****
USACE / NAVFAC / AFCEC / NASA **UFGS-28 20 00.00 20 (April 2006)**

Preparing Activity: NAVFAC **Superseding**
UFGS-13703N (February 2004)

UNIFIED FACILITIES GUIDE SPECIFICATIONS

References are in agreement with UMRL dated October 2015
****

SECTION TABLE OF CONTENTS

DIVISION 28 - ELECTRONIC SAFETY AND SECURITY

SECTION 28 20 00.00 20

ELECTRONIC SECURITY SYSTEMS (ESS), COMMERCIAL

04/06

PART 1 GENERAL

1.1 REFERENCES
1.2 STANDARD PRODUCTS
1.3 DEFINITIONS
1.4 SYSTEM DESCRIPTION
1.4.1 Design Requirements
1.4.1.1 Backup Battery Capacity Calculations
1.4.1.2 Probability of Detection Calculations
1.5 SUBMITTALS
1.6 QUALITY ASSURANCE
1.6.1 Drawings
1.6.1.1 ESS Components
1.6.1.2 Overall System Schematic
1.6.2 Evidence of Experience and Qualifications
1.6.2.1 Installer's Qualifications
1.6.2.2 Instructor's Qualifications
1.6.3 Regulatory Requirements
1.6.3.1 Reference Standard Compliance
1.6.3.2 Independent Testing Organization Certificate
1.6.4 ESS Operational Test Plan
1.6.5 User's Software Data
1.6.6 Standard Products
1.6.6.1 Alternative Qualifications
1.6.6.2 Material and Equipment Manufacturing Date

PART 2 PRODUCTS

2.1 ESS SUBSYSTEMS
2.2 INTEGRATED SYSTEM FUNCTIONAL REQUIREMENTS
2.2.1 Growth Capability
2.2.2 Intrinsically Safe
2.3 INTEGRATED SYSTEM PERFORMANCE REQUIREMENTS
2.3.1 Detection Coverage
2.3.2 Detection Resolution (Sensitivity)
2.3.3 Detection Alarm and Reporting Capacity

2.3.4 Probability of Detection
2.3.4.1 Combinational Processing
2.3.4.2 Other System Success Considerations
2.3.5 Intrusion Detection System (IDS)
2.3.5.1 Premise Control Unit (PCU)
2.3.5.2 Detection devices
2.3.5.3 Tamper Switches
2.3.5.4 Fail-Safe Capability
2.3.5.5 Line Fault Detection
2.3.5.6 Power Loss Detection
2.3.6 Manual and Self-Test
2.3.7 Electrical Power
2.3.7.1 Primary Power
2.3.7.2 Backup Power
2.4 SYSTEM PERFORMANCE REQUIREMENTS
2.4.1 Modularity
2.4.2 Reliability
2.4.3 Maintainability
2.4.4 Availability
2.4.5 Environmental Conditions
2.4.5.1 Interior Conditions
2.4.5.2 Exterior Conditions
2.4.5.3 Transient voltage surge suppression
2.4.6 Electromagnetic Interference (EMI)
2.4.7 Electromagnetic Radiation (EMR)
2.4.8 Interchangeability
2.4.9 Safety
2.4.10 Human Engineering
2.4.10.1 Visual Annunciators
2.4.10.2 Controls
2.4.11 Computer Software
2.4.11.1 Mission Software
2.4.11.2 Support Software
2.4.11.3 Software Performance Requirements
2.4.12 Test Points
2.4.13 Component Enclosures
2.4.13.1 Metal Thickness
2.4.13.2 Doors and Covers
2.4.13.3 Ventilation
2.4.13.4 Mounting
2.4.13.5 Labels
2.4.13.6 Enclosure Locks
2.4.14 Detection Sensors
2.4.14.1 Interior Point Sensors
2.4.14.2 Interior Volumetric Sensors
2.4.14.3 Exterior Fence and Perimeter Sensors
2.4.14.4 Duress Alarms
2.4.15 Automated Access Control System (AACS)
2.4.15.1 Error and Throughput Rates
2.4.15.2 Access Control Subsystem Central Processing
2.4.15.3 Access Control Unit (ACU)
2.4.15.4 Card Reader and Keypad Access Control Devices
2.4.15.5 Access Control Cards
2.4.16 Communications
2.4.16.1 Link Supervision
2.4.16.2 Hardwire
2.4.16.3 Radio Frequency Link
2.4.17 Closed-Circuit Television (CCTV) System
2.4.17.1 Cameras

