50 degrees C minus 30 to 122 degrees F dry bulb and 10 to 95 percent relative humidity, condensing. In addition, the system components shall be rated for continuous operation when exposed to performance conditions as specified in UL 294 and UL 639 for outdoor use equipment. Components shall be rated for continuous operation when exposed to rain as specified in NEMA 250, winds up to 137 km per hr 85 mph and snow cover up to 610 mm 2 feet thick, measured vertically.

1.2.20.4 Hazardous Environment

System components located in areas where fire or explosion hazards may exist because of flammable gases or vapors, flammable liquids, combustible dust, or ignitable fibers or flyings, shall be rated and installed according to Chapter 5 of the NFPA 70 and as shown.

1.2.20.5 Console

Console equipment, unless designated otherwise, shall be rated for continuous operation under ambient environmental conditions of 16 to 29 degrees C 60 to 85 degrees F and a relative humidity of 20 to 80 percent.

1.2.21 System Capacity

NOTE: The designer will show the devices to be monitored and controlled on the drawings. These devices include all types of ESS hardware to be interconnected into the system. The designer should also include provision for any known future expansion needs plus 25% (minimum).

The system will monitor and control the number of inputs and outputs shown and will include an expansion capability of a minimum of 25 percent. The system will discriminate to the individual sensors, switches, and terminal devices and report status at the central station as shown.

1.3 DELIVERY OF TECHNICAL DATA AND COMPUTER SOFTWARE

NOTE: The acquisition of technical data, data bases, and computer software items that are identified herein will be accomplished in accordance with the Federal Acquisition Regulation (FAR) and the Department of Defense Acquisition Regulation Supplement (DOD FARS). Those regulations as well as

the Army and Corps of Engineers implementations thereof should also be consulted to ensure that a delivery of critical items of technical data is not inadvertently lost. Specifically, the Rights in Technical Data and Computer Software Clause, DOD FARS 52.227-7013, and the Data Requirements Clause, DOD FARS 52.227-7013, as well as any requisite software licensing agreements will be made a part of the CONTRACT CLAUSES or SPECIAL CONTRACT REQUIREMENTS of the contract. In addition, the appropriate DD FORM 1423 Contract Data Requirements List, will be filled out for each distinct deliverable data item and made a part of the contract. Where necessary, DD FORM 1664, Data Item Description, shall be used to explain and more fully identify the data items listed on the DD FORM 1423. It is to be noted that all of these clauses and forms are required to assure the delivery of data in question and that such data is obtained with the requisite rights to use by the Government. Include with the request for proposals a completed DD FORM 1423, Contract Data Requirements List. This form is essential to obtain delivery of all documentation. Each deliverable will be clearly specified, both description and quantity being required. Include a payment schedule in the SPECIAL CONTRACT REQUIREMENTS of the request for proposals. This payment schedule will define payment milestones and percentages at specific times during the contract period.

All items of computer software and technical data (including technical data which relates to computer software), which is specifically identified in this specification shall be delivered in accordance with the CONTRACT CLAUSES, SPECIAL CONTRACT REQUIREMENTS, and in accordance with the Contract Data Requirements List (CDRL), DD FORM 1423, which is attached to and thereby made a part of this contract. All data delivered shall be identified by reference to the particular specification paragraph against which it is furnished.

1.3.1 Group I Technical Data Package

1.3.1.1 System Drawings

NOTE: Item (i) is required only if a CCTV system is incorporated as part of this design.

The data package shall include the following:

- a. System block diagram.
- b. Console installation, block diagrams, and wiring diagrams.
- c. Local processor installation, typical block, and wiring diagrams.
- d. Local processor physical layout and schematics.

- e. Device wiring and installation drawings.
- f. Details of connections to power sources, including power supplies and grounding.
- g. Details of surge protection device installation.
- h. Sensor detection patterns.
- i. Details of interconnections with CCTV system.

1.3.1.2 Manufacturer's Data

The data package shall include manufacturer's data for all materials and equipment, including terminal devices, local processors and central station equipment provided under this specification.

1.3.1.3 System Description and Analyses

The data package shall include system descriptions, analyses, and calculations used in sizing equipment specified. Descriptions and calculations shall show how the equipment will operate as a system to meet the performance of this specification. The data package shall include the following:

- a. Central processor memory size.
- b. Communication speeds and protocol descriptions.
- c. Hard disk size and configuration.
- d. Floppy disk size and configuration.
- e. Alarm response time calculations.
- f. Command response time calculations.
- g. Start-up operations.
- h. Expansion capability and method of implementation.
- i. Sample copy of each report specified.
- j. Color photographs representative of typical graphics.
- k. System throughput calculation.

1.3.1.4 Software Data

The software data package shall consist of descriptions of the operation and capability of system, and application software as specified.

1.3.1.5 Overall System Reliability Calculations

The overall system reliability calculations data package shall include all manufacturer's reliability data and calculations required to show compliance with the specified reliability in accordance with paragraph, OVERALL SYSTEM RELIABILITY REQUIREMENTS.

1.3.1.6 Certifications

Specified manufacturer's certifications shall be included with the data package certification.

1.3.1.7 Key Control Plan

The Contractor shall provide a key control plan. The key control plan shall include the following:

- a. Procedures that will be used to log and positively control all keys during installation.
- b. A listing of all keys and where they are used.
- c. A listing of all persons allowed access to the keys.

1.3.2 Group II Technical Data Package

The Contractor shall prepare a report of "Current Site Conditions" to the Government documenting changes to the site, or conditions that affect performance of the system to be installed. The Contractor shall provide specification sheets, or written functional requirements to support the findings, and a cost estimate to correct those site changes or conditions. The Contractor shall not correct any deficiency without written permission from the Government.

1.3.3 Group III Technical Data Package

The Contractor shall prepare test procedures and reports for the pre-delivery test.

1.3.4 Group IV Technical Data Package

The Contractor shall prepare test procedures and reports for the performance verification test and the endurance test. The Contractor shall deliver the performance verification test and endurance test procedures to the Government for approval.

1.3.4.1 Operation and Maintenance Manuals

A draft copy of the operation and maintenance manuals, as specified for the Group V technical data package, shall be delivered to the Government prior to beginning the performance verification test for use during site testing.

1.3.4.2 Training Documentation

Lesson plans and training manuals for the training phases, including type of training to be provided, and a list of reference material, shall be delivered for approval.

1.3.4.3 Data Entry

The Contractor shall enter all data needed to make the system operational. The Contractor shall deliver the data to the Government on data entry forms, utilizing data from the contract documents, Contractor's field surveys, and other pertinent information in the Contractor's possession required for complete installation of the data base. The Contractor shall

identify and request from the Government, any additional data needed to provide a complete and operational ESS. The completed forms shall be delivered to the Government for review and approval at least 30 days prior to the Contractor's scheduled need date.

1.3.4.4 Graphics

NOTE: The designer will show on the drawings the areas that are to be incorporated into the graphics package.

Where graphics are required and are to be delivered with the system, the Contractor shall create and install the graphics needed to make the system operational. The Contractor shall utilize data from the contract documents, Contractor's field surveys, and other pertinent information in the Contractor's possession to complete the graphics. The Contractor shall identify and request from the Government, any additional data needed to provide a complete graphics package. Graphics shall have sufficient level of detail for the system operator to assess the alarm. The Contractor shall supply hard copy, color examples at least 200 x 250 mm 8 x 10 inches in size, of each type of graphic to be used for the completed system. The graphics examples shall be delivered to the Government for review and approval at least 30 days prior to the Contractor's scheduled need date.

1.3.5 Group V Technical Data Package

NOTE: The designer will specify the correct number of manuals on DD FORM 1423. Unless the installation has a specific requirement, specify 2 copies of all manuals, except the Operator's Manual, which should be specified to be 6 copies.

Final copies of the manuals as specified, bound in hardback, loose-leaf binders, shall be delivered to the Government within 30 days after completing the endurance test. The draft copy used during site testing shall be updated with any changes required prior to final delivery of the manuals. Each manual's contents shall be identified on the cover. The manual shall include names, addresses, and telephone numbers of each subcontractor installing equipment and systems, and nearest service representative for each item of equipment. The manuals shall have a table of contents and tab sheets. Tab sheets shall be placed at the beginning of each chapter or section and at the beginning of each appendix. The final copies delivered after completion of the endurance test shall include modifications made during installation, checkout, and acceptance. The number of copies of each manual to be delivered shall be as specified on DD FORM 1423.

1.3.5.1 Functional Design Manual

The functional design manual shall identify the operational requirements for the system and explain the theory of operation, design philosophy, and specific functions. A description of hardware and software functions, interfaces, and requirements shall be included for all system operating modes.

1.3.5.2 Hardware Manual

A manual describing all equipment furnished including:

- a. General description and specifications.
- b. Installation and checkout procedures.
- c. Equipment electrical schematics and layout drawings.
- d. System schematics and layout drawings.
- e. Alignment and calibration procedures.
- f. Manufacturer's repair parts list indicating sources of supply.
- g. Interface definition.

1.3.5.3 Software Manual

The software manual shall describe the functions of all software and shall include all other information necessary to enable proper loading, testing, and operation. The manual shall include:

- a. Definition of terms and functions.
- b. Use of system and applications software.
- c. Procedures for system initialization, start-up and shutdown.
- d. Alarm reports.
- e. Reports generation.
- f. Data base format and data entry requirements.
- g. Directory of all disk files.
- h. Description of all communication protocols, including data formats, command characters, and a sample of each type of data transfer.

1.3.5.4 Operator's Manual

The operator's manual shall fully explain all procedures and instructions for the operation of the system, including:

- a. Computers and peripherals.
- b. System start-up and shutdown procedures.
- c. Use of system, and applications software.
- d. Recovery and restart procedures.
- e. Graphic alarm presentation.
- f. Use of report generator and generation of reports.

- g. Data entry.
- h. Operator commands.
- i. Alarm and system messages and printing formats.
- j. System entry requirements.

1.3.5.5 Maintenance Manual

The maintenance manual shall include descriptions of maintenance for all equipment including inspection, periodic preventive maintenance, fault diagnosis, and repair or replacement of defective components.

1.3.5.6 Final System Drawings

The Contractor shall maintain a separate set of drawings, elementary diagrams and wiring diagrams of the system to be used for final system drawings. This set shall be accurately kept up-to-date by the Contractor with all changes and additions to the ESS and shall be delivered to the Government with the final endurance test report. In addition to being complete and accurate, this set of drawings shall be kept neat and shall not be used for installation purposes. Final drawings submitted with the endurance test report shall be finished drawings on vellum and CD-ROM.

1.4 TESTING

1.4.1 General

The Contractor shall perform pre-delivery testing, site testing, and adjustment of the completed ESS. The Contractor shall provide personnel, equipment, instrumentation, and supplies necessary to perform testing. Written notification of planned testing shall be given to the Government at least 14 days prior to the test; notice shall not be given until after the Contractor has received written approval of the specific test procedures.

1.4.2 Test Procedures and Reports

Test procedures shall explain in detail, step-by-step actions and expected results, demonstrating compliance with the requirements specified. Test reports shall be used to document results of the tests. Reports shall be delivered to the Government within 7 days after completion of each test.

1.5 TRAINING

1.5.1 General

NOTE: The designer shall coordinate the training requirements with the installation and designate the number of persons to be trained.

The Contractor shall conduct training courses for designated personnel in the maintenance and operation of the system as specified. The training shall be oriented to the specific system being installed. Training manuals shall be delivered for each trainee with 2 additional copies delivered for archiving at the project site. The manuals shall include an agenda, defined objectives for each lesson, and a detailed description of the

subject matter for each lesson. The Contractor shall furnish audio-visual equipment and other training materials and supplies. Where the Contractor presents portions of the course by audio-visual material, copies of the audio-visual material shall be delivered to the Government either as a part of the printed training manuals or on the same media as that used during the training sessions. A training day is defined as 8 hours of classroom instruction, including 2 15-minute breaks and excluding lunchtime, Monday through Friday, during the daytime shift in effect at the training facility. For guidance in planning the required instruction, the Contractor shall assume that attendees will have a high school education or equivalent, and are familiar with ESS. Approval of the planned training schedule shall be obtained from the Government at least 30 days prior to the training.

1.5.2 Operator's Training I

The first course shall be taught at the project site for a period of 5 consecutive training days at least 3 months prior to the scheduled performance verification test. A maximum of [12] [_____] personnel shall attend this course. Upon completion of this course, each student, using appropriate documentation, shall be able to perform elementary operations with guidance and describe the general hardware architecture and functionality of the system. This course shall include:

- a. General System hardware architecture.
- b. Functional operation of the system.
- c. Operator commands.
- d. Data base entry.
- e. Reports generation.
- f. Alarm reporting.
- g. Diagnostics.

1.5.3 Operator's Training II

The second course shall be taught at the project site for a period of 5 consecutive training days during or after the Contractor's field testing, but before commencing the performance verification test. A maximum of [12] [_____] personnel shall attend the course. No part of the training given during this course will be counted toward completion of the performance verification test. The course shall include instruction on the specific hardware configuration of the installed system and specific instructions for operating the installed system. Upon completion of this course, each student shall be able to start the system, operate the system, recover the system after a failure, and describe the specific hardware architecture and operation of the system.

1.5.4 Operator's Training III

The third course shall be taught while the endurance test is in progress for a total of 16 hours of instruction per student, in time blocks of 4 hours. A maximum of [12] [_____] personnel shall attend the course. The schedule of instruction shall allow for each student to receive individual instruction for a 4-hour period in the morning (or afternoon) of the same

weekday. The Contractor shall schedule his activities during this period so that the specified amount of time will be available during the endurance test for instructing the students. The course shall consist of hands-on training under the constant monitoring of the instructor. The instructor shall be responsible for determining the appropriate password to be issued to the student commensurate with each student's acquired skills at the beginning of each of these individual training sessions. Upon completion of this course, the students shall be fully proficient in the operation of the system.

1.5.5 System Manager Training

[_____] system managers shall be trained for at least 3 consecutive days. The system manager training shall consist of the operator's training and the following:

- a. Enrollment/disenrollment.
- b. Assignments of identifier data.
- c. Assign operator password/levels.
- d. Change database configuration.
- e. Modify graphics.
- f. Print special or custom reports.
- g. System backup.
- h. Any other functions necessary to manage the system.

1.5.6 Maintenance Personnel Training

The system maintenance course shall be taught at the project site after completion of the endurance test for a period of 5 training days. A maximum of [5][_____] personnel, designated by the Government, will attend the course. The training shall include:

- a. Physical layout of each piece of hardware.
- b. Troubleshooting and diagnostics procedures.
- c. Repair instructions.
- d. Preventive maintenance procedures and schedules.
- e. Calibration procedures. Upon completion of this course, the students shall be fully proficient in the maintenance of the system.

1.6 LINE SUPERVISION

NOTE: Specify 5 percent line supervision for Level
A assets.

1.6.1 Signal and Data Transmission System (DTS) Line Supervision

All signal and DTS lines shall be supervised by the system. The system shall supervise the signal lines by monitoring the circuit for changes or disturbances in the signal, and for conditions as described in UL 1076 for line security equipment. The system shall initiate an alarm in response to a current change of [5] [10] percent or greater. The system shall also initiate an alarm in response to opening, closing, shorting, or grounding of the signal and DTS lines.

1.6.2 Data Encryption

NOTE: Data encryption should be used when required
by governing regulations or when it has been
determined that unauthorized persons may have access
to system intercommunications. The designer must
indicate which DTS circuits require data encryption.

The system shall incorporate data encryption equipment on data transmission circuits as shown. The algorithm used for encryption shall be the Data Encryption Standard (DES) algorithm described in ANSI INCITS 92.

1.7 DATA TRANSMISSION SYSTEM

NOTE: Include in the project specification 1 or
more of the following UFGS for the appropriate Data
Transmission required at the project site: Section
16792A WIRELINE DATA TRANSMISSION SYSTEMS; Section
16768A FIBER OPTIC DATA TRANSMISSION SYSTEM; or
Section 16794A COAXIAL CABLE DATA TRANSMISSION MEDIA.

The Contractor shall provide DTS as specified in Section [_____] and as shown.

1.8 MAINTENANCE AND SERVICE

NOTE: The maintenance and service to be provided by
the Contractor during first year's warranty period
will be included as a separate bid item, and must be
funded with O & M funds. The designer will
coordinate funding requirements with the
installation.

1.8.1 Warranty Period

The Contractor shall provide services required and equipment necessary to maintain the entire system in an operational state as specified, for a period of 1 year after formal written acceptance of the system, and shall provide necessary material required for performing scheduled adjustments or other nonscheduled work.

1.8.2 Description of Work

The adjustment and repair of the system includes all computer equipment, software updates, communications transmission equipment and DTS, local processors, sensors and entry control, facility interface, and support equipment. Responsibility shall be limited to Contractor installed equipment. The manufacturer's required adjustments and other work as necessary shall be provided.

1.8.3 Personnel

Service personnel shall be certified in the maintenance and repair of similar types of equipment and qualified to accomplish work promptly and satisfactorily. The Government shall be advised in writing of the name of the designated service representative, and of any change in personnel.

1.8.4 Schedule of Work

The Contractor shall perform 2 minor inspections at 6 month intervals (or more often if required by the manufacturer), and 2 major inspections offset equally between the minor inspections to effect quarterly inspection of alternating magnitude.

1.8.4.1 Minor Inspections

Minor inspections shall include visual checks and operational tests of console equipment, peripheral equipment, local processors, sensors, and electrical and mechanical controls. Minor inspections shall also include mechanical adjustments, new ribbons, and other necessary adjustments on printers.

1.8.4.2 Major Inspections

Major inspections shall include work described under paragraph Minor Inspections and the following work:

- a. Clean all system equipment and local processors, including interior and exterior surfaces.
- b. Perform diagnostics on all equipment.
- c. Check, walk test, and calibrate each sensor.
- d. Run all system software diagnostics and correct all diagnosed problems.
- e. Resolve any previous outstanding problems.
- f. Purge and compress data bases.

1.8.4.3 Scheduled Work

Scheduled work shall be performed during regular working hours, Monday through Friday, excluding federal holidays.

1.8.5 Emergency Service

NOTE: In some cases the designer may determine a

less rapid response time is acceptable when weighed
against the cost of the service. The designer must
insert a time based upon input from the user.

The Government will initiate service calls when the system is not functioning properly. Qualified personnel shall be available to provide service to the complete system. The Government shall be furnished with a telephone number where the service supervisor can be reached at all times. Service personnel shall be at site within [2][_____] hours after receiving a request for service. The system shall be restored to proper operating condition within 8 hours after service personnel arrive onsite.