2.4.17.2 Video Signal
2.4.17.3 Video Matrix Switchers
2.4.17.4 Video Transmission
2.4.17.5 Color Video Monitors
2.4.17.6 Ancillary Equipment
2.4.18 Security Command Center (SCC)
2.4.18.1 ESS Software
2.4.18.2 Digital Receiver
2.4.18.3 Printer Requirements
2.4.18.4 ESS Monitor Display Software
2.4.18.5 Graphical Map Software
2.4.18.6 Control and Display Integration
2.5 FIELD FABRICATED NAMEPLATES
2.5.1 Manufacturer's Nameplate
2.6 FACTORY APPLIED FINISH

PART 3 EXECUTION

3.1 EQUIPMENT INSTALLATION
3.1.1 Cable and Wire Runs
3.1.2 Soldering
3.1.3 Galvanizing
3.1.4 Fungus Treatment
3.1.5 Conduit
3.1.6 Underground Cable Installation
3.1.7 Exterior Fences
3.2 ADJUSTMENT, ALIGNMENT, SYNCHRONIZATION, AND CLEANING
3.3 ESS System Acceptance and Training
3.3.1 ESS System Acceptance Test
3.3.2 ESS Training Outline
3.3.2.1 ESS Administrator Training
3.3.2.2 ESS Operator Training
3.3.3 Follow-up Training
3.3.4 Training Operating and Maintenance Personnel
3.4 FIELD APPLIED PAINTING
3.5 NAMEPLATE MOUNTING

-- End of Section Table of Contents --

****

USACE / NAVFAC / AFCEC / NASA	**UFGS-28 20 00.00 20 (April 2006)**

Preparing Activity: NAVFAC	**Superseding**
	UFGS-13703N (February 2004)

UNIFIED FACILITIES GUIDE SPECIFICATIONS

References are in agreement with UMRL dated October 2015

****

SECTION 28 20 00.00 20

ELECTRONIC SECURITY SYSTEMS (ESS), COMMERCIAL
04/06

****

NOTE: This guide specification covers the requirements for commercial electronic security systems consisting of commercial equipment which is limited to a full range of interior point protection devices duress sensors, volumetric (space) protection sensors, simple exterior sensors limited to devices that can be hung on or attached to perimeter barriers, closed-circuit television (CCTV) for remote alarm assessment purposes, alarm signal data communications media, alarm reporting and monitoring systems, control systems. System requirements must conform to UFC 4-021-02, "Electronic Security Systems". Consult the appropriate Facilities Engineering Command for questions concerning system design.

Adhere to UFC 1-300-02 **Unified Facilities Guide Specifications (UFGS) Format Standard when editing this guide specification or preparing new project specification sections. Edit this guide specification for project specific requirements by adding, deleting, or revising text. For bracketed items, choose applicable items(s) or insert appropriate information.**

Remove information and requirements not required in respective project, whether or not brackets are present.

Comments, suggestions and recommended changes for this guide specification are welcome and should be submitted as a Criteria Change Request (CCR)**.**

****

****

NOTE: The following information shall be shown on the project drawings:

1. Floor plans: Location of security devices, control units, alarm display equipment, and electrical power cabinets;

2. Site plan: Exterior devices and routing of conductors and conduit into building;

3. Single line type system riser diagram. Connection of equipment should be indicated for typical system chosen for cost estimating purposes;

4. Single line type electrical riser diagram; and

5. Mounting: Details for each device required for complete installation, including junction boxes for recessed BMS where required. Include device height and installation of wiring.

6. The device symbol presents an easy to use and efficient means of identifying the essential features of the security engineering design effort. The symbol provides a method by which the phenomenology of the device, necessary identifying details related to the phenomenology of the device, and the means by which the device is positioned or mounted can be readily indicated on the engineering plans. The symbol also provides a means of identifying the device in order to develop accurate bills of material and system diagrams.

****

PART 1 GENERAL

1.1 REFERENCES

****

NOTE: This paragraph is used to list the publications cited in the text of the guide specification. The publications are referred to in the text by basic designation only and listed in this paragraph by organization, designation, date, and title.

Use the Reference Wizard's Check Reference feature when you add a RID outside of the Section's Reference Article to automatically place the reference in the Reference Article. Also use the Reference Wizard's Check Reference feature to update the issue dates.

References not used in the text will automatically be deleted from this section of the project specification when you choose to reconcile references in the publish print process.