1.8.6 Operation

Performance of scheduled adjustments and repair shall verify operation of the system as demonstrated by the applicable tests of the performance verification test.

1.8.7 Records and Logs

The Contractor shall keep records and logs of each task, and shall organize cumulative records for each component, and for the complete system chronologically. A continuous log shall be maintained for all devices. The log shall contain all initial settings. Complete logs shall be kept and shall be available for inspection on site, demonstrating that planned and systematic adjustments and repairs have been accomplished for the system.

1.8.8 Work Requests

The Contractor shall separately record each service call request, as received. The form shall include the serial number identifying the component involved, its location, date and time the call was received, specific nature of trouble, names of service personnel assigned to the task, instructions describing what has to be done, the amount and nature of the material to be used, the time and date work started, and the time and date of completion. The Contractor shall deliver a record of the work performed within 5 days after work is accomplished.

1.8.9 System Modifications

The Contractor shall make any recommendations for system modification in writing to the Government. System modifications shall not be made without prior approval of the Government. Any modifications made to the system shall be incorporated into the operation and maintenance manuals, and other documentation affected.

1.8.10 Software

The Contractor shall provide a description of all software updates to the Government, who will then decide whether or not they are appropriate for implementation. After notification by the Government, the Contractor shall implement the designated software updates and verify operation in the system. These updates shall be accomplished in a timely manner, fully coordinated with system operators, and shall be incorporated into the operation and maintenance manuals, and software documentation. There shall be at least 1 scheduled update near the end of the first year's warranty period, at which time the Contractor shall install and validate the latest

released version of the Contractor's software.

PART 2 PRODUCTS

2.1 MATERIALS REQUIREMENTS

NOTE: Some sensors have special or optional features that may be required for this project. Refer to Technical Manual 5-853-4 for guidance on applicability. Add descriptions of special or optional features to this specification if they are required.

2.1.1 Materials and Equipment

Units of the same type of equipment shall be products of a single manufacturer. All material and equipment shall be new and currently in production. Each major component of equipment shall have the manufacturer's model and serial number in a conspicuous place. System equipment shall conform to UL 294 and UL 1076.

2.1.2 Field Enclosures

NOTE: Show on the drawings which specific type of enclosure is needed. Show metallic enclosures for very high security areas or when a higher degree of tamper protection is desirable.

2.1.2.1 Interior Sensor

Sensors to be used in an interior environment shall be housed in an enclosure that provides protection against dust, falling dirt, and dripping noncorrosive liquids.

2.1.2.2 Exterior Sensor

Sensors to be used in an exterior environment shall be housed in an enclosure that provides protection against windblown dust, rain and splashing water, and hose directed water. Sensors shall be undamaged by the formation of ice on the enclosure.

2.1.2.3 Interior Electronics

System electronics to be used in an interior environment shall be housed in enclosures which meet the requirements of NEMA 250 Type 12.

2.1.2.4 Exterior Electronics

System electronics to be used in an exterior environment shall be housed in enclosures which meet the requirements of NEMA 250 Type 4X.

2.1.2.5 Corrosion Resistant

System electronics to be used in a corrosive environment as defined in NEMA 250 shall be housed in metallic enclosures which meet the requirements of

NEMA 250 Type 4X.

2.1.2.6 Hazardous Environment Equipment

System electronics to be used in a hazardous environment shall be housed in a enclosures which meet the requirements of paragraph Hazardous Environment.

2.1.3 Nameplates

Laminated plastic nameplates shall be provided for local processors. Each nameplate shall identify the local processor and its location within the system. Laminated plastic shall be 3 mm 1/8 inch thick, white with black center core. Nameplates shall be a minimum of 25 x 75 mm, 1 x 3 inches, with minimum 6 mm 1/4 inch high engraved block lettering. Nameplates shall be attached to the inside of the enclosure housing the local processor. Other major components of the system shall have the manufacturer's name, address, type or style, model or serial number, and catalog number on a corrosion resistant plate secured to the item of equipment. Nameplates will not be required for devices smaller than 25 x 75 mm. 1 x 3 inches.

2.1.4 Fungus Treatment

NOTE: Fungus treatment should only be used on equipment to be installed in climates that are known to have problems with fungus growth. Examples are extremely tropical climates or humid, poorly ventilated areas. If these conditions do not exist, delete the fungus treatment requirement.

System components located in fungus growth inductive environments shall be completely treated for fungus resistance. Treating materials containing a mercury bearing fungicide shall not be used. Treating materials shall not increase the flammability of the material or surface being treated. Treating materials shall cause no skin irritation or other injury to personnel handling it during fabrication, transportation, operation, or maintenance of the equipment, or during use of the finished items when used for the purpose intended.

2.1.5 Tamper Provisions

2.1.5.1 Tamper Switches

Enclosures, cabinets, housings, boxes, and fittings having hinged doors or removable covers and which contain circuits or connections of the system and its power supplies, shall be provided with cover operated, corrosion-resistant tamper switches, arranged to initiate an alarm signal when the door or cover is moved. The enclosure and the tamper switch shall function together and shall not allow direct line of sight to any internal components before the switch activates. Tamper switches shall be inaccessible until the switch is activated; have mounting hardware concealed so that the location of the switch cannot be observed from the exterior of the enclosure; be connected to circuits which are under electrical supervision at all times, irrespective of the protection mode in which the circuit is operating; shall be spring-loaded and held in the closed position by the door or cover; and shall be wired so that they break the circuit when the door or cover is disturbed.

a. Nonsensor Enclosures: Tamper switches on nonsensor enclosures which must be opened to make routine maintenance adjustments to the system and to service the power supplies shall be push/pull-set, automatic reset type.

b. Sensor Enclosures: Tamper switches on sensor enclosures which must be opened to make routine maintenance adjustments to the sensor shall be provided.

2.1.5.2 Enclosure Covers

Covers of pull and junction boxes provided to facilitate initial installation of the system need not be provided with tamper switches if they contain no splices or connections, but shall be protected by tack welding or brazing the covers in place or by tamper resistant security fasteners. Labels shall be affixed to such boxes indicating they contain no connections.

2.1.6 Locks and Key-Lock Switches

NOTE: Either round key or conventional key type locks are acceptable for use in the system. Selection should be based on hardware availability at the time of design and the requirements for matching locks currently in use at the site. If the locks do not have to be matched to locks in use, and the designer has no preference, all brackets may be removed.

2.1.6.1 Locks

Locks shall be provided on system enclosures for maintenance purposes. Locks shall be UL listed, [round-key type with 3 dual, 1 mushroom, 3 plain pin tumblers] [or] [conventional key type lock having a combination of 5 cylinder pin and 5-point 3 position side bar]. Keys shall be stamped "U.S. GOVT. DO NOT DUP." The locks shall be arranged so that the key can only be withdrawn when in the locked position. Maintenance locks shall be keyed alike and only 2 keys shall be furnished for all of these locks. These keys shall be controlled in accordance with the key control plan as specified in paragraph Key Control Plan.

2.1.6.2 Key-Lock-Operated Switches

Key-lock-operated switches required to be installed on system components shall be UL listed, [round-key type, with 3 dual, 1 mushroom, and 3 plain pin tumblers] [or] [conventional key type lock having a combination of 5 cylinder pin and 5-point 3 position side bar]. Keys shall be stamped "U.S. GOVT. DO NOT DUP." Key-lock-operated switches shall be 2 position, with the key removable in either position. All key-lock-operated switches shall be keyed differently and only 2 keys shall be furnished for each key-lock-operated-switch. These keys shall be controlled in accordance with the key control plan as specified in paragraph Key Control Plan.

2.1.6.3 Construction Locks

If the Contractor requires locks during installation and construction, a set of temporary locks shall be used. The final set of locks installed and

delivered to the Government shall not include any of the temporary locks.

2.1.7 System Components

System components shall be designed for continuous operation. Electronic components shall be solid state type, mounted on printed circuit boards conforming to UL 796. Printed circuit board connectors shall be plug-in, quick-disconnect type. Power dissipating components shall incorporate safety margins of not less than 25 percent with respect to dissipation ratings, maximum voltages, and current carrying capacity. Control relays and similar switching devices shall be solid state type or sealed electro-mechanical.

2.1.7.1 Modularity

Equipment shall be designed for increase of system capability by installation of modular components. System components shall be designed to facilitate maintenance through replacement of modular subassemblies and parts.

2.1.7.2 Maintainability

Components shall be designed to be maintained using commercially available tools and equipment. Components shall be arranged and assembled so they are accessible to maintenance personnel. There shall be no degradation in tamper protection, structural integrity, EMI/RFI attenuation, or line supervision after maintenance when it is performed in accordance with manufacturer's instructions. The system shall be configured and installed to yield a mean time to repair (MTTR) of not more than 8 hours. Repair time is the clock time from when maintenance personnel gain entrance to the system and begin work, until the system is fully functional.

2.1.7.3 Interchangeability

The system shall be constructed with off-the-shelf components which are physically, electrically and functionally interchangeable with equivalent components as complete items. Replacement of equivalent components shall not require modification of either the new component or of other components with which the replacement items are used. Custom designed or one-of-a-kind items shall not be used. Interchangeable components or modules shall not require trial and error matching in order to meet integrated system requirements, system accuracy, or restore complete system functionality.

2.1.7.4 Product Safety

System components shall conform to applicable rules and requirements of NFPA 70 and UL 294. System components shall be equipped with instruction plates including warnings and cautions describing physical safety, and special or important procedures to be followed in operating and servicing system equipment.

2.1.8 Controls and Designations

Controls and designations shall be as specified in NEMA ICS 1.

2.1.9 Special Test Equipment

The Contractor shall provide all special test equipment, special hardware,

software, tools, and programming or initialization equipment needed to start or maintain any part of the system and its components. Special test equipment is defined as any test equipment not normally used in an electronics maintenance facility.

2.1.10 Alarm Output

The alarm output of each sensor shall be a single pole double throw (SPDT) contact rated for a minimum of 0.25 A at 24 Volts dc.

2.2 CENTRAL STATION HARDWARE

The central station computer shall be a standard unmodified digital computer of modular design. The CPU word size shall be 64 bits or larger. The operating speed of the processor shall be at least 150 MHZ.

2.2.1 Memory

The computer shall contain at least 32 megabytes of usable installed memory, expandable to a minimum of 256 megabytes without additional chassis or power supplies.

2.2.2 Power Supply

The power supply shall have a minimum capacity of 250 Watts.

2.2.3 Real Time Clock (RTC)

A RTC shall be provided. Accuracy shall be within plus or minus 1 minute per month. The RTC shall maintain time in a 24-hour format including seconds, minutes, hours, date, and month and shall be resettable by software. The clock shall continue to function for a period of 1 year without power.

2.2.4 Serial Ports

a. Two EIA ANSI/EIA/TIA-232-F serial ports shall be provided for general use.

b. Adjustable data transmission rates from 9600 to 57.6 Kbps shall be selectable under program control.

c. Sixteen additional EIA ANSI/EIA/TIA-232-F serial ports shall be provided as part of a communications coprocessor. The coprocessor word size shall be 32 bytes or larger and the operating speed of the coprocessor shall be at least 66 MHZ. Communications with the field equipment shall be managed by this device. Multiplexed serial ports shall be expandable to 48 ports with 8 character transmit and receive buffers to each port. Total buffer size shall be a minimum of 1 megabyte.

2.2.5 Parallel Port

An enhanced parallel port shall be provided.

2.2.6 Color Monitor

The monitor shall be no less than 430 mm, 17 inches, with a minimum resolution of 1280 by 1024 pixels, noninterlaced, and a maximum dot pitch of 0.28 millimeters. The video card shall support at least 256 colors at a

resolution of 1280 by 1024 at a minimum refresh rate of 70 Hz.

2.2.7 Keyboard A101

A keyboard having a minimum 64 character, standard ASCII character, based on ANSI INCITS 154 shall be furnished.

2.2.8 Enhancement Hardware

Enhancement hardware such as special function keyboards, special function keys, touch screen devices, or mouse shall be provided for frequently used operator commands such as: Help, Alarm Acknowledge, Place Zone In Access, Place Zone In Secure, System Test, Print Reports, Change Operator, Security Lighting Controls, and Display Graphics.

2.2.9 Disk Storage

A hard disk with controller having a maximum average access time of 10 milliseconds shall be provided. The hard disk shall provide a minimum of 2.0 gigabytes of formatted storage. Additionally, a PCMCIA slot with a removable 500 megabyte hard drive shall be provided.

2.2.10 Floppy Disk Drives

A high density floppy disk drive and controller in 90 mm 3-1/2 inch size shall be provided.

2.2.11 Magnetic Tape System

A 4 mm cartridge magnetic tape system shall be provided. The system capacity shall be 8.0 gigabytes minimum per tape. Each tape shall be computer grade, in a rigid cartridge with spring-loaded cover and write-protect.

2.2.12 Modem

A modem shall be provided and operate at 28,800 bps, full duplex on circuits using asynchronous communications. Modem shall have error detection, auto answer/autodial, and call-in-progress detection. The modem shall meet the requirements of ITU V.34, ITU V.42 for error correction and ITU V.42 for data compression standards, and shall be suitable for operating on unconditioned voice grade telephone lines in conformance with 47 CFR 68.

2.2.13 Audible Alarm

The manufacturer's standard audible alarm shall be provided.

2.2.14 Mouse

A mouse with a minimum resolution of 400 dots per inch shall be provided.

2.2.15 CD-ROM Drive

A CD-ROM drive having a nominal storage capacity of 650 megabytes shall be provided. The CD-ROM drive shall have the following minimum characteristics:

- a. Data Transfer Rate: 1.2 Mbps.

- b. Average Access Time: 150 milliseconds.
- c. Cache memory: 256 Kbytes.
- d. Data throughput: 1 Mbyte/second, minimum.

2.2.16 Dot Matrix Alarm Printer

A dot matrix alarm printer shall be provided and interconnected to the central station equipment. The dot matrix alarm printer shall have a minimum 96 character, standard ASCII character set, based on ANSI INCITS 154 and with graphics capability. The printer shall be able to print in both red and black without ribbon change. The printers shall have adjustable sprockets for paper width up to 11 inches, print at least 80 columns per line and have a minimum speed of 200 characters per second. Character spacing shall be selectable at 10, 12 or 17 characters per inch. The printers shall utilize sprocket-fed fan fold paper. The units shall have programmable control of top-of-form. Twenty-five thousand sheets of printer paper and 12 ribbons shall be provided after successful completion of the endurance test.

2.2.17 Report Printer

A report printer shall be provided and interconnected to the central station equipment. The printer shall be a laser printer with printer resolution of at least 600 dots per inch. The printer shall have at least 2 megabytes of RAM. Printing speed shall be at least 8 pages per minute with a 100 sheet paper cassette and with automatic feed. Two thousand sheets of paper and 5 toner cartridges shall be furnished after successful completion of the endurance test.

2.2.18 Controllers

Controllers required for operation of specified peripherals, serial, and parallel ports shall be provided.

2.2.19 Redundant Central Computer

**NOTE: Redundant processors and associated hardware
and software should be used only when required by
governing regulations or when a single point failure
would be unacceptable.**

An identical redundant central computer shall be provided. It shall be interconnected in a hot standby, peer configuration. Each central computer shall maintain its own copies of system software, application software and data files. System transactions and other activity that alter system data files shall cause near real-time updates to both sets of system files. In the event of a central computer failure, the other central computer shall assume control immediately and automatically.

2.2.20 Central Station Equipment Enclosures

The Contractor shall provide color coordinated consoles and equipment cabinets. Equipment cabinets shall have front and back plexiglass doors, thermostatic controlled bottom-mounted fan, and metal fitted and louvered

tops. One locking cabinet approximately 1.8 m 6 feet high, 1 meter 3 feet wide, 0.5 to 1 meter 18 to 36 inches deep with 3 adjustable shelves, and 4 storage racks for storage of disks, tapes, printouts, printer paper, ribbons, manuals, and other documentation shall be provided.

2.2.21 Uninterruptible Power Supply (UPS)

A self contained UPS, suitable for installation and operation at the central station, shall be provided. The UPS shall be sized to provide a minimum of 6 hours of operation of the central station equipment. Equipment connected to the UPS shall not be affected by a power outage of a duration less than the rated capacity of the UPS. UPS shall be complete with necessary power supplies, transformers, batteries, and accessories and shall include visual indication of normal power operation, UPS operation, abnormal operation and visual and audible indication of low battery power. The UPS shall be as specified in Section 16265A UNINTERRUPTIBLE POWER SUPPLY (UPS) SYSTEM ABOVE 15 kVa CAPACITY. The UPS condition shall be monitored by the ESS and displayed at the Central Station.

2.2.22 Fixed Map Display

**NOTE: A map display should be used only if required
by regulation or user requirement.**

A fixed map display shall be provided showing a layout of the protected facilities. Zones corresponding to those monitored by the system shall be highlighted on the display. Status of each zone shall be displayed using LED's as required within each designated zone. An LED test switch shall be provided on the map display.

2.2.23 Enrollment Center Equipment

**NOTE: The designer will calculate if 50 percent is
adequate for future use. If it is not, the designer
will specify the correct percentage.**

Enrollment stations shall be provided and located as shown to enroll personnel into, and disenroll personnel from the system database. The enrollment equipment shall only be accessible to authorized entry control enrollment personnel. The Contractor shall provide enough credential cards for all personnel to be enrolled at the site plus an extra [50] [_____] percent for future use. The enrollment equipment shall include subsystem configuration controls and electronic diagnostic aids for subsystem setup and troubleshooting with the central station. A printer shall be provided for the enrollment station which meets the requirements of paragraph Report Printer.

2.2.23.1 Enrollment Center Accessories

A steel desk-type console, a swivel chair on casters and equipment racks shall be provided. The console shall be as specified in EIA ANSI/EIA-310-D and as shown. Equipment racks shall be as specified in EIA ANSI/EIA-310-D and as shown. All equipment, with the exception of the printers, shall be rack mounted in the console and equipment racks or as shown. The console and equipment racks and cabinets shall be color coordinated. A locking

cabinet approximately 1.8 m 6 feet high, 900 mm 3 feet wide, and 600 mm 2 feet deep with 3 adjustable shelves, and 2 storage racks for storage of disks, tapes, printouts, printer paper, ribbons, manuals, and other documentation shall be provided.

2.2.24 Secondary Alarm Annunciation Site

NOTE: Show secondary alarm annunciation console on the drawings. Eliminate this paragraph if the system does not have secondary alarm annunciation console.

Secondary alarm annunciation console shall be located as shown. Hardware and software needed for the secondary alarm annunciation console shall be provided. [The secondary alarm annunciation console shall allow the operator to duplicate all functions of the main operator interface, and shall show system status changes.] [The secondary alarm annunciation console shall display alarms or system status changes only.]