****

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 NATIONAL STANDARDS INSTITUTE (ANSI)

ANSI C39.1	(1981; R 1992) Requirements for Electrical Analog Indicating Instruments

ASTM INTERNATIONAL (ASTM)

ASTM A123/A123M	(2013) Standard Specification for Zinc (Hot-Dip Galvanized) Coatings on Iron and Steel Products
ASTM B32	(2008; R 2014) Standard Specification for Solder Metal
ASTM D709	(2013) Laminated Thermosetting Materials

INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS (IEEE)

IEEE 100	(2000; Archived) The Authoritative Dictionary of IEEE Standards Terms

NATIONAL ELECTRICAL MANUFACTURERS ASSOCIATION (NEMA)

NEMA 250	(2014) Enclosures for Electrical Equipment (1000 Volts Maximum)
NEMA ICS 2	(2000; R 2005; Errata 2008) Standard for Controllers, Contactors, and Overload Relays Rated 600 V
NEMA ICS 6	(1993; R 2011) Enclosures

NATIONAL FIRE PROTECTION ASSOCIATION (NFPA)

NFPA 70	(2014; AMD 1 2013; Errata 1 2013; AMD 2 2013; Errata 2 2013; AMD 3 2014; Errata 3-4 2014; AMD 4-6 2014) National Electrical Code

SOCIETY OF MOTION PICTURE AND TELEVISION ENGINEERS (SMPTE)

SMPTE 170M	(2004) Television - Composite Analog Video Signal - NTSC for Studio Applications

TELECOMMUNICATIONS INDUSTRY ASSOCIATION (TIA)

TIA-232	(1997f; R 2012) Interface Between Data Terminal Equipment and Data Circuit-Terminating Equipment Employing Serial Binary Data Interchange

U.S. DEFENSE INTELLIGENCE AGENCY (DIA)

DIA DCID 6/9	(2002) Director of Central Intelligence Directive No. 6/9

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

47 CFR 15	Radio Frequency Devices

UNDERWRITERS LABORATORIES (UL)

UL 1037	(1999; Reprint Dec 2009) Safety Antitheft Alarms and Devices
UL 1076	(1995; Reprint Mar 2015) Proprietary Burglar Alarm Units and Systems
UL 1610	(1998; Reprint Mar 2015) Standard for Central-Station Burglar-Alarm Units
UL 294	(2013; Reprint Feb 2015) Access Control System Units
UL 497B	(2004; Reprint Dec 2012) Protectors for Data Communication Circuits
UL 636	(1996; Reprint Jan 2013) Holdup Alarm Units and Systems
UL 639	(2007; Reprint May 2012) Standard for Intrusion Detection Units
UL 681	(2014) Installation and Classification of Burglar and Holdup Alarm Systems
UL 796	(2010; Reprint Sep 2013) Standard for Printed-Wiring Boards

1.2 STANDARD PRODUCTS

Material and equipment shall be the standard products of a manufacturer regularly engaged in the manufacture of such products. Items of equipment shall essentially duplicate equipment that have been in satisfactory use at least 2 years prior to bid opening. Equipment shall be supported by a service organization that is, in the opinion of the Contracting Officer, reasonably convenient to the site.

1.3 DEFINITIONS

Unless otherwise specified or indicated, electrical and electronics terms used in these specifications, and on the drawings, shall be as defined in IEEE 100.

a. Active mode: That in which some type of signal is continuously sent across the link, resulting in simple link breaks being readily detected.

b. Fail-safe: The capability to monitor system functions and report an alarm when a failure is detected in a critical system function.

c. Installer: Either the Contractor or a subcontractor with whom the Contractor has a firm contractual agreement.

d. Intruder: An animate object at least 1220 mm 48 inches in height, 34 kg 75 pounds in weight and 0.113 cubic meter 4 cubic feet in volume, moving through the protected zones or portals at a velocity of 30 to 3000 mm 0.1 to 10 feet per second.

e. Sensor zone: A geographic position for which an intrusion must be identified and displayed and may be the combination of multiple detection devices.

f. Element: As used in this section means a constituent part of a complex signal such as an ac or dc voltage or current, ac phase, or frequency duration.

1.4 SYSTEM DESCRIPTION

[Provide new] [or] [modify existing] Electronic Security Systems (ESS), including associated equipment and appurtenances. The design of the ESS shall include devices and equipment used to detect intrusion, control access to restricted areas, detect and deny unauthorized entries within specific areas, generate reports, produce Photo Identification badges, provide surveillance and annunciate alarms. The ESS shall be designed to provide operational flexibility and reliable performance. The ESS shall be modular, allowing for future incremental expansion or modification of inputs, outputs, and remote control stations. Integrated system capabilities shall include but not be limited to Intrusion Detection, Automated Access Control, Intercommunications, CCTV and Photo Badge Identification. Each system shall be complete and ready for operation and provide for a fully integrated central station solution. [Existing system was manufactured by [_____], and new equipment shall be compatible with and operate accurately and reliably with the existing system.] Include materials not normally furnished by the manufacturer with the ESS equipment as specified in [Section 33 71 02 UNDERGROUND ELECTRICAL DISTRIBUTION] [and] [Section 33 71 01 OVERHEAD TRANSMISSION AND DISTRIBUTION] [and] Section 26 20 00 INTERIOR DISTRIBUTION SYSTEM.

1.4.1 Design Requirements

1.4.1.1 Backup Battery Capacity Calculations

Submit calculations showing that backup battery capacity exceeds sensor operation, communications supervision, and alarm annunciation power requirements.

1.4.1.2 Probability of Detection Calculations

Submit calculations showing probability Detection (Pd) meets the requirements for the ESS in accordance with paragraph entitled "Combinational Processing."

1.5 SUBMITTALS

****

NOTE: Review Submittal Description (SD) definitions in Section 01 33 00 SUBMITTAL PROCEDURES and edit the following list to reflect only the submittals required for the project.

The Guide Specification technical editors have designated those items that require Government approval, due to their complexity or criticality, with a "G". Generally, other submittal items can be reviewed by the Contractor's Quality Control System. Only add a “G” to an item, if the submittal is sufficiently important or complex in

context of the project.

For submittals requiring Government approval on Army projects, a code of up to three characters within the submittal tags may be used following the "G" designation to indicate the approving authority. Codes for Army projects using the Resident Management System (RMS) are: "AE" for Architect-Engineer; "DO" for District Office (Engineering Division or other organization in the District Office); "AO" for Area Office; "RO" for Resident Office; and "PO" for Project Office. Codes following the "G" typically are not used for Navy projects.

An "S" following a submittal item indicates that the submittal is required for the Sustainability Notebook to fulfill federally mandated sustainable requirements in accordance with Section 01 33 29 SUSTAINABILITY REPORTING.

Submittal items not designated with a "G" are considered as being for information only for Army projects and for Contractor Quality Control approval for Navy projects.

****

Government approval is required for submittals with a "G" designation; submittals not having a "G" designation are [for Contractor Quality Control approval.][for information only. When used, a designation following the "G" designation identifies the office that will review the submittal for the Government.] Submittals with an "S" are for inclusion in the Sustainability Notebook, in conformance to Section 01 33 29 SUSTAINABILITY REPORTING. Submit the following in accordance with Section 01 33 00 SUBMITTAL PROCEDURES:

[[The [_____] will review and] [_____] Division, Naval Facilities Engineering Command will approve submittals requiring special review in this section.

] Include wiring diagrams and installation details of equipment indicating proposed location, layout and arrangement, control panels, accessories, piping, ductwork, and other items that must be shown to ensure a coordinated installation. Wiring diagrams shall identify circuit terminals and indicate the internal wiring for each item of equipment and the interconnection between each item of equipment. Drawings shall indicate adequate clearance for operation, maintenance, and replacement of operating equipment devices. Submittals shall include the nameplate data, size, and capacity. Submittals shall also include applicable federal, military, industry, and technical society publication references.

SD-02 Shop Drawings

ESS components; G[, [_____]]

Overall system schematic; G[, [_____]]

SD-03 Product Data

Interior point sensors; G[, [_____]]

Interior volumetric sensors; G[, [_____]]

Duress alarms; G[, [_____]]

Card reader; G[, [_____]]

Keypad; G[, [_____]]

Biometric finger print reader; G[, [_____]]

Communications cable; G[, [_____]]

Microwave sensors; G[, [_____]]

Radio frequency link communications systems; G[, [_____]]

Communications interface devices; G[, [_____]]

CCTV camera; G[, [_____]]

CCTV lenses; G[, [_____]]

Auxiliary CCTV camera equipment; G[, [_____]]

Video tape recorder; G[, [_____]]

Video, Digital Video Recorder (DVR); G[, [_____]]

Video, Biometric Iris Scan; G[, [_____]]

Printer; G[, [_____]]

Uninterruptible power supply (UPS); G[, [_____]]

Batteries; G[, [_____]]

Graphic map display; G[, [_____]]

Four quadrant multiplexer; G[, [_____]]

SD-05 Design Data

Backup battery capacity calculations; G[, [_____]]

Probability of Detection Calculations

SD-06 Test Reports

ESS operational test plan; G[, [_____]]

SD-07 Certificates

ESS operational test plan; G[, [_____]]

Installer's qualifications; G[, [_____]]

Instructor's qualifications; G[, [_____]]

SD-10 Operation and Maintenance Data

ESS components, Data Package 5; G[, [_____]]

ESS software, Data Package 1; G[, [_____]]

Submit in accordance with Section 01 78 23 OPERATION AND MAINTENANCE DATA and Section 26 00 00.00 20 BASIC ELECTRICAL MATERIALS AND METHODS.

SD-11 Closeout Submittals

As-Built drawings for ESS; G[, [_____]]

Posted operating instructions for ESS; G[, [_____]]

1.6 QUALITY ASSURANCE

1.6.1 Drawings

1.6.1.1 ESS Components

Submit drawings that clearly and completely indicate the function of each ESS component. Indicate termination points of devices, and interconnections required for system operation. Indicate interconnection between modules and devices. In addition, submit a layout drawing showing spacing of components, location, mounting and positioning details.