2.3 CENTRAL STATION SOFTWARE

Software shall support all specified functions. The central station shall be online at all times and shall perform required functions as specified. Software shall be resident at the central station and/or the local processor as required to perform specified functions.

2.3.1 System Software

System software shall perform the following functions:

- a. Support multiuser operation with multiple tasks for each user.
- b. Support operation and management of peripheral devices.
- c. Provide file management functions for disk I/O, including creation and deletion of files, copying files, a directory of all files including size and location of each sequential and random ordered record.
- d. Provide printer spooling.

2.3.2 Real Time Clock Synchronization

The system shall synchronize each real time clock within 1 second and at least once per day automatically, without operator intervention and without requiring system shutdown.

2.3.3 Database Definition Process

Software shall be provided to define and modify each point in the database using operator commands. The definition shall include all parameters and constraints associated with each sensor, commandable output, zone, facility interface device, terminal device, etc. Each database item shall be callable for display or printing, including EPROM, ROM and RAM resident data. The database shall be defined and entered into the ESS by the Contractor based upon input from the Government.

2.3.4 Software Tamper

The ESS shall annunciate a tamper alarm when unauthorized changes to the system database files are attempted. Three consecutive unsuccessful attempts to log onto the system shall generate a software tamper alarm. A software tamper alarm shall also be generated when an operator or other individual makes 3 consecutive unsuccessful attempts to invoke central processor functions beyond their authorization level. The ESS shall maintain a transcript file of the last 5000 commands entered at each central station to serve as an audit trail. The system shall not allow write access to the system transcript files by any person, regardless of their authorization level. The system shall only allow acknowledgment of software tamper alarms and read access to the system transcript files by operators and managers with the highest password authorization level available in the system.

2.3.5 Peer Computer Control Software

**NOTE: Redundant processors and associated hardware
and software should be used only when required by
governing regulations or when a single point failure
would be unacceptable.**

The peer computer control software shall detect a failure of a central computer, and shall cause the other central computer to assume control of all system functions without interruption of operation. Drivers shall be provided in both central computers to support this mode of operation.

2.3.6 Application Software

The application software shall provide the interface between the alarm annunciation and entry control local processors; monitor all sensors and DTS links; operate displays; report alarms; generate reports; and assist in training system operators.

2.3.6.1 Operator Commands

The operator's commands shall provide the means for entry of monitoring and control commands, and for retrieval of system information. Processing of operator commands shall commence within 1 second of entry, with some form of acknowledgment provided at that time. The operator's commands shall perform tasks including:

- a. Request help with the system operation.
- b. Acknowledge alarms.
- c. Place zone in access.
- d. Place zone in secure.
- e. Test the system.
- f. Generate and format reports.
- g. Print reports.

- h. Change operator.
- i. Control security lighting.
- j. Request any graphic displays implemented in the system. Graphic displays shall be completed within 20 seconds from time of operator command.
- k. Entry control functions.

2.3.6.2 Command Input

Operator's commands shall be full English language words and acronyms selected to allow operators to use the system without extensive training or data processing backgrounds. The system shall prompt the operator in English word, phrase, or acronym. Commands shall be available in an abbreviated mode, in addition to the full English language (words and acronyms) commands, allowing an experienced operator to disregard portions, or all, of the prompt-response requirements.

2.3.6.3 Command Input Errors

The system shall supervise operator inputs to ensure they are correct for proper execution. Operator input assistance shall be provided whenever a command cannot be executed because of operator input errors. The system shall explain to the operator, in English words and phrases, why the command cannot be executed. Error responses requiring an operator to look up a code in a manual or other document will not be accepted. Conditions for which operator error assist messages shall be generated include:

- a. The command used is incorrect or incomplete.
- b. The operator is restricted from using that command.
- c. The command addresses a point which is disabled or out of service.
- d. The command addresses a point which does not exist.
- e. The command would violate constraints.

2.3.6.4 Enhancements

The system shall implement the following enhancements by use of special function keys, touch screen, or mouse, in addition to all other command inputs specified:

- a. Help: Used to produce a display for all commands available to the operator. The help command, followed by a specific command shall produce a short explanation of the purpose, use, and system reaction to that command.
- b. Acknowledge Alarms: Used to acknowledge that the alarm message has been observed by the operator.
- c. Place Zone in Access: Used to remotely disable intrusion alarm circuits emanating from a specific zone. The system shall be structured so that tamper circuits cannot be disabled by the console operator.
- d. Place Zone in Secure: Used to remotely activate intrusion alarm circuits emanating from a specific zone.

e. System Test: Allows the operator to initiate a system wide operational test.

f. Zone Test: Allows the operator to initiate an operational test for a specific zone.

g. Print Reports: Allows the operator to initiate printing of reports.

h. Change Operator: Used for changing operators.

i. Security Lighting Controls: Allows the operator to remotely turn on/off security lights.

j. Display Graphics: Used to display any graphic displays implemented in the system.

2.3.6.5 System Access Control

The system shall provide a means to define system operator capability and functions through multiple, password protected operator levels. At least 3 operator levels shall be provided. System operators and managers with appropriate password clearances shall be able to change operator levels for all operators. Three successive attempts by an operator to execute functions beyond their defined level during a 24-hour period shall initiate a software tamper alarm. A minimum of 32 passwords shall be usable with the system software. The system shall display the operator's name or initials in the console's first field. The system shall print the operator's name or initials, action, date, and time on the system printer at log-on and log-off. The password shall not be displayed or printed. Each password shall be definable and assignable for the following:

a. Commands usable.

b. Access to system software.

c. Access to application software.

d. Individual zones which are to be accessed.

e. Access to database.

2.3.6.6 Alarm Monitoring Software

This program shall monitor all sensors, local processors and DTS circuits and notify the operator of an alarm condition. Alarms shall be printed in red on the alarm printer and displayed on the console's text and graphics map monitors. Higher priority alarms shall be displayed first; and within alarm priorities, the oldest unacknowledged alarm shall be displayed first.

Operator acknowledgment of one alarm shall not be considered as acknowledgment of any other alarm nor shall it inhibit reporting of subsequent alarms. Alarm data to be displayed shall include type of alarm, location of alarm, and secondary alarm messages. Alarm data to be printed shall include: type of alarm, location of alarm, date and time (to nearest second) of occurrence, and operator response. A unique message field with a width of 60 characters shall be provided for each alarm. Assignment of messages to a zone or sensor shall be an operator editable function. Secondary messages shall be assignable by the operator for printing to

provide further information and shall be editable by the operator. The system shall provide for 25 secondary messages with a field of 4 lines of 60 characters each. The most recent 1000 alarms shall be stored and shall be recallable by the operator using the report generator.

2.3.6.7 Monitor Display Software

Monitor display software shall provide for text and graphics map displays that include zone status integrated into the display. Different colors shall be used for the various components and real time data. Colors shall be uniform on all displays. The following color coding shall be followed.

- a. FLASHING RED to alert an operator that a zone has gone into an alarm or that primary power has failed.
- b. RED to alert an operator that a zone is in alarm and that the alarm has been acknowledged.
- c. YELLOW to advise an operator that a zone is in access.
- d. GREEN to indicate that a zone is secure or that power is on.

2.3.6.8 Map Displays/Graphics Linked to Alarms

The System shall relate map displays or other graphics to alarms. Whenever one of the predefined alarms is annunciated on a system control terminal, the map display or graphic related to the alarm shall be automatically displayed. The definition of which maps or graphics shall be displayed with each alarm shall be selectable by system operators through simple menu choices as part of the system initial configuration.

2.3.6.9 User Defined Prompts/Messages Linked to Alarms

The System shall provide a means to relate operator defined prompts and other messages to predefined alarms. Whenever one of the predefined alarms is annunciated on a system control terminal, the prompts or messages related to the alarm shall be automatically displayed.

2.3.6.10 System Test Software

This software shall enable the operator to initiate a test of the system. This test can be of the entire system or of a particular portion of the system at the operator's option. The results of each test shall be stored for future display or print out in report form.

2.3.6.11 Report Generator

Software shall be provided with commands to generate reports for displaying, printing, and storing on disk and tape. Reports shall be stored by type, date, and time and shall be printed on the report printer. Reports shall be spooled, allowing the printing of one report to be complete before the printing of another report commences. The dynamic operation of the system shall not be interrupted to generate a report. The report generation mode, either periodic, automatic or on request, shall be operator selectable. The report shall contain the time and date when the report was printed, and the name of operator generating the report. The exact format of each report type shall be operator configurable.

- a. Periodic Automatic Report Modes: The system shall allow for

specifying, modifying, or inhibiting the report to be generated, the time the initial report is to be generated, the time interval between reports, end of period, and the output peripheral.

b. Request Report Mode: The system shall allow the operator to request at any time an immediate printout of any report.

c. Alarm Report: The alarm report shall include all alarms recorded by the system over an operator selectable time. The report shall include such information as: the type of alarm (intrusion, tamper, etc.); the type of sensor; the location; the time; and the action taken.

d. System Test Report: This report documents the operational status of all system components following a system test.

e. Access/Secure Report: This report documents all zones placed in access, the time placed in access, and the time placed in secure mode.

f. Entry Control Reports: The system shall generate hard copy reports of identifier, terminal, and guard tour tracking reports, and versions with defined parameters of the manufacturer's standard management and activity reports.

2.3.6.12 Simulation (Training) Software

This program shall enable operators to practice system operation including alarm acknowledgment, alarm assessment, response force deployment, and response force communications. The system shall continue normal operation during training exercises and shall terminate exercises when an alarm signal is received at the console.

2.3.6.13 Entry Control Enrollment Software

The enrollment station shall provide database management functions for the system, and shall allow an operator to change and modify the data entered in the system as needed. The enrollment station shall not have any alarm response or acknowledgment functions. Multiple, password protected access levels shall be provided at the enrollment station. Database management and modification functions shall require a higher operator access level than personnel enrollment functions. The program shall provide a means for disabling the enrollment station when it is unattended to prevent unauthorized use. The program shall provide a method to enter personnel identifying information into the entry control database files through enrollment stations. In the case of personnel identity verification subsystems, this data shall include biometric data. The program shall allow entry of this data into the system database files through the use of simple menu selections and data fields. The data field names shall be customized to suit user and site needs. All personnel identity verification subsystems selected for use with the system shall fully support the enrollment function and shall be compatible with the entry control database files.

2.4 FIELD PROCESSING HARDWARE

2.4.1 Alarm Annunciation Local Processor

The alarm annunciation local processor shall respond to interrogations from the field device network, recognize and store alarm status inputs until they are transmitted to the central station and change outputs based on

commands received from the central station. The local processor shall also automatically restore communication within 10 seconds after an interruption with the field device network and provide dc line supervision on each of its alarm inputs.

a. Inputs. Local processor inputs shall monitor dry contacts for changes of state that reflect alarm conditions. The local processor shall have at least 8 alarm inputs which allow wiring as normally open or normally closed contacts for alarm conditions. It shall also provide line supervision for each input by monitoring each input for abnormal open, grounded, or shorted conditions using dc current change measurements. The local processor shall report line supervision alarms to the central station. Alarms shall be reported for any condition that remains off normal at an input for longer than 500 milliseconds. Each alarm condition shall be transmitted to the central computer during the next interrogation cycle.

b. Outputs. Local processor outputs shall reflect the state of commands issued by the central station. The outputs shall be a form C contact and shall include normally open and normally closed contacts. The local processor shall have at least 4 command outputs.

2.4.1.1 Processor Power Supply

Local processor and sensors shall be powered from an uninterruptible power source. The uninterruptible power source shall provide 6 hours of battery back-up power in the event of primary power failure and shall automatically fully recharge the batteries within 12 hours after primary power is restored. There will be no equipment malfunctions or perturbations or loss of data during the switch from primary to battery power and vice versa. Batteries shall be sealed, non-outgassing type. The power supply shall be equipped with an indicator for ac input power and an indicator for dc output power. Loss of primary power shall be reported to the central station as an alarm.

2.4.1.2 Auxiliary Equipment Power

A GFI service outlet shall be furnished inside the local processor's enclosure.

2.4.2 Entry Control Local Processor

The entry control local processor shall respond to interrogations from the field device network, recognize and store alarm status inputs until they are transmitted to the central station and change outputs based on commands received from the central station. The local processor shall also automatically restore communication within 10 seconds after an interruption with the field device network and provide dc line supervision on each of its alarm inputs. The entry control local processor shall provide local entry control functions including communicating with field devices such as card readers, keypads, biometric personal identity verification devices, door strikes, magnetic latches, gate and door operators and exit pushbuttons. The processor shall also accept data from entry control field devices as well as database downloads and updates from the central station that include enrollment and privilege information. The processor shall also send indications of success or failure of attempts to use entry control field devices and make comparisons of presented information with stored identification information. The processor shall grant or deny entry by sending control signals to portal control devices and mask intrusion

alarm annunciation from sensors stimulated by authorized entries. The entry control local processor shall use inputs from entry control devices to change modes between access and secure. The local processor shall maintain a date-time and location stamped record of each transaction and transmit transaction records to the central station. The processor shall operate as a stand-alone portal controller using the downloaded data base during periods of communication loss between the local processor and the field device network. The processor shall store up to 1000 transactions during periods of communication loss between the local processor and the field device network for subsequent upload to the central station upon restoration of communication. The local processor shall provide power for field devices and portal control devices.

a. Inputs. Local processor inputs shall monitor dry contacts for changes of state that reflect alarm conditions. The local processor shall have at least 8 alarm inputs which allow wiring as normally open or normally closed contacts for alarm conditions. It shall also provide line supervision for each input by monitoring each input for abnormal open, grounded, or shorted conditions using dc current change measurements. The local processor shall report line supervision alarms to the central station. Alarms shall be reported for any condition that remains off normal at an input for longer than 500 milliseconds. Each alarm condition shall be transmitted to the central station during the next interrogation cycle. The entry control local processor shall include the necessary software drivers to communicate with entry control field devices. Information generated by the entry control field devices shall be accepted by the local processor and automatically processed to determine valid identification of the individual present at the portal. Upon authentication of the credentials or information presented, the local processor shall automatically check privileges of the identified individual, allowing only those actions granted as privileges. Privileges shall include, but not be limited to, time of day control, day of week control, group control, and visitor escort control. The local processor shall maintain a date-time and location stamped record of each transaction. A transaction is defined as any successful or unsuccessful attempt to gain access through a controlled portal by the presentation of credentials or other identifying information.

b. Outputs. Local processor outputs shall reflect the state of commands issued by the central station. The outputs shall be a form C contact and shall include normally open and normally closed contacts. The local processor shall have at least 4 commandable outputs. The entry control local processor shall also provide control outputs to portal control devices.

c. Degraded Mode of Operation. The entry control local processor shall provide a degraded mode of operation for periods when communication between the local processor and the field device network is lost. While in this degraded mode, the local processor shall continue to control entry by accepting identifying information, making authentication decisions, checking privileges, and controlling portal control devices. Transactions shall be stored for subsequent transmission to the central station when communication is restored.

2.4.2.1 Processor Power Supply

Local processor and sensors shall be powered from an uninterruptible power source. The uninterruptible power source shall provide 6 hours of battery back-up power in the event of primary power failure and shall automatically

fully recharge the batteries within 12 hours after primary power is restored. There shall be no equipment malfunctions or perturbations or loss of data during the switch from primary to battery power and vice versa. Batteries shall be sealed, non-outgassing type. The power supply shall be equipped with an indicator for ac input power and an indicator for dc output power.

2.4.2.2 Auxiliary Equipment Power

A GFI service outlet shall be furnished inside the local processor's enclosure.

2.5 FIELD PROCESSING SOFTWARE

All Field processing software described in this specification shall be furnished as part of the complete system.

2.5.1 Operating System

Each local processor shall contain an operating system that controls and schedules that local processor's activities in real time. The local processor shall maintain a point database in its memory that includes all parameters, constraints, and the latest value or status of all points connected to that local processor. The execution of local processor application programs shall utilize the data in memory resident files. The operating system shall include a real time clock function that maintains the seconds, minutes, hours, date and month, including day of the week. Each local processor real time clock shall be automatically synchronized with the central station at least once per day to plus or minus 10 seconds. The time synchronization shall be accomplished automatically, without operator action and without requiring system shutdown.

2.5.1.1 Startup

The local processor shall have startup software that causes automatic commencement of operation without human intervention, including startup of all connected Input/Output functions. A local processor restart program based on detection of power failure at the local processor shall be included in the local processor software. The startup software shall initiate operation of self-test diagnostic routines. Upon failure of the local processor, if the database and application software are no longer resident, the local processor shall not restart and systems shall remain in the failure mode indicated until the necessary repairs are made. If the database and application programs are resident, the local processor shall immediately resume operation.

2.5.1.2 Operating Mode

Each local processor shall control and monitor inputs and outputs as specified, independent of communications with the central station. Alarms, status changes and other data shall be transmitted to the central station when communications circuits are operable. If communications are not available, each local processor shall function in a stand-alone mode and operational data, including the status and alarm data normally transmitted to the central station shall be stored for later transmission to the central station. Storage for the latest 1024 events shall be provided at each local processor. Each local processor shall accept software downloaded from the central station.

2.5.1.3 Failure Mode

Upon failure for any reason, each local processor shall perform an orderly shutdown and force all local processor outputs to a predetermined (failure mode) state, consistent with the failure modes shown and the associated control device.

2.5.2 Functions

The Contractor shall provide software necessary to accomplish the following functions, as appropriate, fully implemented and operational, within each local processor.

- a. Monitoring of inputs.
- b. Control of outputs.
- c. Reporting of alarms automatically to the central station.
- d. Reporting of sensor and output status to central station upon request.
- e. Maintenance of real time, automatically updated by the central station at least once a day.
- f. Communication with the central station.
- g. Execution of local processor resident programs.
- h. Diagnostics.
- i. Download and upload data to and from the central station.

2.6 INTERIOR SENSORS AND CONTROL DEVICES

NOTE: Show sensor patterns and installation details on drawings. Add requirement for additional site specific conditions such as furniture/equipment layout within protected areas, hazard location area, type of hazard, class, and group. Remote test capability should be used only when required by governing regulations or when sensors are installed in hard to reach areas. Within the U.S., the FCC regulates the operating frequencies of all microwave sensors. Other countries have their own frequencies. The designer must determine what frequency is allowed at the project site.

2.6.1 Balanced Magnetic Switch (BMS)

The BMS shall detect a 6 mm 1/4 inch of separating relative movement between the magnet and the switch housing. Upon detecting such movement, the BMS shall transmit an alarm signal to the alarm annunciation system.