1.6.1.2 Overall System Schematic

Indicate the relationship of integrated components on one diagram and show power source, system controls, impedance matches; plus number, size, identification, and maximum lengths of interconnecting wires. Drawings shall be not less than [420 by 297] [_____] mm [11 by 17] [_____] inches.

1.6.2 Evidence of Experience and Qualifications

1.6.2.1 Installer's Qualifications

Prior to installation, submit data of the installer's experience and certified qualifications. Show that the installer who will perform the work has a minimum of [2] [_____] years experience successfully installing ESS of the same type and design as specified herein. Include the names, locations, and points of contact of at least two installations of the same type and design as specified herein where the installer has installed such systems. Indicate the type of each system and certify that each system has performed satisfactorily in the manner intended for a period of not less than [12] [_____] months.

1.6.2.2 Instructor's Qualifications

Prior to installation, submit data of the instructor's experience and certified qualifications. Show that the instructor, who will train operating and maintenance personnel, has received a minimum of 24 hours of ESS training from a technical organization such as the National Burglar and Fire Alarm Association, and 2 years experience in the installation of ESS of the type specified.

1.6.3 Regulatory Requirements

In each of the publications referred to herein, consider the advisory provisions to be mandatory, as though the word, "shall" had been substituted for "should" wherever it appears. Interpret references in these publications to the "authority having jurisdiction," or words of similar meaning, to mean the Contracting Officer. Equipment, materials, installation, and workmanship shall be in accordance with the mandatory and advisory provisions of NFPA 70 unless more stringent requirements are specified or indicated.

1.6.3.1 Reference Standard Compliance

Where equipment or materials are specified to conform to industry and technical society reference standards of the organizations such as American National Standards Institute (ANSI), American Society for Testing and Materials (ASTM), National Electrical Manufacturers Association (NEMA), Underwriters Laboratories (UL), and Association of Edison Illuminating Companies (AEIC), submit proof of such compliance. The label or listing by the specified organization will be acceptable evidence of compliance

1.6.3.2 Independent Testing Organization Certificate

In lieu of the label or listing, submit a certificate from an independent testing organization, competent to perform testing, and approved by the Contracting Officer. The certificate shall state that the item has been tested in accordance with the specified organization's test methods and that the item complies with the specified organization's reference standard Provide only UL listed ESS equipment for Both exterior and interior ESS sensors, access control, and closed-circuit television (CCTV) components.

1.6.4 ESS Operational Test Plan

Submit at least 30 days prior to commencement of formal operational testing. Include detailed procedures for operational testing of each ESS component and subsystem, and for performance of an integrated system test.

1.6.5 User's Software Data

Submit for approval not later than 30 days prior to formal operational testing or instruction to Government personnel on ESS software, whichever is earlier. ESS software shall be documented in the user's manual.

1.6.6 Standard Products

Provide materials and equipment that are products of manufacturers regularly engaged in the production of such products which are of equal material, design and workmanship. Products shall have been in satisfactory commercial or industrial use for 2 years prior to bid opening. The 2-year period shall include applications of equipment and materials under similar circumstances and of similar size. The product shall have been on sale on the commercial market through advertisements, manufacturers' catalogs, or brochures during the 2-year period. Where two or more items of the same class of equipment are required, these items shall be products of a single manufacturer; however, the component parts of the item need not be the products of the same manufacturer unless stated in this section

1.6.6.1 Alternative Qualifications

Products having less than a 2-year field service record will be acceptable if a certified record of satisfactory field operation for not less than 6000 hours, exclusive of the manufacturers' factory or laboratory tests, is furnished

1.6.6.2 Material and Equipment Manufacturing Date

Products manufactured more than 3 years prior to date of delivery to site shall not be used, unless specified otherwise.

PART 2 PRODUCTS

2.1 ESS SUBSYSTEMS

Provide a complete integrated ESS consisting of the following major subsystems:

[a. Intrusion Detection System

][b. Automated Access Control System

] c. Communications

[d. Closed-circuit television (CCTV)

] e. Alarm reporting and display

f. Power

2.2 INTEGRATED SYSTEM FUNCTIONAL REQUIREMENTS

Ensure that ESS is fully integrated with physical security and other elements of the overall facility security system. Provide specific subsystem consisting of the following:

[a. Intrusion Detection subsystem: Sensors, premise control units (PCU) and software modules to detect and report intrusion attempts [and provide means to indicate a duress condition].