2.6.1.1 BMS Subassemblies

The BMS shall consist of a switch assembly and an actuating magnet

assembly. The switch mechanism shall be of the balanced magnetic type. Each switch shall be provided with an overcurrent protective device, rated to limit current to 80 percent of the switch capacity. Switches shall be rated for a minimum lifetime of 1,000,000 operations. The magnet assembly shall house the actuating magnet.

2.6.1.2 Housing

The housings of surface mounted switches and magnets shall be made of nonferrous metal and shall be weatherproof. The housings of recess mounted switches and magnets shall be made of nonferrous metal or plastic.

2.6.1.3 Remote Test

A remote test capability shall be provided. The remote test shall be initiated when commanded by the alarm annunciation system. The remote test shall activate the sensor's switch mechanism causing an alarm signal to be transmitted to the alarm annunciation system. The remote test shall simulate the movement of the actuating magnet relative to the switch subassembly.

2.6.2 Glass Break Sensor, Piezoelectric

The glass break sensor shall detect high frequency vibrations generated by the breaking of glass while ignoring all other mechanical vibrations. An alarm signal shall be transmitted to the alarm annunciation system upon detecting such frequencies.

2.6.2.1 Sensor Element, Piezoelectric

The sensor element shall consist of piezoelectric crystals. The sensor element housing shall be designed to be mounted directly to the glass surface being protected. Only the adhesive recommended by the manufacturer of the sensor shall be used to mount detectors to glass. The detection pattern of a sensor element shall be circular with at least a 1.5 meter 5 foot radius on a continuous pane of glass. A factory installed hookup cable of not less than 1.8 meters 6 feet shall be included with each sensor. The sensor element shall not exceed 2600 square mm. 4 square inches. The sensor element shall be equipped with a light emitting diode (LED) activation indicator. The activation indicator shall light when the sensor responds to the high frequencies associated with breaking glass. The LED shall be held on until it is turned off manually at the sensor signal processor or by command from the alarm annunciation system.

2.6.2.2 Sensor Signal Processor, Piezoelectric

The sensor signal processor shall process the signals from the sensor element and provide the alarm signal to the alarm annunciation system. The sensitivity of the sensor shall be adjustable by controls within the sensor signal processor. The controls shall not be accessible when the sensor signal processor housing is in place. The sensor signal processor may be integral with the sensor or may be a separate assembly.

2.6.2.3 Glass Break Simulator, Piezoelectric

The Contractor shall provide a device that can induce frequencies into the protected pane of glass that will simulate breaking glass to the sensor element without causing damage to the pane of glass.

2.6.3 Glass Break Sensor, Acoustic

The glass break sensor shall detect high frequency vibrations generated by the breaking of glass while ignoring all other mechanical vibrations. An alarm signal shall be transmitted upon detecting such frequencies to the alarm annunciation system.

2.6.3.1 Sensor Element, Acoustic

The sensor element shall be a microprocessor based digital device. The sensor shall detect breakage of plate, laminated, tempered, and wired glass while rejecting common causes of nuisance alarms. The detection pattern of the sensor element shall be a range of 6 m 20 feet minimum. The sensor element shall be equipped with a light emitting diode (LED) activation indicator. The activation indicator shall light when the sensor responds to the high frequencies associated with breaking glass. The LED shall be held on until it is turned off manually at the sensor signal processor or by command from the alarm annunciation system.

2.6.3.2 Sensor Signal Processor, Acoustic

The sensor signal processor shall process the signals from the sensor element and provide the alarm signal to the alarm annunciation system. The sensitivity of the sensor shall be adjustable by controls within the sensor signal processor. The controls shall not be accessible when the sensor signal processor housing is in place. The sensor signal processor may be integral with the sensor or may be a separate assembly.

2.6.3.3 Glass Break Simulator, Acoustic

The contractor shall provide a device that can simulate breaking glass to the sensor. The device shall be rated for use with the specific sensor selected. The simulator shall not cause damage to the pane of glass.

2.6.4 Duress Alarm Switches

**NOTE: The designer will show type and location of
duress alarm switches.**

Duress alarm switches shall provide the means for an individual to covertly notify the alarm annunciation system that a duress situation exists.

2.6.4.1 Footrail

Footrail duress alarms shall be designed to be foot activated and floor mounted. No visible or audible alarm or noise shall emanate from the switch when activated. The switch housing shall shroud the activating lever to prevent accidental activation. Switches shall be rated for a minimum lifetime of 50,000 operations.

2.6.4.2 Push-button

Latching push-button duress alarm switches shall be designed to be activated by depressing a push-button located on the duress switch housing. No visible or audible alarm or noise shall emanate from the switch. The switch housing shall shroud the activating button to prevent accidental activation. Switches shall be rated for a minimum lifetime of 50,000

operations.

2.6.4.3 Wireless

Wireless duress alarm switches shall consist of portable alarm transmitters and permanently installed receivers. The transmitter shall be activated by depressing a push-button located on the housing. An alarm signal shall be transmitted to one or more receivers located within a protected zone. The receivers shall, in-turn, transmit an alarm signal to the alarm annunciation system. No visible or audible alarm or noise shall emanate from the transmitter or receiver when activated. The transmitter housing shall shroud the activating button to prevent accidental activation. The transmitter shall be designed to be unobtrusive and still be activated in a covert manner. Switches shall be rated for a minimum lifetime of 50,000 operations. The transmitters shall have a range of 30 meters. 100 feet.

2.6.5 Security Screen

Security screens shall detect an intruder when the sensor wire is disconnected, cut, or broken. An alarm signal shall be transmitted to the alarm annunciation system. The sensor shall be constructed from 26 gauge insulated hard-drawn copper wire installed in a grid pattern on a wooden frame or as shown. The sensor grid wires connection to the alarm annunciation system shall be housed within a junction box as shown. A tamper switch shall be provided to detect attempts to remove the screen and to detect attempts to tamper with connections and end of line resistors.

2.6.6 Vibration Sensor

**NOTE: The area protected by a single sensor can be
increased by installing a steel strap grid.**

The vibration sensor shall detect attempts to penetrate a structural barrier. The vibration sensor shall detect the high frequency vibrations generated by the use of such tools as oxyacetylene torches; oxygen lances; high speed drills and saws; and explosives, to penetrate a structure while ignoring all other mechanical vibrations. An alarm signal shall be transmitted to the alarm annunciation system when 1 or more of these incidents occur. The sensor shall consist of a sensor signal processor and piezoelectric crystal sensor elements that are designed to be rigidly mounted to the structure being protected. The sensor signal processor may be integral with the sensor element or may be a separate assembly. The sensor signal processor shall process the signals from the sensor elements and provide the alarm signal to the alarm annunciation system. The sensitivity of the sensor shall be adjustable by controls within the sensor signal processor. The controls shall not be accessible when the sensor signal processor housing is in place. The detection pattern of a sensor element shall be circular with at least a 1.8 meter 6 foot radius on the protected structure. A factory installed hookup cable of not less than 1.8 meters 6 feet shall be included with each sensor. The mounting area of the vibration sensor shall not exceed 5200 square mm. 8 square inches.

2.6.7 Ultrasonic Motion Sensor

The ultrasonic motion sensor shall detect Doppler shifts in an ultrasonic signal. An alarm signal shall be transmitted to the alarm annunciation system upon detecting such Doppler shifts. The sensor shall detect a

standard intruder moving within the sensor's detection pattern at a speed of 0.09 to 2.3 m/s. 0.3 to 7.5 feet per second. The ultrasonic signal shall be in the 25 to 33 KHz range. The sensor's coverage pattern shall be as shown. The sensitivity of the sensor shall be adjustable by controls within the sensor. The controls shall not be accessible when the sensor housing is in place. The sensor shall be adjustable to obtain the coverage shown.

2.6.7.1 Test Indicator, Ultrasonic System

The ultrasonic motion sensor shall be equipped with an LED walk test indicator. The walk test indicator shall not be visible during normal operations. When visible, the walk test indicator shall light when the sensor detects an intruder. The sensor shall either be equipped with a manual control, located within the sensor's housing, to enable/disable the test indicator or the test indicator shall be located within the sensor housing so that it can only be seen when the housing is open or removed.

2.6.7.2 Remote Test, Ultrasonic System

A remote test capability shall be provided. The remote test hardware may be integral to the sensor or a separate piece of equipment. The remote test shall be initiated when commanded by the alarm annunciation system. The remote test shall excite the sensing element and associated electronics causing an alarm signal to be transmitted to the alarm annunciation system. The sensor stimulation generated by the remote test hardware shall simulate a standard intruder moving within the sensor's detection pattern.

2.6.8 Microwave Motion Sensor

The microwave motion sensor shall detect changes in a microwave signal. Upon detecting a specific change, the sensor shall transmit an alarm signal to the alarm annunciation system. The sensor shall detect a standard intruder moving within the sensor's detection pattern at a speed of 0.09 to 2.3 m/s. 0.3 to 7.5 feet per second. The sensor shall comply with 47 CFR 15, Subpart F. The sensor's coverage pattern shall be as shown. The sensitivity of the sensor shall be adjustable by controls within the sensor housing. The controls shall not be accessible when the sensor housing is in place. The sensor shall be adjustable to obtain the coverage shown.

2.6.8.1 Test Indicator, Microwave System

The microwave motion sensor shall be equipped with an LED walk test indicator. The walk test indicator shall not be visible during normal operations. When visible, the walk test indicator shall light when the sensor detects an intruder. The sensor shall either be equipped with a manual control, located within the sensor's housing, to enable/disable the test indicator or the test indicator shall be located within the sensor housing so that it can only be seen when the housing is open or removed.

2.6.8.2 Remote Test, Microwave System

A remote test capability shall be provided. The remote test hardware may be integral to the sensor or a separate piece of equipment. The remote test shall be initiated when commanded by the alarm annunciation system. The remote test shall excite the sensing element and associated electronics causing an alarm signal to be transmitted to the alarm annunciation system. The sensor stimulation generated by the remote test hardware shall simulate a standard intruder moving within the sensor's detection pattern.

2.6.9 Passive Infrared Motion Sensor

The passive infrared motion sensor shall detect changes in the ambient level of infrared emissions caused by the movement of a standard intruder within the sensor's field of view. Upon detecting such changes, the sensor shall transmit an alarm signal to the alarm annunciation system. The sensor shall detect a change in temperature of no more than 1.1 degrees C, 2.5 degrees F, and shall detect a standard intruder traveling within the sensor's detection pattern at a speed of 0.09 to 2.3 m/s 0.3 to 7.5 feet per second across 2 adjacent segments of the field of view. Emissions monitored by the sensor shall be in the 8 to 14 micron range. The sensor shall be adjustable to obtain the coverage pattern shown. The sensor shall be equipped with a temperature compensation circuit.

2.6.9.1 Test Indicator, Passive Infrared

The passive infrared motion sensor shall be equipped with an LED walk test indicator. The walk test indicator shall not be visible during normal operations. When visible, the walk test indicator shall light when the sensor detects an intruder. The sensor shall either be equipped with a manual control, located within the sensor's housing, to enable/disable the test indicator or the test indicator shall be located within the sensor housing so that it can only be seen when the housing is open or removed.

2.6.9.2 Remote Test, Passive Infrared

A remote test capability shall be provided. The remote test hardware may be integral to the sensor or a separate piece of equipment. The remote test shall be initiated when commanded by the alarm annunciation system. The remote test shall excite the sensing element and associated electronics causing an alarm signal to be transmitted to the alarm annunciation system. The sensor stimulation generated by the remote test hardware shall simulate a standard intruder moving within the sensor's detection pattern.

2.6.10 Microwave-Passive Infrared Dual Detection Motion Sensor

The dual detection motion sensor shall be a single unit combining a detector which detects changes in a microwave signal and a detector which detects changes in the ambient level of infrared emissions caused by the movement of a standard intruder within the detection pattern. The detection pattern shall be capable of covering a 6 x 9 meter 20 x 30 foot room. Upon intruder detection by either detector, a time window of more than 3 seconds but less than 8 seconds shall be opened. If the other detector detects an intruder during this window, the sensor shall transmit an alarm signal to the alarm annunciation system. The passive infrared detector shall detect a change in temperature of no more than 1.1 degrees C, 2 degrees F, and shall detect a standard intruder traveling within the detection pattern at a speed of 0.09 to 2.3 m/s 0.3 to 7.5 feet per second across 2 adjacent segments of the field of view. Emissions monitored by the sensor shall be in the range of 8 to 14 microns. The microwave detector shall detect a standard intruder moving within the detection pattern at a speed of 0.09 to 2.3 m/s. 0.3 to 7.5 feet per second. The microwave detector shall comply with 47 CFR 15, Subpart F. Controls shall not be accessible when the sensor housing is in place. The sensor shall be configured to produce an alarm when both detectors sense an intruder.

2.6.10.1 Test Indicator

The sensor shall be equipped with an LED walk test indicator for both the passive infrared detector and the microwave detector. The walk test indicators shall not be visible during normal operations. When visible, the walk test indicators shall light when the sensor detects an intruder. The sensor shall either be equipped with a manual control, located within the sensor's housing, to enable/disable the test indicators or the test indicators shall be located within the sensor housing so that they can only be seen when the housing is open or removed.

2.6.10.2 Remote Test

A remote test capability shall be provided. The remote test hardware may be integral to the sensor or a separate piece of equipment. The remote test shall be initiated when commanded by the alarm annunciation system. The remote test shall excite each sensing element and associated electronics causing an alarm signal to be transmitted to the alarm annunciation system. The sensor stimulation generated by the remote test hardware shall simulate a standard intruder moving within the sensor's detection pattern.

2.6.11 Photo-Electric Sensor (Interior)

The photo-electric sensor shall detect an interruption of the light beam that links the transmitter and receiver caused by a standard intruder walking at a speed of less than 2.3 meters 7.5 feet per second through the beam. Upon detecting such an interruption, the sensor shall transmit an alarm signal to the alarm annunciation system. The sensor shall use a pulsed infrared light source. Multiple sensors shall be able to operate within the same zone without interfering with each other. The coverage pattern shall be as shown.

2.6.11.1 Test Indicator, Photo-Electric

The sensor shall be equipped with an LED walk test indicator. The walk test indicator shall not be visible during normal operations. When visible, the walk test indicator shall light when the sensor detects an intruder. The sensor shall either be equipped with a manual control, located within the sensor's housing, to enable/disable the test indicator or the test indicator shall be located within the sensor housing so that it can only be seen when the housing is open or removed.

2.6.11.2 Remote Test, Photo-Electric

A remote test capability shall be provided. The remote test hardware may be integral to the sensor or a separate piece of equipment. The remote test shall be initiated when commanded by the alarm annunciation system. The remote test shall excite each sensing element and associated electronics causing an alarm signal to be transmitted to the alarm annunciation system. The sensor stimulation generated by the remote test hardware shall simulate a standard intruder moving within the sensor's detection pattern.

2.6.12 Capacitance Proximity Sensor

The capacitance sensor shall detect the change in capacitance of at least 20 picofarads between an insulated asset and ground. The sensor shall detect a standard intruder approaching or touching the protected asset.

Upon detecting such a change, the sensor shall transmit an alarm signal to the alarm annunciation system. The sensor shall be able to protect multiple assets. The sensitivity of the sensor shall be adjustable by controls within the sensor. The controls shall not be accessible when the sensor housing is in place. Insulator blocks shall be provided for each asset to be protected by the sensor.

2.6.12.1 Test Indicator, Capacitance

The sensor shall be equipped with an LED walk test indicator. The walk test indicator shall not be visible during normal operations. When visible, the walk test indicator shall light when the sensor detects an intruder. The sensor shall either be equipped with a manual control, located within the sensor's housing, to enable/disable the test indicator or the test indicator shall be located within the sensor housing so that it can only be seen when the housing is open or removed.

2.6.12.2 Remote Test, Capacitance

A remote test capability shall be provided. The remote test hardware may be integral to the sensor or a separate piece of equipment. The remote test shall be initiated when commanded by the alarm annunciation system. The remote test shall excite the sensing element and associated electronics causing an alarm signal to be transmitted to the alarm annunciation system. The sensor stimulation generated by the remote test hardware shall simulate a standard intruder moving within the sensor's detection pattern.

2.6.13 Video Motion Sensor (Interior)

**NOTE: Video motion sensor systems require inclusion
of Section 16751 CLOSED CIRCUIT TELEVISION SYSTEMS
in the project.**

The video motion sensor shall detect changes in the video signal within a user defined detection zone. The system shall detect changes in the video signal corresponding to a standard intruder moving within the defined detection zone and wearing clothing with a reflectivity that differs from that of the background scene by a factor of 2. All other changes in the video signal shall be rejected by the sensor. Upon detecting such changes, the sensor shall transmit an alarm signal to the alarm annunciation system.

The sensor shall include the controls and method needed by the operator to define and adjust the sensor detection zone within the video picture. The number of detection zones, the size of the detection zones, and the sensitivity of the detection zones shall be user definable. The sensor shall be a modular system that allows for expansion or modification of the number of inputs. The video inputs shall accept composite video as defined in EIA 170. Sensor controls shall be mounted on the front panel or in an adjacent rack panel. The sensor shall not require external sync for operation. One alarm output shall be provided for each video input. The number of video inputs and alarm outputs shall be as shown. All components, cables, power supplies, and other items needed for a complete video motion sensor shall be provided. Sensor equipment shall be rack mounted in a standard 19 inch rack as described in EIA ANSI/EIA-310-D. The rack shall include hardware required to mount the sensor components.

2.6.14 Access/Secure Switches

NOTE: The designer should refer to TM 5-853-4 for proper application of this piece of hardware.

An access/secure switch shall be used to place a protected zone in the ACCESS or SECURE mode. The switch shall consist of a double pull key-operated switch housed in a NEMA 12 equivalent enclosure. The switch shall disable zone sensor alarm outputs, but shall not disable tamper alarms, duress alarms, and other 24 hr sensors, as shown.

2.7 EXTERIOR INTRUSION SENSORS

NOTE: Show sensor patterns and installation details on drawings. Add requirement for additional site specific conditions such as equipment layout within protected areas, hazard location area, type of hazard, class, and group. Remote test capability should be used only when required by governing regulations or when sensors are installed in hard to reach areas. Within the U.S., the FCC regulates the operating frequencies of all microwave sensors. Other countries have their own frequencies. The designer must determine what frequency is allowed at the project site.

2.7.1 Bistatic Microwave Sensor

The bistatic microwave sensor shall consist of a separate transmitter and receiver. The sensor shall detect changes in the received microwave signal caused by the movement of a standard intruder within the sensor's detection pattern. Upon detecting such changes, the sensor shall transmit an alarm signal to the alarm annunciation system. The sensor shall detect a standard intruder moving perpendicular through the sensor's detection pattern at a speed of 0.06 to 7.6 m/s. 0.2 to 25 feet per second. The sensor shall be equipped with circuitry that produces an alarm signal when the sensor's receiver is captured by another microwave transmitter. The sensor shall comply with 47 CFR 15, Subpart F. The sensor's coverage pattern shall be as shown. Multiple sensors shall be able to operate in adjacent zones without interfering with each other. The sensitivity of the sensor shall be adjustable by controls within the sensor. The controls shall not be accessible when the sensor housing is in place. The sensor shall be adjustable to obtain the coverage pattern shown.

2.7.1.1 Test Indicator, Bistatic

The sensor shall be equipped with an LED walk test indicator. The walk test indicator shall not be visible during normal operations. When visible, the walk test indicator shall light when the sensor detects an intruder. The sensor shall either be equipped with a manual control, located within the sensor's housing, to enable/disable the test indicator or the test indicator shall be located within the sensor housing so that it can only be seen when the housing is open or removed.

2.7.1.2 Remote Test, Bistatic

A remote test capability shall be provided. The remote test hardware may be integral to the sensor or a separate piece of equipment. The remote test shall be initiated when commanded by the alarm annunciation system. The remote test shall excite the sensing element and associated electronics causing an alarm signal to be transmitted to the alarm annunciation system. The sensor stimulation generated by the remote test hardware shall simulate a standard intruder moving within the sensor's detection pattern.

2.7.2 Monostatic Microwave Sensor

The monostatic microwave sensor shall consist of an integrated transceiver. The sensor shall detect changes in the received microwave signal caused by the movement of a standard intruder within the sensor's detection pattern. Upon detecting such changes, the sensor shall transmit an alarm signal to the alarm annunciation system. The sensor shall detect a standard intruder moving perpendicular through the sensor's detection pattern at a speed of 0.06 to 7.6 m/s. 0.2 to 25 feet per second. The sensor shall comply with 47 CFR 15, Subpart F. The sensor's coverage pattern shall be as shown. Multiple sensors shall be able to operate in adjacent zones without interfering with each other. The sensitivity of the sensor shall be adjustable by controls within the sensor. The controls shall not be accessible when the sensor housing is in place. The sensor shall be adjustable to obtain the coverage pattern shown.

2.7.2.1 Test Indicator, Monostatic

The sensor shall be equipped with an LED walk test indicator. The walk test indicator shall not be visible during normal operations. When visible, the walk test indicator shall light when the sensor detects an intruder. The sensor shall either be equipped with a manual control, located within the sensor's housing, to enable/disable the test indicator or the test indicator shall be located within the sensor housing so that it can only be seen when the housing is open or removed.

2.7.2.2 Remote Test, Monostatic

A remote test capability shall be provided. The remote test hardware may be integral to the sensor or a separate piece of equipment. The remote test shall be initiated when commanded by the alarm annunciation system. The remote test shall excite the sensing element and associated electronics causing an alarm signal to be transmitted to the alarm annunciation system. The sensor stimulation generated by the remote test hardware shall simulate a standard intruder moving within the sensor's detection pattern.

2.7.3 Strain Sensitive Cable Sensor

The strain sensitive cable sensor shall detect induced mechanical vibrations in the fence structure and fabric resulting from climbing, cutting, and lifting caused by a standard intruder, while rejecting other vibration frequencies. Upon detecting such frequencies, the sensor shall transmit an alarm signal to the alarm annunciation system. The sensor shall consist of coaxial transducer cable mounted to the fence structure including fabric and a sensor signal processor. The sensor element shall be coaxial transducer cable. The sensitivity of the transducer cable shall not vary more than 10 percent over the length of the cable. The exterior jacket of the cable shall be ultraviolet radiation resistant. Where required, the sensor manufacturer's nonsensitive lead-in cable, shall be

supplied as part of the sensor system. The transducer cable shall be supervised by the signal processor to protect against tampering. The sensitivity of the sensor shall be adjustable by controls within the sensor signal processor. The controls shall not be accessible when the sensor interface module's housing is in place. Ultraviolet radiation resistant carbon impregnated plastic tie wraps shall be provided for installation of the sensor cable to the fence. The sensor shall cover up to a 92 m 300 foot zone and as shown.

2.7.3.1 Test Indicator, Strain Sensitive

The sensor may be equipped with a test indicator if it is an integral function of the sensor signal processor.

2.7.3.2 Remote Test, Strain Sensitive

A remote test capability shall be provided. The remote test hardware may be integral to the sensor or a separate piece of equipment. The remote test shall be initiated when commanded by the alarm annunciation system. The remote test shall excite the sensing element and associated electronics causing an alarm signal to be transmitted to the alarm annunciation system. The sensor stimulation generated by the remote test hardware shall simulate a standard intruder moving within the sensor's detection pattern.

2.7.4 Passive Infrared Motion Sensor (Exterior)

The passive infrared motion sensor shall detect changes in the ambient level of infrared emissions caused by the movement of a standard intruder within the sensor's field of view. Upon detection of such changes, the sensor shall transmit an alarm signal to the alarm annunciation system. The sensor shall detect a change in temperature of no more than 1.1 degrees C 2 degrees F and shall detect a standard intruder traveling within the sensor's detection pattern at a speed of 0.2 to 15 m/s 0.6 to 50 feet per second across 2 adjacent segments of the field of view. The sensor shall have a detection range of at least 92 meters. 300 feet. Emissions monitored by the sensor shall be in the 8 to 14 micron range. The sensor shall be adjustable to obtain the coverage pattern shown. The sensor shall be equipped with a temperature compensation circuit.

2.7.4.1 Test Indicator, Passive Infrared Motion Sensor

The sensor shall be equipped with an LED walk test indicator. The walk test indicator shall not be visible during normal operations. When visible, the walk test indicator shall light when the sensor detects an intruder. The sensor shall either be equipped with a manual control, located within the sensor's housing, to enable/disable the test indicator or the test indicator shall be located within the sensor housing so that it can only be seen when the housing is open or removed.

2.7.5 Tension Wire Fence Sensor

The tension wire fence sensor shall detect displacement or changes in tension within the sensor wires resulting from climbing, cutting, lifting and stepping through by a standard intruder. Upon detecting such changes, the sensor shall transmit an alarm signal to the alarm annunciation system. The configuration shall be as shown. The tension wires shall be double strand barbed wire. The configuration shall be as shown. The sensor post shall house the switches or electronics used to monitor the tension wires. The space between tension wires shall not exceed 150 mm. 6 inches.

2.7.6 Capacitance Fence Sensor

The capacitance fence sensor shall detect changes in capacitance between the sense wires and ground as a standard intruder approaches or touches the sensor. Upon detecting such changes in capacitance, the sensor shall transmit an alarm signal to the alarm annunciation system. The sensor shall consist of sense wires and a sensor signal processor. The sense wires shall be made of stainless steel. The sense wires shall be mounted to the fence with insulated support brackets. Ancillary mounting hardware shall be stainless steel. The sensitivity of the sensor shall be adjustable by controls within the sensor signal processor. The controls shall not be accessible when the sensor signal processor's housing is in place.

2.7.7 Buried Ported Cable

The buried ported cable shall detect changes in the electromagnetic field between the leaky coax transmit and receive cables caused by the movement of a standard intruder within the sensor's detection pattern. Upon detecting such changes, the sensor shall transmit an alarm signal to the alarm annunciation system. The sensor shall detect a standard intruder moving through the sensor's detection pattern at a speed of 0.06 to 7.6 m/s. 0.2 to 25 feet per second. The transmit and receive cables shall be ported coaxial cables designed for direct burial. The sensor's detection pattern shall be as shown. The sensitivity of the sensor shall be adjustable by controls within the sensor signal processor. The controls shall not be accessible when the sensor signal processor's housing is in place.

2.7.7.1 Test Indicator, Buried Ported Cable

The sensor may be equipped with a test indicator if it is an integral function of the sensor signal processor.

2.7.7.2 Remote Test, Buried Ported Cable

A remote test capability shall be provided. The remote test hardware may be integral to the sensor or a separate piece of equipment. The remote test shall be initiated when commanded by the alarm annunciation system. The remote test shall excite the sensing element and associated electronics causing an alarm signal to be transmitted to the alarm annunciation system. The sensor stimulation generated by the remote test hardware shall simulate a standard intruder moving within the sensor's detection pattern.

2.7.8 Photo-Electric Sensor (Exterior)

The photo-electric sensor shall detect an interruption of the light beam that links the transmitter and receiver caused by a standard intruder moving at a speed of less than 2.92 m/s 7.5 feet per second through the beam. Upon detecting such an interruption, the sensor shall transmit an alarm signal to the alarm annunciation system. The sensor shall use a pulsed infrared light source. Multiple sensors shall be able to operate within the same zone without interfering with each other. The coverage pattern shall be as shown. The sensitivity of the sensor shall be adjustable by controls within the sensor signal processor. The controls shall not be accessible when the sensor signal processor's housing is in place.

2.7.8.1 Test Indicator, Photo-Electric Exterior

The sensor may be equipped with a test indicator if it is an integral function of the sensor signal processor.

2.7.8.2 Remote Test, Photo-Electric Exterior

The sensor may incorporate remote test if it is an integral function of the sensor. The sensor shall be equipped with an LED walk test indicator. The walk test indicator shall not be visible during normal operations. When visible, the walk test indicator shall light when the sensor detects an intruder. The sensor shall either be equipped with a manual control, located within the sensor's housing, to enable/disable the test indicator or the test indicator shall be located within the sensor housing so that it can only be seen when the housing is open or removed.

2.7.9 Video Motion Sensor (Exterior)

**NOTE: Video motion sensor systems require inclusion
of Section 16751 CLOSED CIRCUIT TELEVISION SYSTEMS
in the project.**

The video motion sensor shall detect changes in the video signal within a user defined detection zone. The system shall detect changes in the video signal corresponding to a standard intruder moving within the defined detection zone and wearing clothing with a reflectivity that differs from that of the background scene by a factor of 2. All other changes in the video signal shall be rejected by the sensor. Upon detecting such changes, the sensor shall transmit an alarm signal to the alarm annunciation system. The sensor shall include the controls and method needed by the operator to define and adjust the sensor detection zone within the video picture. The number of detection zones, the size of the detection zones, and the sensitivity of the detection zones shall be user definable. The sensor shall be a modular system that allows for expansion or modification of the number of inputs. The video inputs shall accept composite video as defined in EIA 170. Sensor controls shall be mounted on the front panel or in an adjacent rack panel. The sensor shall not require external sync for operation. One alarm output shall be provided for each video input. The number of video inputs and alarm outputs shall be as shown. Components, cables, power supplies, and other items needed for a complete video motion sensor shall be provided. Sensor equipment shall be rack mounted in a standard 19 inch rack as described in EIA ANSI/EIA-310-D. The rack shall include hardware required to mount the sensor components.

2.8 ENTRY CONTROL DEVICES

2.8.1 Card Readers and Credential Cards

Entry control card readers shall use unique coded data stored in or on a compatible credential card as an identifier. The card readers shall be [insertion] [swipe-through] [proximity] type, and shall incorporate built-in heaters or other cold weather equipment to extend the operating temperature range as needed for operation at the site. Communications protocol shall be compatible with the local processor. The Contractor shall furnish card readers to read [magnetic stripe] [Weigand wire effect] [active proximity detection] [passive proximity detection] entry cards, and the matching credential cards. The cards shall contain coded data arranged

as a unique identification code stored on or within the card, and of the type readable by the card readers. The Contractor shall include within the card's encoded data, a non-duplicated unique facility identification code common to all credential cards provided at the site. Enrollment equipment to support local encoding of badges including cryptographic and other internal security checks shall be supplied.

2.8.1.1 Magnetic Stripe

Magnetic stripe card readers shall read credential cards which meet the requirements of ISO 7810, ISO 7811-1, ISO 7811-2, ISO 7811-3, ISO 7811-4, and ISO 7811-5. Magnetic stripe credential cards shall use single layer 4000 ersted magnetic tape material. The magnetic tape material shall be coated with Teflon and affixed to the back of the credential card near the top. The number of bits per inch, number of tracks, and number of unique codes available for the magnetic tape shall be in accordance with ISO 7811-1, ISO 7811-2, ISO 7811-3, ISO 7811-4, and ISO 7811-5.

2.8.1.2 Weigand Wire Effect

Weigand card readers shall read credential cards which are encoded using Weigand effect ferromagnetic wires laminated into the credential card. The Weigand card reader shall create a magnetic field and output a coded representation of the unique pattern of magnetic flux changes produced by moving the credential card through the card reader. The output shall be a series of electrical signals and shall constitute a unique identification code number. Weigand credential cards shall use at least 24 binary digits to generate a unique credential card identification code.

2.8.1.3 Proximity

**NOTE: Specify the type of proximity card operation
desired, and coordinate the operation method with
the type of card specified.**

Proximity card readers shall use [active] [passive] proximity detection and shall not require contact with the proximity credential card for proper operation. [Active detection proximity card readers shall provide power to compatible credential cards through magnetic induction and receive and decode a unique identification code number transmitted from the credential card.] [Passive detection proximity card readers shall use a swept-frequency, radio frequency field generator to read the resonant frequencies of tuned circuits laminated into compatible credential cards. The resonant frequencies read shall constitute a unique identification code number.] The card reader shall read proximity cards in a range from 0 mm 0 inches to at least 150 mm 6 inches from the reader. The credential card design shall allow for a minimum of 32,000 unique identification codes per facility.

2.8.1.4 Card Reader Display

The card readers shall include an LED or other visual indicator display. The display shall indicate power on/off, and whether user passage requests have been accepted or rejected.

2.8.1.5 Card Reader Response Time

The card reader shall respond to passage requests by generating a signal to the local processor. The response time shall be 800 milliseconds or less, from the time the card reader finishes reading the credential card until a response signal is generated.

2.8.1.6 Card Reader Power

The card reader shall be powered from the source as shown and shall not dissipate more than 5 Watts.

2.8.1.7 Card Reader Mounting Method

Card readers shall be suitable for surface, semi-flush, pedestal, or weatherproof mounting as required.

2.8.1.8 Credential Card Modification

Entry control cards shall be able to be modified by lamination or direct print process during the enrollment process for use as a picture and identification badge as needed for the site without reduction of readability. The design of the credential cards shall allow for the addition of at least one slot or hole to accommodate the attachment of a clip for affixing the credential card to the type badge holder used at the site.

2.8.1.9 Card Size and Dimensional Stability

NOTE: Specify the standard card size of 54 x 85 mm
(2-1/8 x 3-3/8 in.) unless a different size card is
needed. If a non-standard size card is specified
the designer must make certain that the card size
specified will work with the photo badging system
and the card reader specified.

Credential cards shall be [54 x 85 mm (2-1/8 x 3-3/8 inches)] [_____] mm.
[2-1/8 x 3-3/8] [_____] inches. The credential card material shall be
dimensionally stable so that an undamaged card with deformations resulting
from normal use shall be readable by the card reader.

2.8.1.10 Card Materials and Physical Characteristics

The credential card shall be abrasion resistant, non-flammable, and present no toxic hazard to humans when used in accordance with manufacturer's instructions. The credential card shall be impervious to solar radiation and the effects of ultra-violet light.

2.8.1.11 Card Construction

NOTE: Specify whether additional security
enhancements are needed. Choose which security
enhancement is needed. Specify card lamination and
assembly equipment if needed at the site.

The credential card shall be of core and laminate or monolithic construction. Lettering, logos and other markings shall be hot stamped into the credential material or direct printed. [The credential card shall incorporate [holographic images] [phosphorous ink] as a security enhancement.] [The Contractor shall provide a means to allow onsite assembly and lamination of credential cards by Government personnel.]

2.8.1.12 Card Durability and Maintainability

The credential cards shall be designed and constructed to yield a useful lifetime of at least 5000 insertions or swipes or 5 years whichever results in a longer period of time. The credential card shall be able to be cleaned by wiping the credential card with a sponge or cloth wet with a soap and water solution.

2.8.2 Keypads

NOTE: The designer will specify the type of keypad needed for the site. The scrambled keypad should be specified for very high security needs. If a scrambled keypad is specified the designer will specify the reduced viewing angle feature. The designer will specify whether visual and audible prompts are needed.

Entry control keypads shall use a unique combination of alphanumeric and other symbols as an identifier. Keypads shall contain an integral alphanumeric/special symbols keyboard with symbols arranged in [ascending ASCII code ordinal sequence] [random scrambled order]. Communications protocol shall be compatible with the local processor.

2.8.2.1 Keypad Display

Keypads shall include an LED or other type of visual indicator display and provide [visual] [visual and audible] status indications and user prompts. The display shall indicate power on/off, and whether user passage requests have been accepted or rejected. The design of the keypad display or keypad enclosure shall limit the maximum horizontal and vertical viewing angles of the keypad. The maximum horizontal viewing angle shall be plus and minus 5 degrees or less off a vertical plane perpendicular to the plane of the face of the keypad display. The maximum vertical viewing angle shall be plus and minus 15 degrees or less off a horizontal plane perpendicular to the plane of the face of the keypad display.

2.8.2.2 Keypad Response Time

The keypad shall respond to passage requests by generating a signal to the local processor. The response time shall be 800 milliseconds or less from the time the last alphanumeric symbol is entered until a response signal is generated.

2.8.2.3 Keypad Power

The keypad shall be powered from the source as shown and shall not dissipate more than 150 Watts.

2.8.2.4 Keypad Mounting Method

Keypads shall be suitable for surface, semi-flush, pedestal, or weatherproof mounting as required.

2.8.2.5 Keypad Duress Codes

Keypads shall provide a means for users to indicate a duress situation by entering a special code.

2.8.3 Card Readers With Integral Keypad

2.8.3.1 Magnetic Stripe

The magnetic stripe card reader, as specified in paragraph Card Readers And Credential Cards and paragraph Magnetic Stripe, shall be equipped with integral keypads as specified in paragraph Keypads.

2.8.3.2 Proximity

The proximity card reader, as specified in paragraph Card Readers And Credential Cards and paragraph Proximity, shall be equipped with integral keypads as specified in paragraph Keypads.

2.8.4 Personal Identity Verification Equipment

Entry control personnel identity verification equipment shall use a unique personal characteristic or unique personal physiological measurement to establish the identity of authorized, enrolled personnel. Personnel identity verification equipment shall include a means to construct individual templates or profiles based upon measurements taken from the person to be enrolled. This template shall be stored as part of the System Reference Database Files. The stored template shall be used as a comparative base by the personnel identity verification equipment to generate appropriate signals to the associated local processors.

2.8.4.1 Eye Retina Scanner

NOTE: The designer will specify if audible status indication if required.