][b. Automated Access Control subsystem: Electronic devices, access control units (ACU), sensors and software modules to detect intrusion attempts monitor and control personnel movement through normal access routes in and out of the facility and between protected areas within the facility.

] c. Communications subsystem: Elements required to ensure that pertinent data is transferred from point of origin to point where appropriate actions can be taken. [Provide redundant communications links from control units to central processor unit.]

[d. CCTV subsystem: Electronic devices required to provide visual assessment of ESS alarms. [Interface to ESS for control of camera call up to monitors, Pan-tilt-Zoom control, Video recording based on alarm event triggers. Integration shall provide the means to associate ESS archived alarm events with recorded video] [at two separate locations].

] e. Alarm reporting and display subsystem: Software, hardware and devices to control, process, integrate, and annunciate ESS data [at [two]

[_____] or more locations]

f. Power subsystem: Components required to ensure continuous operation of the entire ESS.

2.2.1 Growth Capability

Provide capability for modular ESS expansion with minimal equipment modification. Products provided shall not limit growth capability to products of a single manufacturer.

[2.2.2 Intrinsically Safe

****
NOTE: Do not locate alarm reporting and display equipment within a hazardous area. If point sensors and volumetric sensors are required in hazardous areas, clearly identify their location on the plans. Delete this paragraph if no hazardous areas exist in this project.
****

System components located in areas where fire or explosion hazards may exist due to flammable gases or vapors, flammable liquids, combustible dust, or ignitable fibers or flyings shall be rated and installed according to Chapter 5 of NFPA 70. Classification of area and corresponding equipment ratings and installation procedures shall be as defined and specified in Chapter 5 of NFPA 70.

]2.3 INTEGRATED SYSTEM PERFORMANCE REQUIREMENTS

The installed and operating ESS shall be integrated into the overall facility to detect intrusion, Control Access, provide Closed Circuit Television (CCTV) surveillance, provide visual verification and shall perform as an entity, as specified below.

2.3.1 Detection Coverage

Provide and adjust sensors so that coverage is [overlapping and] maximized without mutual interference. [ESS coverage shall include [the facility perimeter] [and] critical spaces within the facility.]

2.3.2 Detection Resolution (Sensitivity)

Sensitivity shall be capable of the following:

a. Locating intrusions [within [100] [_____] meter zones along a line or perimeter] [to one side of the [facility] [building]];

b. Locating intrusions at individually protected assets or at an individual portal;

c. Locating intrusions within volume or areas to within the coverage on a single volumetric sensor; and

d. Locating failures or tampering at individual sensors.

2.3.3 Detection Alarm and Reporting Capacity

****

NOTE: Select system capacity parameters based on the specific facility design requirements. System capacity should be expressed as a binary number. Include a 25 percent expansion factor to accommodate changes in design caused by reconfiguration of equipment within interior spaces or renovation.

****

The ESS shall have the capacity to collect, communicate, and display up to [12] [32] [256] [_____] sensor zone alarms [and to enable control of [one] [two] [_____] response devices in each of the sensor zones]. If the sensor zone is a combination of multiple alarm sources, the system shall maintain the capability to identify individual sensors in an alarm state. A single alarm shall be annunciated within one second average, 2 seconds maximum, after sensor transducer or other detection device activation [except that alarms transmitted by radio frequency signaling shall communicate in approximately 2 seconds].

2.3.4 Probability of Detection

****

NOTE: For U.S. Navy facilities, minimum Ps is 0.9. Delete this paragraph for simple, non-high security systems. Use this paragraph when specific DoD and USN directives require a high level of performance, which is usually expressed as "probability of detection." See NAVFAC for discussion of "probability of detection."

****

Success shall be predicated on the proposed system architecture. Overall system probability of detection shall be [0.90] [0.95] [0.99] [_____] minimum.

2.3.4.1 Combinational Processing

The required system probability of detection at the 90 [_____] percent confidence level is based on the standard Chi-square distribution and is calculated from the formula Ps = Pd x Pc x Pa x Pp where:

Ps = Probability of system success.

Pd = Probability of detection for an individual sensor or sensor combination when more than one sensor is used.

Pc = Probability of correctly transmitting sensor data. The performance measure will account for remote processing and transmission error.

Pa = Probability of correctly annunciating alarm data and of providing the correct response at the operator interface, including accounting for errors introduced by central processing and display functions, but not including operator performance.

Pp = Probability of providing operating power of suitable quality.

2.3.4.2 Other System Success Considerations

****

NOTE: Select the most restrictive choice(s) based upon the degree of annunciation granularity required.