Eye retina scanners shall use unique human retinal characteristics to identify authorized, enrolled personnel. The design of this device shall incorporate positive measures to establish that the eye retina being scanned by the device belongs to a living human being. The efficiency and accuracy of the eye retina scanner shall not be adversely affected by wearing contact lenses. Retina scanners shall provide an eye alignment system which does not require eye contact with the retina scan equipment. Each eye template shall not require more than 512 eight bit bytes of storage media space. Retina scanners shall provide a means for manual initiation of the scan process under user control. The scanner shall provide a means to grant or deny user passage requests based upon scans of one eye. The light emitting source used for retina scans shall not use light levels exceeding 20 percent of the maximum safe level established in ACGIH 0100Doc. Eye scanners shall include an LED or other type of visual indicator display and provide [visual] [visual and audible] status indications and user prompts. The display shall indicate power on/off, and

whether user passage requests have been accepted or rejected.

a. Template Update and Acceptance Tolerance: Eye scanners shall not automatically update a user's template. Significant changes in an individual's eye shall require re-enrollment. The eye scanners shall provide an adjustable acceptance tolerance or template match criteria under system manager/operator control. The eye scanner shall determine when multiple attempts are needed to verify the eye being scanned, and shall automatically prompt the user for additional attempts up to a maximum of 3. Three failed attempts shall generate an entry control alarm.

b. Average Verification Time: The eye scanner shall respond to passage requests by generating signals to the local processor. The verification time shall be 1.5 seconds or less from the moment the eye scanner initiates the scan process until the eye scanner generates a response signal.

c. Modes: The eye scanner shall provide an enrollment mode, recognition mode, and code/credential verification mode. The enrollment mode shall create an eye template for new personnel and enter the template into the system database file created for that person. Template information shall be compatible with the system application software. When operating in recognition mode, the eye scanner shall allow passage when the eyescan data from the verification attempt matches an eye template stored in the database files. When operating in code/credential verification mode, the eye scanner shall allow passage when the eye scan data from the verification attempt matches the eye scan template associated with the identification code entered into a keypad or matches the eye scan template associated with credential card data read by a card reader.

d. Electrical: The eye scanner shall not dissipate more than 45 Watts from the voltage source shown.

e. Mounting Method: Eye scanners shall be suitable for surface, semi-flush, or pedestal mounting as required and shown.

f. Communications Protocol: The communications protocol between the eye scanner and its associated local processor shall be compatible.

2.8.4.2 Hand Geometry

**NOTE: The designer will specify if audible status
indication if required.**

Hand geometry devices shall use unique human hand measurements to identify authorized, enrolled personnel. The design of this device shall incorporate positive measures to establish that the hand being measured by the device belongs to a living human being. Hand geometry devices shall provide an alignment system which allows the user's hand to remain in full view of the user at all times. During the scan process the hand geometry device shall make 3 dimensional measurements of the size and shape of the user's hand. The hand geometry device shall automatically initiate the scan process once the user's hand is properly positioned by the alignment system. The hand geometry device shall be able to use either left or right hands for enrollment and verification. User hand geometry template shall not require more than 50 eight-bit bytes of storage media space. Hand geometry devices shall include an LED or other type of visual indicator

display and provide [visual] [visual and audible] status indications and user prompts. The display shall indicate power on/off, and whether user passage requests have been accepted or rejected.

a. Template Update and Acceptance Tolerances: Hand geometry devices shall not automatically update a user's profile. Significant changes in an individual's hand geometry shall require re-enrollment. The hand geometry devices shall provide an adjustable acceptance tolerance or template match criteria under system manager/operator control. The hand geometry device shall determine when multiple attempts are needed for hand geometry verification, and shall automatically prompt the user for additional attempts up to a maximum of 3. Three failed attempts shall generate an entry control alarm.

b. Average Verification Time: The hand geometry device shall respond to passage requests by generating signals to the local processor. The verification time shall be 1.5 seconds or less from the moment the hand geometry device initiates the scan process until the hand geometry device generates a response signal.

c. Modes: The hand geometry device shall provide an enrollment mode, recognition mode, and code/credential verification mode. The enrollment mode shall create a hand template for new personnel and enter the template into the entry control database file created for that person. Template information shall be compatible with the system application software. The operating mode shall be selectable by the system manager/operator from the central processor. When operating in recognition mode, the hand geometry device shall allow passage when the hand scan data from the verification attempt matches a hand geometry template stored in the database files. When operating in code/credential verification mode, the hand geometry device shall allow passage when the hand scan data from the verification attempt matches the hand geometry template associated with the identification code entered into a keypad; or matches the hand geometry template associated with credential card data read by a card reader.

d. Reports: The hand geometry device shall create and store template match scores for all transactions involving hand geometry scans. The template match scores shall be stored in the matching personnel data file in a file format compatible with the system application software, and shall be used for report generation.

e. Electrical: The hand geometry device shall not dissipate more than 45 Watts from the source shown.

f. Mounting Method: Hand geometry devices shall be suitable for surface, flush, or pedestal mounting as required.

g. Communications Protocol: The communications protocol between the hand geometry device and the local processor shall be compatible.

2.8.4.3 Fingerprint Analysis Scanner

NOTE: The designer will specify if audible status indication if required.

Fingerprint analysis scanners shall use a unique human fingerprint pattern to identify authorized, enrolled personnel. The design of this device

shall incorporate positive measures to establish that the hand or fingers being scanned by the device belong to a living human being. Fingerprint analysis scanners shall provide an alignment system which allows the enrollee's hand to remain in full view of the enrollee at all times. During the scan process, the fingerprint analysis scanner shall perform an optical or other type of scan of the enrollee's fingers. The fingerprint analysis scanner shall automatically initiate the scan process provided the enrollee's fingers are properly positioned. Each enrollee fingerprint template shall not require more than 1250 eight-bit bytes of storage media space. Fingerprint analysis scanners shall include an LED or other type of visual indicator display and provide [visual] [visual and audible] status indications and enrollee prompts. The display shall indicate power on/off, and whether enrollee passage requests have been accepted or rejected.

a. Template Update and Acceptance Tolerances: Fingerprint analysis scanners shall not automatically update an enrollee's profile. Significant changes in an individual's fingerprints shall require re-enrollment. The fingerprint analysis scanners shall provide an adjustable acceptance tolerance or template match criteria under system manager/operator control. The fingerprint analysis scanner shall determine when multiple attempts are needed for fingerprint verification, and shall automatically prompt the enrollee for additional attempts up to a maximum of 3. Three failed attempts shall generate an entry control alarm.

b. Average Verification Time: The fingerprint analysis scanner shall respond to passage requests by generating signals to the local processor. The verification time shall be 2.0 seconds or less from the moment the finger print analysis scanner initiates the scan process until the fingerprint analysis scanner generates a response signal.

c. Modes: The fingerprint analysis scanner shall provide an enrollment mode, recognition mode, and code/credential verification mode. The enrollment mode shall create a fingerprint template for new personnel and enter the template into the system database file created for that person. Template information shall be compatible with the system application software. The operating mode shall be selectable by the system manager/operator from the central station. When operating in recognition mode, the fingerprint analysis scanner shall allow passage when the fingerprint data from the verification attempt matches a fingerprint template stored in the database files. When operating in code/credential verification mode, the fingerprint analysis scanner shall allow passage when the fingerprint data from the verification attempt matches the fingerprint template associated with the identification code entered into a keypad or matches the fingerprint template associated with credential card data read by a card reader.

d. Electrical: The fingerprint analysis scanner shall not dissipate more than 45 Watts from the source shown.

e. Mounting Method: Fingerprint analysis scanners shall be suitable for surface, flush, or pedestal mounting as required.

f. Communications Protocol: The communications protocol between the fingerprint analysis scanner and its associated local processor shall be compatible.

2.8.4.4 Iris Scan Device

NOTE: The designer will specify if audible status indication if required.

The iris scan identification device shall use the unique patterns found in the iris of the human eye to identify authorized, enrolled personnel. The device shall use ambient light to capture an image of the iris of a person presenting themselves for identification. The resulting video image shall be compared against a stored template that was captured during the enrollment process. When the presented image is sufficiently similar to the stored image template, then the device shall authenticate the presenting individual as identified. The threshold of similarity shall be adjustable. The efficiency and accuracy of the device shall not be adversely affected by enrollees who wear contact lenses or eye glasses. The iris scan device shall provide a means for enrollees to align their eye for identification that does not require facial contact with the device. A manual push-button shall be provided to initiate the scan process when the enrollee has aligned their eye in front of the device. The device shall include adjustments to accommodate differences in enrollee height.

a. Display Type: Iris scanners shall include an LED or other type of visual indicator display and provide [visual] [visual and audible] status indications and enrollee prompts. The display shall indicate power on/off, and whether enrollee passage requests have been accepted or rejected.

b. Template Update and Acceptance Tolerances: Iris scanners shall not automatically update an enrollee's template. Significant changes in an individual's eye shall require re-enrollment. The iris scanner shall provide an adjustable acceptance tolerance or template match criteria under system manager/operator control. The iris scanner shall determine when multiple attempts are needed to verify the iris being scanned, and shall automatically prompt the enrollee for additional attempts up to a maximum of 3. Three failed attempts shall generate an entry control alarm.

c. Average Verification Time: The iris scanner shall respond to passage requests by generating signals to the local processor. The verification time shall be 1.5 seconds or less from the moment the eye scanner initiates the scan process until the eye scanner generates a response signal.

d. Modes: The iris scanner shall provide an enrollment mode, recognition mode, and code/credential verification mode. The enrollment mode shall create an iris template for new personnel and enter the template into the system database file created for that person. Template information shall be compatible with the system application software. When operating in recognition mode, the iris scanner shall allow passage when the iris scan data from the verification attempt matches an iris template stored in the database files. When operating in code/credential verification mode, the iris scanner shall allow passage when the iris scan data from the verification attempt matches the iris scan template associated with the identification code entered into a keypad or matches the iris scan template associated with credential card data read by a card reader.

e. Electrical: The eye scanner shall not dissipate more than 45 Watts from the voltage source shown.

f. Mounting Method: Eye scanners shall be suitable for surface, flush, or pedestal mounting as required and shown.

2.8.5 Portal Control Devices

2.8.5.1 Push-button Switches

The Contractor shall provide momentary contact, back lighted push buttons and stainless steel switch enclosures for each push button as shown. Switch enclosures shall be suitable for flush, or surface mounting as required. Push buttons shall be suitable for flush mount in the switch enclosures. The push button switches shall meet the requirements of NEMA 250 for the area in which they are to be installed. Where multiple push buttons are housed within a single switch enclosure they shall be stacked vertically with each push button switch labeled with 7 mm 1/4 inch high text and symbols as required. The push button switches shall be connected to the local processor associated with the portal to which they are applied and shall operate the appropriate electric strike, electric bolt or other facility release device. Switches shall have a minimum continuous current rating of 10 Amperes at 120 Vac or 5 Amperes at 240 Vac. The push button switches shall have double-break silver contacts that will make 720 VA at 60 amperes and break 720 VA at 10 amperes.

2.8.5.2 Panic Bar Emergency Exit With Alarm

Entry control portals shall include panic bar emergency exit hardware as shown. Panic bar emergency exit hardware shall provide local alarm annunciation and alarm communications to the portal's local processor. The panic bar shall include a conspicuous warning sign with 25 mm 1 inch high, red lettering notifying personnel that an alarm will be annunciated if the panic bar is operated. Operation of the panic bar hardware shall generate an intrusion alarm. The panic bar, except for local alarm annunciation and alarm communications, shall depend upon a mechanical connection only and shall not depend upon electric power for operation. The panic bar shall be compatible with mortise or rim mount door hardware and shall operate by retracting the bolt.

2.8.5.3 Electric Door Strikes/Bolts

NOTE: The designer will specify whether the electric strike or lock will fail open or secure. The designer should coordinate this with requirements of the site safety and fire personnel. Life safety will be designed in accordance with NFPA 101, Code for Safety to Life from Fire in Buildings and Structures.

NOTE: The designer will determine if signal switches are required for the site.

Electric door strikes/bolts shall be designed to [release automatically] [remain secure] in case of power failure. These facility interface devices shall use dc power to energize the solenoids. Electric strikes/bolts shall incorporate end of line resistors to facilitate line supervision by the system.

a. Solenoid: The actuating solenoid for the strikes/bolts furnished shall not dissipate more than 12 Watts and shall operate on 12 or 24 Volts dc. The inrush current shall not exceed 1 ampere and the holding current

shall not be greater than 500 milliamperes. The actuating solenoid shall move from the fully secure to fully open positions in not more than 500 milliseconds.

b. Signal Switches: The strikes/bolts shall include signal switches to indicate to the system when the bolt is not engaged or the strike mechanism is unlocked. The signal switches shall report a forced entry to the system.

c. Tamper Resistance: The electric strike/bolt mechanism shall be encased in hardened guard barriers to deter forced entry.

d. Size and Weight: Electric strikes/bolts shall be compatible with standard door frame preparations.

e. Mounting Method: The electric door strikes/bolts shall be suitable for use with single and double door with mortise or rim type hardware as shown, and shall be compatible with right or left hand mounting.

2.8.5.4 Electromagnetic Lock

NOTE: The designer will specify whether the electric strike or lock will fail open or secure. The designer should coordinate this with requirements of the site safety and fire personnel. Life safety will be designed in accordance with NFPA 101, Code for Safety to Life from Fire in Buildings and Structures.

Electromagnetic locks shall contain no moving parts and shall depend solely upon electromagnetism to secure a portal by generating at least 5.3 kN 1200 pounds of holding force. The electromagnetic lock shall release automatically in case of power failure and shall require manual reset to resume normal function. The lock shall interface with the local processors without external, internal or functional alteration of the local processor. The electromagnetic lock shall incorporate an end of line resistor to facilitate line supervision by the system.

a. Armature: The electromagnetic lock shall contain internal circuitry to eliminate residual magnetism and inductive kickback. The actuating armature shall operate on 12 or 24 Volts dc and shall not dissipate more than 12 Watts. The holding current shall be not greater than 500 milliamperes. The actuating armature shall take not more than 300 milliseconds to change the status of the lock from fully secure to fully open or fully open to fully secure.

b. Tamper Resistance: The electromagnetic lock mechanism shall be encased in hardened guard barriers to deter forced entry.

c. Mounting Method: The door electromagnetic lock shall be suitable for use with single and double door with mortise or rim type hardware as shown, and shall be compatible with right or left hand mounting.

2.8.5.5 Entry Booth

NOTE: The designer will choose either keypads or

cardreaders as needed.

Entry booths shall be constructed as an integral part of the physical structure of the boundary for the area or facility to which entry is being controlled. In case of power failure, the entry booth shall automatically lock the high security side door's electric strike or other facility interface release device and shall automatically open the low security side door's electric strike or other facility interface release device. Entry booths shall be designed and configured for direct connection to the central station and shall include a local processor. The entry booth local processor subsystem shall support paired card readers on a single entry booth for anti-passback functions.

a. Local Alarm Annunciation: The entry booth local processor subsystem shall provide local alarm annunciation for all system equipment located within the entry booth itself and its associated portals/zones and terminal devices. The entry booth local processor subsystem shall provide a means to enable and disable this feature from the central station under operator control.

b. Terminal and Facility Interface Device Support: The entry booth local processor subsystem shall support the full range of system terminal and facility interface devices as specified.

c. Response Times: The entry booth local processor subsystem shall respond to a central station interrogation within 100 milliseconds. The entry booth local processor shall respond to valid passage requests from its associated terminal devices by generating a signal to the appropriate electric strike or other type of facility interface within 100 milliseconds after verification.

d. Autonomous Local Control: In the event of a communication loss, the entry booth local processor subsystem shall automatically convert to autonomous local control and monitoring of its associated card readers, keypads, electric door strikes, and other terminal devices or facility interface devices and shall automatically revert to central control upon restoration of communications. Entry control transactions occurring during the communications outage shall be recorded and retained in local memory and reported to the central data base files upon restoration of communications. The entry booth shall begin the report to the central station's database within 10 seconds after communications have been restored.

e. Entry Booth Local Processor Subsystem Capacities: As a minimum, the entry booth local processor subsystem shall have sufficient capacity to control and monitor a combination of 6 electric door strikes, card readers, keypads, or other entry control terminal and facility interface devices. The entry booth local processor subsystem shall provide capacity to store a subset of the entry control reference file database sufficient to support the enrollees requiring entry through each booth, and including personal, entry authorization, and identifier data for each enrollee as needed to support passage requests. The local processor subsystem shall make identification decisions and control portals so that all entry control functions are done at the local panel. The entry booth local processor subsystem shall provide a local transaction history file with capacity to store at least 1,000 entry control transactions without losing any data.

f. Diagnostics: The entry booth local processor subsystem shall

incorporate built-in diagnostics implemented in software/firmware, hardware or both. Each time the entry booth local processor subsystem is started up or re-booted it shall automatically execute a series of built-in tests and report equipment malfunctions, configuration errors, and inaccuracies to the central station. The system shall annunciate a fail-safe alarm if the local processor fails the built-in diagnostics. Diagnostic aids shall be provided within the entry booth local processor subsystem to aid in system set-up, maintenance, and troubleshooting.

g. Memory Type and Size: The design of the memory into which enrollee entered data is stored shall ensure storage of entered data for a minimum of 1 year in the absence of power from sources external to the entry booth.

h. Tamper Protection: The local processor subsystem shall monitor all service entry panels for tamper. Tamper lines shall not be accessible except through tamper protected entry panels. Entry panels shall have key locks. The booth shall have the capability to be taken off-line for service.

i. Entry Booth Configuration: Entry booths shall be closed-in structures suitable for occupancy by 1 person and shall incorporate: a personnel passage area, equipment bay, a low security entry/exit door and a high security entry/exit door. Entry booths shall be configured with paired [card readers] [keypads], 1 each, on the high security entry/exit door and low security entry/exit door; a key release switch outside the low security door; a glass break type emergency release switch. Both doors to the entry booth shall be normally secured.

j. Entry Booth Operation: The entry booth shall be designed to allow passage requests to be initiated from only 1 door at a time. The person shall enter the booth by presenting valid credential card to the card reader or keypad identification code data to the keypad device. An unsuccessful attempt to enter the booth shall generate an entry denial alarm. The booth shall incorporate a personal identity verification device as specified, and the person shall be granted egress from the booth after successful personal identity verification. If the person fails the personal identity verification test, the entry booth shall confine the person and generate an entry control alarm. The local processor subsystem shall compare all data presented to the entry booth terminal devices with its local reference database file contents, and grant the person's passage request if all data is valid. If a tamper alarm is generated by any of the equipment associated with the subject entry booth while an person is inside, the person shall be confined. Operating the glass break type emergency release switch shall command the entry door electric strike or other type of facility interface release to the fully open position, or with a delay after the egress door has been confirmed secured. Once inside the entry booth and prior to initiation of the personal identity verification test, the person may exit through the door used for entry.

k. Display Type: Entry booths shall include an LED or other type of visual indicator display and provide visual status indications and person prompts. The display shall indicate power on/off, and whether enrollee passage requests have been accepted or rejected. There shall be 3 status lights outside each door. They shall indicate entry booth status by marking the green light as READY; the amber light as BUSY; and the red light as INOPERATIVE.

l. Lighting: Two 40 Watt fluorescent lights recessed above an

acrylic light diffuser, shall be located in the ceiling of the entry booth. A separate fluorescent lamp shall be located within the overhead lamp assembly to provide emergency lighting in case of a power failure.

m. Heating and Ventilation Equipment: Entry booths shall include built-in heating equipment to extend the useful operating temperature range as needed. Entrance air shall flow through the top of the personnel passage area, and then through the bottom of the equipment bay cabinet. A fine particulate filter shall be provided in the equipment bay cabinet.

n. Size: The outside dimensions of the entry booth shall not exceed 2.4 m long, by 1.3 m wide, by 2.4 m high 96 inches long, by 50 inches wide, by 94 inches high.

o. Entry Booth Wall and Frame Construction: The booth shall be a rigid structure. The strength of the walls shall be greater than or equal to 12 gauge steel with 25 mm 1 inch standing seams. All glass used shall be at least 8 mm 5/16 inch laminated, annealed glass. The glass shall meet UL 972 certification requirements. The entry booth shall meet flame spread rating 25 or less, fuel contribution of 50 or less, smoke development of 50 or less, in accordance with test method ASTM E 84. Entry booths shall be constructed to minimize the heating effects of solar radiation, by using the manufacturer's standard clear, tinted or bronzed glass. The booths shall have over-hanging roofs or other structural means to shade the windows.

p. Entry Booth Doors: Doors shall be at least 889 mm wide, by 2.0 m high 35 inches wide, by 79 inches high with glass panels at least 788 mm wide, by 1.9 m high 31 inches wide, by 74 inches high. Door hinges and closers shall be adjustable for vertical, horizontal, cant, and torque adjustment. The entry booth shall provide an inside push bar, and an outside mechanical pull handle. Aluminum parts shall be anodize finish.

q. Entry Booth Floor Construction: The entry booth shall have a rigid floor. The floor shall be covered by a rubber mat or indoor/outdoor carpeting. The rubber mat or carpet shall be at least 1.6 mm 1/16 inch thick and shall provide a continuous floor covering with no seams.

2.8.5.6 Booth Security and Operational Enhancements

NOTE: The designer will specify the equipment and features for the booth configuration and eliminate the subparagraphs not needed.

a. CCTV Camera: The CCTV camera shall be designed and configured for continuous operation and shall transmit video information to the central station as specified in Section 16751A CLOSED CIRCUIT TELEVISION SYSTEMS.

b. Weight Check Monitor: The entry booth shall incorporate a weight check monitor which continuously monitors the weight of the booth plus any occupant. The weight check monitor shall consist of synchronized, matched, electronic load cells located at the base of the entry booth and shall be connected to the local processor subsystem. The weight check monitor shall be accurate to within plus or minus 2.3 kg. 5 pounds. The entry booth shall be designed to compensate for side loading to prevent damage to the load cells by the passage of equipment through the booth. Individual weights for each user shall be included in the reference database files as

part of the enrollment process. The design of the entry booth shall provide a method to enter a custom, predefined tolerance on valid weights of authorized persons. Each person's weight profile shall be automatically updated based upon the last 3 uses of entry control booths. The entry booth shall generate an entry control alarm for any passage attempt for which the person's weight does not agree with system reference database file data and confine the person. The weight check monitor shall not increase the portal door threshold height by more than 6 mm. 1/4 inch.

c. Double Occupancy Floor Mat Sensor: Entry booths shall incorporate a floor mat sensor to detect attempts at double occupancy. The double occupancy floor mat sensor shall be connected to the local processor subsystem. Activation of the double occupancy floor mat sensor shall generate a system alarm and confine the enrollees. The double occupancy floor mat sensor shall monitor the entire occupant area covered by a rubber mat or indoor/outdoor carpet. The rubber mat or carpet shall be at least 1.6 mm 1/16 inch thick and shall provide a continuous floor covering with no seams.

d. Intercom: Each entry booth shall have 3 combination speaker/microphones to provide 2 way communications at each of the speaker/microphone locations. The speakers shall be at least 4 inches in diameter. Two of the speaker/microphones shall be located, one each, at the high and low security entry/exit doors, behind louvered panels, to provide communications for people outside the booth. The third speaker/microphone shall be located inside the booth behind a perforated metal screen above the personal identity verification device to provide communications for people inside the booth. Each of the speaker/microphones shall be connected to the operator console at the security center and to the voice prompt system as indicated.

e. Voice Prompts: The entry booths shall include a voice prompt system using human voice commands. Its purpose shall be to speed up the entry control process and improve throughput rate. This audible prompt system shall respond to the next sequential activity requirement as each employee accesses the booth. All commands shall be stored in electrically programmable read only memory chips located in the local processor subsystem. The voice prompts shall only be directed to the speaker/microphone nearest the employee. The voice prompts shall only be used if the employee does not perform the next step in the entry booth entry control process within a 5 second time window. The system shall allow enable/disable of voice prompts and adjustment of the time window under operator control from the central station.

2.8.5.7 Entry Booth Electrical Requirements

NOTE: The designer will specify whether the electric strike or lock will fail open or secure. The designer should coordinate this with requirements of the site safety and fire personnel. Life safety will be designed in accordance with NFPA 101, titled, Code for Safety to Life from Fire in Buildings and Structures.

The entry booth, including associated terminal and facility interface and other type of devices housed within the entry booth, shall not dissipate more than 1500 Watts at power source as shown. The booth shall have an

integral battery back-up system. The battery back-up system shall power the entry control devices and electric door strikes for at least 30 minutes. If ac power is not restored to the booth within 30 minutes, the doors to the booth shall be [secured] [opened], and the booth shall go into an inoperative status. Upon restoration of ac power, the booth shall upload all entry transactions from the local processor subsystem to the central station.

2.8.5.8 Vehicle Gate Opener

The vehicle gate shall include housing, mounting hardware, electrical wiring, and appurtenances as required. The vehicle gate openers shall be suitable for connection to, and monitoring and control by the system local processors. A hand crank for manual operation of the vehicle gate opener and a solenoid actuated brake to prevent gate coasting shall be provided. The vehicle gate opener shall provide an auto reverse time delay of at least 1 second and not more than 3 seconds to minimize shock loads on vehicle gate opener drive components. The vehicle gate opener shall include a contactor type motor starter which meets or exceeds NEMA size "0" specifications.

a. Input Power: The vehicle gate opener shall operate from the voltage source shown. The vehicle gate opener shall include manual reset type thermal and electrical overload devices.

b. Audible Warning: The vehicle gate opener shall have an audible warning system to signal personnel in the vicinity of the vehicle gate opener that an opening or closing is about to commence. The audible shall sound at least 2 seconds and no more than 5 seconds before movement begins.

c. Maximum Run Timer: The vehicle gate opener shall incorporate an internal maximum run timer which limits the motor run time. The maximum run time shall be operator adjustable for at least the maximum amount of time gate opening or closing takes during normal operation.

d. Adjustable Load Monitor for Obstruction Sensing: The vehicle gate opener shall have an operator adjustable load monitor that shall sense obstructions in the path of the gate and automatically reverse the vehicle gate opener drive motor.

e. Operator Override Controls: The vehicle gate opener shall interface to a 3 push-button control station located within an entry controlled area. The 3 push-button switches shall be labeled and function as open, close, and stop controls, and shall meet the requirements of paragraph Push-button Switches.

f. Limit Switches: The vehicle gate opener shall have adjustable limit switches and shall provide a means to securely lock the switches in place after adjustment. The range of gate travel shall be defined by the location of the limit switches.

g. Type of Gate: The vehicle gate openers provided shall be compatible with cantilever, roller, v-track, overhead, slide, and swing gates.

2.9 SURVEILLANCE AND DETECTION EQUIPMENT

2.9.1 Article Surveillance/X-Ray

**NOTE: Contact the Electronic Security Center for
the latest text information.**

The X-ray package search system shall be [automated] [manual] suitable for detection and identification of materials and material densities. The article surveillance/X-ray device shall be suitable for connection to the local processors and alarm monitoring and control by the local processors; and shall function as a sensor/detector subsystem. The article surveillance/X-ray device shall provide adjustable contrast and a surface area threshold setting. The article surveillance/X-ray device shall incorporate a long-term image storage system to document subsystem operations. The article surveillance/X-ray device shall have a minimum throughput rate of 600 packages per hour and shall be designed for continuous operation. The article surveillance/X-ray device shall meet the requirements of 21 CFR 1020, Section 1020.40.

2.9.1.1 Size and Weight

The article surveillance/X-ray device shall not exceed 3.1 m long, by 1.02 m wide, by 1.5 m high. 120 inches long, by 40 inches wide, by 60 inches high. The article surveillance/X-ray device shall not weigh more than 910 kg 2000 pounds.

2.9.1.2 Local Audible Alarms

The article surveillance/X-ray device shall provide local audible alarm annunciation and automatic threat alert based upon an adjustable contrast and a surface area threshold setting. Alarms generated by the article surveillance/X-ray device shall be immediately communicated to and annunciated at the central station.

2.9.1.3 Maximum Package Size

The article surveillance/X-ray device shall be able to inspect packages and other articles up to 380 mm tall, by 610 mm wide and 1.5 m long. 15 inches tall, by 24 inches wide, and 60 inches long.

2.9.1.4 X-Ray Tube

Output from the X-ray tube shall be able to penetrate steel up to 3.2 mm 1/8 inch thick.

2.9.1.5 Electrical

The article surveillance/X-ray device shall operate from the power source shown.

2.9.1.6 Safety

The article surveillance/X-ray device shall include dual lead-lined curtains at the entrance and exit to the conveyer system package scanning region. The radiation exposure to operator for each package inspection shall be not more than 0.2 milliroentgen. The article surveillance/X-ray

device shall not adversely affect magnetic storage media as it is passed through the device.

2.9.1.7 Display

The display system shall use a standard 525 line television monitor to present X-ray data to the article surveillance/X-ray device operator. The article surveillance/X-ray device shall be designed and configured to provide at least 64 gray scale shades or at least 64 distinct colors. The article surveillance/X-ray device shall also provide image enhancement, zoom, pan, split screen, and freeze-frame capabilities.

2.9.1.8 Conveyor

The article surveillance/X-ray device shall have a conveyor system with foot switch controls. The conveyor shall be reversible and suitable for intermittent operation with a minimum speed range of 0 to 0.18 m/s 0 to 35 feet per minute.

2.9.1.9 Material Identification and Resolution

The article surveillance/X-ray device shall be able to detect and identify the full range of ferrous and non-ferrous metals, plastics, plastic explosive compounds, drugs, and other contraband as required. The resolution of this device, including its display, shall be sufficient to identify a 30 AWG solid copper wire.

2.9.2 Metal Detector

The Contractor shall provide a walk through type metal detector. The metal detector shall be interfaced to the system's local processors and shall function as a sensor/detector subsystem. The metal detector shall be designed so that it may be incorporated into entry booths as required, and when incorporated as a subsystem of the entry booth shall be connected to the entry booth local processor subsystem. The metal detector shall be designed for continuous operation. The metal detector shall use an active pulsed or continuous wave induction type detection field. The design of the metal detector shall create a field detection pattern with no holes or gaps from top to bottom and across the passage area, and shall provide 100 percent Faraday shielding of the sensor coil. The metal detector shall incorporate measures to minimize false alarms from external sources. A synchronization module shall be provided to allow simultaneous operation of multiple metal detection subsystems, with no degradation of sensitivity or function, when separated by 1.5 meters 5 feet or more. The metal detector shall not adversely affect magnetic storage media.

2.9.2.1 Size and Weight

Freestanding metal detectors shall not exceed 1.0 m deep, by 1.3 m wide, by 2.3 m high. 40 inches deep, by 50 inches wide, by 90 inches high. Metal detectors to be used in entry control booths shall have dimensions as needed to fit inside the entry control booth. The metal detector shall weigh 160 kg 350 pounds or less.

2.9.2.2 Local Alarms

The metal detector shall provide local audible and visual alarm annunciation. Alarms generated by the metal detector shall be immediately communicated to and annunciated at the central station.

2.9.2.3 Material Identification and Sensitivity

The metal detector shall have a continuously adjustable sensitivity control which allows it to be set to detect 100 grams of ferrous or non-ferrous metal placed anywhere on or in an individual's body.

2.9.2.4 Traffic Counter

NOTE: If the metal detectors require a traffic counter, include this paragraph. If traffic counters are not required, eliminate the paragraph.

The metal detector shall include a built-in traffic counter with manual reset capability. The traffic counter shall be sensor actuated and shall automatically increment each time a person passes through the metal detector. The metal detector shall also provide visual prompts directing the individual to proceed through the metal detector at the proper time or to wait until the metal detector is reset and ready for another scan.

2.9.2.5 Electrical

The metal detector shall not dissipate more than 250 Watts. Neither the metal detector's sensitivity nor its functional capability shall be adversely affected by power line voltage variations of plus or minus 10 percent or less from nominal values.

2.10 ENTRY CONTROL SOFTWARE

2.10.1 Interface Device

The entry control software shall control passage. The decision to grant or deny passage shall be based upon identifier data to be input at a specific location. If all conditions are met, a signal shall be sent to the input device location to activate the appropriate electric strike, bolt, electromagnetic lock or other type of portal release or facility interface device.

2.10.2 Operator Interface

Entry control operation shall be entirely automatic under control of the central station and local processors except for simple operations required for map display, alarm acknowledgment, zone and portal status change operations, audible or visual alarm silencing and audio annunciation. The system shall immediately annunciate changes in zone and portal status. The alarm printer shall print a permanent record of each alarm and status change. The map displays or graphics screens shall display the current status of system zones and portals. The central station shall immediately display the current status of any zone or portal upon command. While the system is annunciating an unacknowledged zone or portal alarm, keyboard operations at the central station, other than alarm acknowledgment, shall not be possible. The system shall provide the capability to change zone and portal status from alarm (after alarm acknowledgment) or access to secure; from alarm (after alarm acknowledgment) or secure to access, or from access to secure by simple control operations. If the operator attempts to change zone status to secure while there is an alarm output for that zone or portal, the system shall immediately annunciate an alarm for

that zone or portal.

2.10.3 Entry Control Functions

2.10.3.1 Multiple Security Levels

The system shall have multiple security levels. Each of the security levels shall be delineated by facility barriers. Access to each security level shall be through portals in the facility barriers using designated entry control procedures. The system shall provide at least 8 security levels. Any attempt to access an area beyond an individual's security level shall initiate an access denial alarm.

2.10.3.2 Two person rule

The system shall provide a 2 person rule feature. When a portal is designated as a 2 person rule portal, it shall not allow passage unless 2 valid identifiers are presented in the proper sequence. The scheme shall be designed so that only the first 2 valid identifiers and the last 2 valid identifiers pass together.

2.10.3.3 Anti-Passback

NOTE: The designer will show on the drawings or in a table all portals that will use anti-passback procedures and equipment. The designer will also show on the drawings the location of release switches for electromagnetic locks or electric strikes at portals not incorporating anti-passback procedures.

Portals as shown shall incorporate anti-passback functions. Anti-passback functions and identifier tracking shall be system-wide for portals incorporating anti-passback. Once an authorized, enrolled individual has passed through a portal using entry control procedures, the system shall not allow use of the same identifier to pass through any portal at the same security level until the individual has egressed through a portal at this same security level using entry control procedures. Any attempt to violate anti-passback procedures shall initiate an access denial alarm. Portals that do not incorporate anti-passback functions shall allow egress from the area by a push-button switch for activation of the facility interface device. Portal egress switch shall be located as shown.

2.10.3.4 Immediate Access Change

The system shall provide functions to disenroll and deny access to any identifier or combination of identifiers without consent of the individual or recovery of a credential. The design of the system shall provide entry change capability to system operators and managers with appropriate passwords at the system operator or enrollment consoles.

2.10.3.5 Multiple Time Zones

NOTE: Specify the number of time zones required during each 24 hour period for the week plus any special access time periods required for the site or

an area.

The system shall provide multiple time zone entry control. Personnel enrolled in the system shall only be allowed access to a facility during the time of day they are authorized to access the facility. Time zone access control shall also include the ability to specify beginning and ending dates that an individual will be authorized to access a facility. The system shall provide automatic activation and deactivation of entry authorization. The design of the system shall provide at least [_____] time zones with overlapping time zones. The system shall provide a means for system operators with proper password clearance, to define custom names for each time zone, and to change the time zone's beginning and ending times through the system operator and enrollment interfaces. The system shall automatically disenroll individuals at the end of their predefined facility access duration. Any attempt during a 24 hour period by an individual or an identifier to gain facility entry outside of the authorized time zone shall initiate an entry denial alarm.

2.10.3.6 Guard Tour

The system shall provide guard tour monitoring capability. The system shall monitor a security guard's progress and timing during performance of routine inspections. The system shall provide a means for operators and managers with appropriate password levels to define facility check points, and create time windows of the shortest and longest times necessary to get from one check point on the tour to the next. The time window between check points shall be adjustable over a range of at least 1 minute to 1 hour with a resolution of at least 1 minute. The system shall annunciate an alarm if the guard does not log in at the next check point within the allotted time window. Time measurements shall be reset at each terminal device check point when the guard logs in so that cumulative time variations do not result in false alarms. The guard tour shall have a random start/stop function so that a tour may start from any designated station at any designated time, and in either a forward or reverse direction to ensure that patrol patterns cannot be deduced by observation. The system operator shall be able to reposition or halt a guard during a tour to allow time for investigations to be made. The system guard tour feature shall be able to store at least 128 programmed guard tours in memory with at least 12 tours active at any one time, and at least 24 check points for each tour. Guard tours shall be configured as needed for the site.

2.10.3.7 Elevator Control

The system shall control elevator operation with entry control terminal devices. The elevator's standard control equipment, components, and actuators shall serve as the facility interface. System components and subsystems shall interface to standard elevator control equipment without modification of the elevator control equipment. The system shall provide means to define access controlled floors of a facility, deny access to these floors by unauthorized individuals, and implement all other system functions as specified.

2.10.4 Electronic Entry Control System Capacities

The system shall be designed and configured to provide the following capacities.