****

a. False alarm: An alarm which does not result from a valid intrusion by personnel, vehicles, other moving objects, or nuisances, but rather as a result of an internally generated sensor or other system component noise. The false alarm rate shall not exceed one per [30] [_____] days for each sensor zone.

b. Nuisance alarm: May result from sources external to the system which provide sensor stimuli similar to those of personnel, vehicles, or moving objects, such as wildlife and natural phenomena. Nuisance alarm rate is a function of sensor adjustment and shall not exceed a rate of one alarm per [7] [_____] days for each sensor zone for the initial 90 days after acceptance by the Government. Nuisance alarm rate shall not exceed a rate of one alarm per [30] [_____] days for each sensor zone thereafter.

c. Reliability and Availability: Reliability for ESS shall be based upon reliabilities of equipment used. Reliability requirements shall be as contained in equipment specifications, and when equipment is combined in particular configuration, shall provide a system-level mean-time-between-failure (MTBF) that is consistent with both the system-level availability requirement stated below and specific requirements for each defined functional area. Inherent availability required (Ai) is based on an assumption of no planned system downtime for preventive maintenance and shall be calculated as:

$$Ai = \frac{MTBF}{MTBF + MTTR}$$

Where MTBF is the mean-time-between-failure of the system as defined by:

$$\frac{1}{MTBF} = \sum_j \frac{1}{(MTBF)_j}$$

Where (MTBF)j is the achieved mean-time-between-failure of each individual piece of equipment used in the given system configuration as demonstrated in the individual equipment reliability qualification test.MTBF for this system shall be not less than [5000] [_____] hours. System shall be capable of pinpointing failures within [20] [_____] minutes.

MTTR is the weighted average mean-time-to-repair of the system as defined by:

$$MTTR = MTBF \times \sum_j \frac{(MTTR)_j}{(MTBF)_j}$$

Where (MTTR)j is the achieved mean-time-to-repair of each individual piece of equipment used in the specified system configuration. MTTR for this system shall not exceed [30] [_____] minutes of on-site time for any one

element.

2.3.5 Intrusion Detection System (IDS)

Provide a complete digital IDS with the performance criteria (posted operating instructions) detailed in this specification. The system shall be inclusive of all necessary functions, monitoring, and control capability as detailed herein and on accompanying Shop drawings. The IDS primary functions shall be to detect intrusion to secured areas. The system shall utilize a single database for all IDS programming data that shall seamlessly integrate with the ESS. This integration shall be provided under one operating environment. The IDS events shall be viewable as separate or as a combined list of all ESS events. Overall control of the IDS intrusion alarm monitoring shall be through software control of the ESS. The IDS shall provide both supervised and non-supervised alarm point monitoring. The system shall be capable of arming or disarming alarm points both manually and automatically by time of day, day of week or by operator command.

Components shall include but not be limited to the following:

a. Premise Control Units (PCU)

b. Detection devices

c. Tamper switches

d. Fail-safe capability

e. Line fault (for hardwire systems only) detection

f. Power loss detection

g. Battery Backup

2.3.5.1 Premise Control Unit (PCU)

PCU shall include a command processor installed in an attack and tamper resistant enclosure. The PCU shall be packaged and include a power transformer, battery(s), network connection cable, keypad(s), keypad connection cable(s) and additional components as required. All system electronic components shall be solid-state type, mounted on printed circuit boards. Light duty relays and similar switching devices shall be solid-state type or electromechanical. The PCU shall have an over current notification LED that lights when devices connected to the Keypad Bus or communication Bus(es) draw more current than the PCU is rated for. When the over current LED lights, the communications Bus(es) and Keypad bus are to shut down. The PCU shall provide at a minimum but not limited to, the following capabilities;

a. Expansion to a total of at least [10,000] [_____] user codes with [99] [_____] user profile definitions.

b. Shall support [4] [8] [16] [_____] keypads with alphanumeric display. Each keypad shall be capable of arming and disarming any system area based on a pass code or Proximity card and or key FOB authorization. The keypad alphanumeric display shall provide complete prompt messages during all stages of operation and system programming and display all relevant operating and test data.

c. Four [4] [_____] shift schedules per area.

d. A total of at least [100] [_____] programmable output relay schedules.

e. [32] [64] [_____] individual reporting areas.

f. Built-in bell and telephone line supervision.

g. Require two-man access code or credentials.

h. Support programming to require the same or different access code entered within a programmed delay time of 1 to 15 [_____] minutes after disarming before activating a silent ambush alarm.

i. Support area programming that disables schedule and time-of-day changes while system is armed so that area can only be disarmed during scheduled times.

j. There shall be a minimum of a [4,000] [_____] event log buffer per PCU. The log buffer shall be used to record and hold alarm activity information until the ESS is connected and receives the information. There shall be a software-configurable warning notification of log buffer filling for PCU(s) configured with modem capabilities.

k. Support a Network Interface Card (NIC) plug in module with built in network router capable of 128 Bit AES Rijndael Encryption process certified by NIST (National Institute of Standards and Technology).