2.10.4.1 Enrollees

NOTE: Specify the maximum number of personnel to be
enrolled in the data base, including future
personnel, so the system will have adequate
expansion capability.

The system shall be configured for [_____] enrollees. The system shall provide a facility-tailorable reference file database containing personal, access authorization, identifier and verification data for each enrollee as required.

2.10.4.2 Transaction History File Size

The system capacity shall be at least the amount of transactions for the system during 1 year without any loss of transaction data.

2.10.5 Entry Control System Alarms

The system shall annunciate an alarm when the following conditions occur. Alarms shall be annunciated at the console both audibly and visually. An alarm report shall also be printed on the system printer. The alarm annunciation shall continue until acknowledged by the system operator. Only 1 control key shall be needed to acknowledge an alarm. The system shall control, monitor, differentiate, rank, annunciate, and allow operators to acknowledge, in real time, alarm signals generated by system equipment. The system shall also provide a means to define and customize the annunciation of each alarm type. The system shall use audio and visual information to differentiate the various types of alarms. Each alarm type shall be assigned an audio and a unique visual identifier.

2.10.5.1 Duress

The system shall annunciate a duress alarm when a duress code is entered at a keypad or a duress switch is activated. Duress alarms shall be annunciated in a manner that distinguishes them from all other system alarms. Duress alarms shall not be annunciated or otherwise indicated locally nor shall a duress alarm cause any special or unusual indications at the portal or area initiating the duress alarm. Individual privileges shall be carried out the same as an authorized entry to the protected area. Duress alarms shall only be annunciated at the central station and remote displays. Alarms shall be annunciated on the monitor and shall be logged on the printer.

2.10.5.2 Guard Tour

The system shall annunciate an alarm when a security guard does not arrive at a guard tour check point during the defined time window or if check points are passed out of the prescribed order.

2.10.5.3 Entry Denial

The system shall annunciate an alarm when an attempt has been made to pass through a controlled portal and entry has been denied.

2.10.5.4 Portal Open

The system shall annunciate an alarm when an entry controlled portal has been open longer than a predefined time delay. The time delay shall be adjustable, under operator control, over a range of at least 1 second to 1 minute with a maximum resolution of 1 second.

2.10.5.5 Bolt Not Engaged

The system shall annunciate an alarm when the bolt at an entry controlled portal has been open longer than a predefined time delay and generate an entry control alarm. The time delay shall be adjustable, under operator control, over a range of at least 1 second to 1 minute with a maximum resolution of 1 second.

2.10.5.6 Strike Not Secured

The system shall annunciate an alarm when the strike at an entry controlled portal has been left unsecured longer than a predefined time delay and generate an entry control alarm. The time delay shall be adjustable, under operator control, over a range of at least 1 second to 1 minute with a maximum resolution of 1 second.

2.10.5.7 Alarm Shunting/System Bypass

The system shall provide a means to ignore operator selected alarm types at operator selected portals in order to allow standard entry control procedures to be bypassed (shunted). Predefined alarm shunting shall only be available to system operators with the proper password. The system shall also provide for predefined alarm shunting based upon time zones. This capability shall only apply to the entry control alarm type.

2.11 WIRE AND CABLE

The Contractor shall provide all wire and cable not indicated as Government furnished equipment. Wiring shall meet NFPA 70 standards.

2.11.1 Above Ground Sensor Wiring

Sensor wiring shall be 20 AWG minimum, twisted and shielded, 2, 3, 4, or 6 pairs to match hardware. Multiconductor wire shall have an outer jacket of PVC.

2.11.2 Direct Burial Sensor Wiring

Sensor wiring shall be 20 AWG minimum, twisted and shielded, 2, 3, 4, or 6 pairs to match hardware. The construction of the direct burial cable shall be as specified in Section 16792A WIRE LINE DATA TRANSMISSION SYSTEM.

2.11.3 Local Area Network (LAN) Cabling

LAN cabling shall be in accordance with EIA ANSI/TIA/EIA-568-A, category 5.

PART 3 EXECUTION

3.1 GENERAL REQUIREMENTS

The Contractor shall install all system components, including Government furnished equipment, and appurtenances in accordance with the

manufacturer's instructions, IEEE C2 and as shown. The contractor shall furnish necessary interconnections, services, and adjustments required for a complete and operable system as specified and shown. Control signal, communications, and data transmission line grounding shall be installed as necessary to preclude ground loops, noise, and surges from adversely affecting system operation.

3.1.1 Installation

NOTE: Designer will specify the correct Section titles and numbers for electrical work. The type of raceway used can be electric metallic or rigid galvanized steel. The requirements of the National Electrical Code are the governing authority.

The contractor shall install the system in accordance with the standards for safety, NFPA 70, UL 681, UL 1037 and UL 1076, and the appropriate installation manual for each equipment type. Components within the system shall be configured with appropriate service points to pinpoint system trouble in less than 20 minutes. Minimum size of conduit shall be 15 mm. 1/2 inch. DTS shall not be pulled into conduits or placed in raceways, compartments, outlet boxes, junction boxes, or similar fittings with other building wiring. Flexible cords or cord connections shall not be used to supply power to any components of the system, except where specifically noted. All other electrical work shall be as specified in Section [_____] and as shown.

3.1.2 Enclosure Penetrations

Enclosure penetrations shall be from the bottom unless the system design requires penetrations from other directions. Penetrations of interior enclosures involving transitions of conduit from interior to exterior, and penetrations on exterior enclosures shall be sealed with rubber silicone sealant to preclude the entry of water. The conduit riser shall terminate in a hot-dipped galvanized metal cable terminator. The terminator shall be filled with an approved sealant as recommended by the cable manufacturer, and in a manner that does not damage the cable.

3.1.3 Cold Galvanizing

Field welds and/or brazing on factory galvanized boxes, enclosures, conduits, etc., shall be coated with a cold galvanized paint containing at least 95 percent zinc by weight.

3.1.4 Current Site Conditions

The Contractor shall verify that site conditions are in agreement with the design package. The Contractor shall report any changes in the site, or conditions that will affect performance of the system to the Government in a report as defined in paragraph Group II Technical Data Package. The Contractor shall not take any corrective action without written permission from the Government.

3.1.5 Existing Equipment

NOTE: This paragraph is required only if this

project includes the use of existing systems,
components, or other Government Furnished Equipment.

The Contractor shall connect to and utilize existing equipment, DTS, and devices as shown. System equipment and DTS that are usable in their original configuration without modification may be reused with Government approval. The Contractor shall perform a field survey, including testing and inspection of all existing system equipment and DTS intended to be incorporated into the system, and furnish a report to the Government as part of the site survey report as defined in paragraph Group II Technical Data Package. For those items considered nonfunctioning, the report shall include specification sheets, or written functional requirements to support the findings and the estimated cost to correct the deficiency. As part of the report, the Contractor shall include the scheduled need date for connection to all existing equipment. The Contractor shall make written requests and obtain approval prior to disconnecting any signal lines and equipment, and creating equipment downtime. Such work shall proceed only after receiving Government approval of these requests. If any device fails after the Contractor has commenced work on that device, signal or control line, the Contractor shall diagnose the failure and perform any necessary corrections to his equipment and work. The Government is responsible for maintenance and the repair of Government equipment. The Contractor shall be held responsible for repair costs due to Contractor negligence or abuse of Government equipment.

3.1.6 Installation Software

The Contractor shall load software as specified and required for an operational system, including data bases and specified programs. Upon successful completion of the endurance test, the Contractor shall provide original and backup copies on CD-ROM of all accepted software, including diagnostics.

3.2 SYSTEM STARTUP

Satisfaction of the requirements below does not relieve the Contractor of responsibility for incorrect installations, defective equipment items, or collateral damage as a result of Contractor work/equipment. The Contractor shall not apply power to the system until after:

a. System equipment items and DTS have been set up in accordance with manufacturer's instructions.

b. A visual inspection of the system has been conducted to ensure that defective equipment items have not been installed and that there are no loose connections.

c. System wiring has been tested and verified as correctly connected.

d. System grounding and transient protection systems have been verified as properly installed.

e. Power supplies to be connected to the system have been verified as the correct voltage, phasing, and frequency.

3.3 SUPPLEMENTAL CONTRACTOR QUALITY CONTROL

NOTE: The contractor quality control requirements for all electronic security projects, as stated in ER 1180-1-6, must be included in contracts, regardless of increase in project cost. Normally this contractor quality control requirement is applicable to projects in excess of \$1,000,000.

The Contractor shall provide the services of technical representatives who are familiar with all components and installation procedures of the installed system; and are approved by the Contracting Officer. These representatives shall be present on the job site during the preparatory and initial phases of quality control to provide technical assistance. These representatives shall also be available on an as needed basis to provide assistance with follow-up phases of quality control. These technical representatives shall participate in the testing and validation of the system and shall provide certification that their respective system portions meet the contractual requirements.

3.4 TESTING

3.4.1 General Requirements for Testing

The Contractor shall provide personnel, equipment, instrumentation, and supplies necessary to perform site testing. The Government will witness all performance verification and endurance testing. Written permission shall be obtained from the Government before proceeding with the next phase of testing. Original copies of all data produced during predelivery, performance verification and endurance testing, shall be turned over to the Government at the conclusion of each phase of testing, prior to Government approval of the test.

3.4.2 Predelivery Testing

The Contractor shall assemble the test system as specified, and perform tests to demonstrate that performance of the system complies with specified requirements in accordance with the approved predelivery test procedures. The tests shall take place during regular daytime working hours on weekdays. Model numbers of equipment tested shall be identical to those to be delivered to the site. Original copies of all data produced during predelivery testing, including results of each test procedure, shall be delivered to the Government at the conclusion of predelivery testing, prior to Government approval of the test. The test report shall be arranged so that all commands, stimuli, and responses are correlated to allow logical interpretation.

3.4.2.1 Test Setup

The predelivery test setup shall include the following:

- a. All central station equipment.
- b. At least 1 of each type DTS link, but not less than 2 links, and associated equipment to provide a fully integrated system.
- c. The number of local processors shall equal the amount required by the site design.
- d. At least 1 of each type sensor used.

e. Enough sensor simulators to provide alarm signal inputs to the system equal to the number of sensors required by the design. The alarm signals shall be manually or software generated.

f. At least 1 of each type of terminal device used.

g. At least 1 of each type of portal configuration with all facility interface devices as specified or shown.

h. Equipment as specified in Section 16751A CLOSED CIRCUIT TELEVISION SYSTEMS when required.

i. The Contractor shall prepare test procedures and reports for the predelivery test, and shall deliver the predelivery test procedures to the Government for approval. The final predelivery test report shall be delivered after completion of the predelivery test.

3.4.3 Contractor's Field Testing

The Contractor shall calibrate and test all equipment, verify DTS operation, place the integrated system in service, and test the integrated system. Ground rods installed by the Contractor shall be tested as specified in IEEE Std 142. The Contractor shall deliver a report describing results of functional tests, diagnostics, and calibrations, including written certification to the Government that the installed complete system has been calibrated, tested, and is ready to begin performance verification testing. The report shall also include a copy of the approved performance verification test procedure.

3.4.4 Performance Verification Test

The Contractor shall demonstrate that the completed system complies with the contract requirements. Using approved test procedures, all physical and functional requirements of the project shall be demonstrated and shown.

The performance verification test, as specified, shall not be started until after receipt by the Contractor of written permission from the Government, based on the Contractor's written report. The report shall include certification of successful completion of testing as specified in paragraph Contractor's Field Testing, and upon successful completion of training as specified. The Government may terminate testing at any time when the system fails to perform as specified. Upon termination of testing by the Government or by the Contractor, the Contractor shall commence an assessment period as described for Endurance Testing Phase II. Upon successful completion of the performance verification test, the Contractor shall deliver test reports and other documentation as specified to the Government prior to commencing the endurance test.

3.4.5 Endurance Test

a. General: The Contractor shall demonstrate system reliability and operability at the specified throughput rates for each portal, and the Type I and Type II error rates specified for the completed system. The contractor shall calculate false alarm rates and the system shall yield false alarm rates within the specified maximums at the specified probability of detection. The endurance test shall be conducted in phases as specified. The endurance test shall not be started until the Government notifies the Contractor, in writing, that the performance verification test is satisfactorily completed, training as specified has been completed, and

correction of all outstanding deficiencies has been satisfactorily completed. The Contractor shall provide 1 operator to operate the system 24 hours per day, including weekends and holidays, during Phase I and Phase III endurance testing, in addition to any Government personnel that may be made available. The Government may terminate testing at any time the system fails to perform as specified. Upon termination of testing by the Government or by the Contractor, the Contractor shall commence an assessment period as described for Phase II. The Contractor shall verify the operation of each terminal device during the last day of the test. Upon successful completion of the endurance test, the Contractor shall deliver test reports and other documentation as specified to the Government prior to acceptance of the system.

b. Phase I Testing: The test shall be conducted 24 hours per day for 15 consecutive calendar days, including holidays, and the system shall operate as specified. The Contractor shall make no repairs during this phase of testing unless authorized by the Government in writing. If the system experiences no failures during Phase I testing, the Contractor may proceed directly to Phase III testing after receipt by the Contractor of written permission from the Government.

c. Phase II Assessment: After the conclusion of Phase I, the Contractor shall identify all failures, determine causes of all failures, repair all failures, and deliver a written report to the Government. The report shall explain in detail the nature of each failure, corrective action taken, results of tests performed, and shall recommend the point at which testing should be resumed. After delivering the written report, the Contractor shall convene a test review meeting at the jobsite to present the results and recommendations to the Government. The meeting shall not be scheduled earlier than 5 business days after receipt of the report by the Government. As a part of this test review meeting, the Contractor shall demonstrate that all failures have been corrected by performing appropriate portions of the performance verification test. Based on the Contractor's report and the test review meeting, the Government will determine the restart date, or may require that Phase I be repeated. If the retest is completed without any failures, the Contractor may proceed directly to Phase III testing after receipt by the Contractor of written permission from the Government.

d. Phase III Testing: The test shall be conducted 24 hours per day for 15 consecutive calendar days, including holidays, and the system shall operate as specified. The Contractor shall make no repairs during this phase of testing unless authorized by the Government in writing.

e. Phase IV Assessment: After the conclusion of Phase III, the Contractor shall identify all failures, determine causes of failures, repair failures, and deliver a written report to the Government. The report shall explain in detail the nature of each failure, corrective action taken, results of tests performed, and shall recommend the point at which testing should be resumed. After delivering the written report, the Contractor shall convene a test review meeting at the jobsite to present the results and recommendations to the Government. The meeting shall not be scheduled earlier than 5 business days after receipt of the report by the Government. As a part of this test review meeting, the Contractor shall demonstrate that all failures have been corrected by repeating appropriate portions of the performance verification test. Based on the Contractor's report and the test review meeting, the Government will determine the restart date, and may require that Phase III be repeated. The Contractor shall not commence any required retesting until after

receipt of written notification by Government. After the conclusion of any retesting which the Government may require, the Phase IV assessment shall be repeated as if Phase III had just been completed.

f. Exclusions: The Contractor will not be held responsible for failures in system performance resulting from the following:

(1) An outage of the main power in excess of the capability of any backup power source, provided that the automatic initiation of all backup sources was accomplished and that automatic shutdown and restart of the ESS performed as specified.

(2) Failure of a Government furnished communications circuit, provided that the failure was not due to Contractor furnished equipment, installation, or software.

(3) Failure of existing Government owned equipment, provided that the failure was not due to Contractor furnished equipment, installation, or software.

(4) The occurrence of specified nuisance alarms.

(5) The occurrence of specified environmental alarms.

3.5 RELIABILITY CALCULATION

This exponential calculation depends on the test duration and assumes that the Mean Time Between Failures (MTBF) does not change after each repair; and that the probability of failure is constant throughout the useful life of the component regardless of how many failures the system has experienced. This calculation does not account for effects of aging.

3.5.1 Definition of Reliability

System reliability is calculated in terms of overall MTBF where the component reliability furnished by vendors is already expressed as MTBF. The mathematical combination of the component MTBF values is defined as the system reliability, $R(t)$; the probability that the system will perform its function during a given time period under specified conditions. In this calculation, each component reliability is determined; the component reliabilities are combined as dictated by the system configuration; and the overall MTBF is computed as follows:

$R(t) = e^{(-t/MTBF)}$; where:

MTBF = mean time between failure

t = duration of test period

e = base of natural logarithms

When $t/MTBF$ is less than 0.1, the reliability can be approximated as follows:

$R(t) = 1 - (t/MTBF)$: A specific reliability value can be interpreted by noting that a value of $R(t)$ greater than $1/e$ (which equals 0.37) indicates that the MTBF value is greater than the test duration.

3.5.2 Series and Parallel Components

Components are in series if failure of 1 component causes a system failure. Reliability of components in series is a product of the individual reliabilities:

$R = 1 - (r_1)(r_2)(r_3) \dots (r_n)$. If components in a system are redundant (parallel), reliability is computed as follows:

$R = 1 - \{(1-r_1)(1-r_2) \dots (1-r_n)\}$. If a system has parallel components, an equivalent series reliability is computed for each set of parallel components. The reliability of the system is then computed as the product of series and equivalent series reliabilities.

3.5.3 Calculation Procedure

The Contractor shall prepare a table showing the following data:

- a. Name and quantity of each component.
- b. Each component identified as series or parallel. (For example, if there are 2 printers, the failure of 1 will not cause a system failure).
- c. MTBF for each component.
- d. Single unit reliability: $R = e(-t/MTBF)$, where $t = 1,000$ hour test period.
- e. Total Component Reliability (TCR) where $TCR = R^n$, and n = number of components. For parallel components, $TCR = 1 - (1-R)^n$, where n = number of components.
- f. Cumulative Reliability (CUMR) is the product of total component reliability; for example: $CUMR_4 = (TCR_1)(TCR_2)(TCR_3)(TCR_4) = (CUMR_3)(TCR_4)$
- g. Cumulative MTBF = $-1,000/LN(CUMR)$; where $LN(CUMR)$ is the natural logarithm of (CUMR). As an example: $CUM.MTBF = -1,000/LN(CUMR_4)$

3.5.4 Sample Calculations

MTBF is not calculated for sensors and controls. Input/Output functions are part of the local processor. Any Input/Output failure not attributable to sensors and controls constitutes a local processor failure and is thus reflected in the local processor MTBF. MTBF for other components are based on the lowest values provided by vendors. The calculation shall be based on the following configuration:

- a. All central station equipment.
- b. Data Transmission System (DTS) equipment associated with one DTS circuit, but excluding the circuit itself.
- c. Sixteen local processors with all the functions as specified in paragraph Local Processor.
- d. Four representative types of devices, per local processor.

-- End of Section --