2.3.5.2 Detection devices

Include full range of interior point protection sensors, volumetric (space) protection sensors, exterior fence sensors, and duress alarms. Duress alarms shall be [annunciated to be clearly distinguishable from other intrusion detection alarms] [silent at the reporting location and clearly distinguishable from other intrusion detection alarms] at the central reporting processor.

2.3.5.3 Tamper Switches

Enclosures, cabinets, housings, boxes, raceways, and fittings with hinged doors or removable covers which contain circuits of the intrusion detection system and associated power supplies shall be provided with cover having corrosion-resistant tamper switches. Arrange tamper switches to initiate an alarm signal when the door or cover is moved as little as 6 mm 1/4 inch from the normally closed position. Mechanically mount tamper switches to maximize defeat time when enclosure covers are opened or removed. Minimum amount of time required to depress or defeat the tamper switch after opening or removing the cover shall be one second. Enclosure and tamper switch shall prevent direct line of sight to internal components and prevent switch or circuit tampering. Conceal mounting hardware so switch cannot be observed from enclosure exterior. Covers of junction boxes provided to facilitate initial installation of the system need not be provided with tamper switches if covers contain no splices or connections. Tamper alarms shall be annunciated to be clearly distinguishable from intrusion detection alarms. Tamper switches on doors which must be opened to make normal maintenance adjustments to the system and to service power supplies shall be the push/pull-set, automatic-reset type. Tamper switches shall be:

a. Inaccessible until switch is activated;

b. Under electrical supervision at all times, irrespective of the protection mode in which the circuit is operating;

c. Spring-loaded and held in the closed position by the door, or cover protected;

d. Wired to break the circuit when the door or cover is disturbed; and

e. Wired so that each sensor and device is annunciated [individually] [by zone] at the central reporting processor.

2.3.5.4 Fail-Safe Capability

Provide fail-safe capability in critical elements of the ESS. This shall include, but not be limited to, capability to monitor communication link integrity and to provide self-test. When diminished functional capabilities are detected, system shall provide annunciation of the fault. Fail-safe alarms shall be annunciated to be clearly distinguishable from other types of alarms.

2.3.5.5 Line Fault Detection

As a minimum, fault isolation at the systems level shall have the same geographic resolution as provided for intrusion detection. Communication links of the ESS shall have an active mode for line fault detection. System shall be either a static, or dynamic system. In a static system, the "no-alarm" condition shall always be represented by the same signal, which shall be different than the signal originally transmitted. The dynamic system shall represent "no-alarm" with a signal which continually changes with time.

2.3.5.6 Power Loss Detection

Provide capability to detect when a critical component of the system experiences temporary or permanent loss of power and to declare an alarm. Alarm shall be annunciated to clearly identify the component experiencing power loss.

2.3.6 Manual and Self-Test

PCU shall have a provision that permits testing from any alphanumeric keypad. The test shall include standby battery, alarm bell or siren, and communication to the SCC. A provision for an automatic, daily, weekly, thirty (30) day, or up to sixty (60)day communication link test from the PCU installation site to the SCC. Include a provision for displaying the internal system power and wiring conditions. Internal monitors shall include the bell circuit, AC power, battery voltage level, charging voltage, panel box tamper, phone trouble line 1, phone trouble line 2, transmit trouble, and network trouble. A battery test shall be automatically performed to test the integrity of the standby battery. The test shall disconnect the standby battery from the charging circuit and place a load on the battery. This test shall be performed no more than every 180 seconds.

2.3.7 Electrical Power

Obtain by the normal commercial or base electrical distribution system. Power shall be continuously monitored and, if interrupted, automatic switching from primary to emergency backup sources shall be accomplished without interruption or degradation of critical system function. Intrusion alarms shall not be generated as a result of power switching; however, an indication of power switching and on-line source shall be provided at the alarm monitor. Upon restoration of prime power, system shall automatically switch back to the primary source. Failure of an on-line battery shall be detected and reported as a fault condition.

2.3.7.1 Primary Power

Furnish [120] [_____] volt ac service, transformed through a two-winding isolation transformer and rectified to low-voltage AC or DC for system operation. Obtain primary power [from the line side of incoming facility power] [at the location indicated]. Provide a separate, lockable, fused safety switch [adjacent to the power distribution panel] [at the location indicated].

2.3.7.2 Backup Power

Provide backup power to the primary power by [dedicated on-site diesel engine generator set (not a part of the ESS)] [backup battery in each element or subsystem as may be appropriate to provide a minimum of [4] [_____] hours of power] [uninterruptible power supply (UPS)].

a. UPS: Backup power required for uninterrupted operation of the ESS [until a diesel engine generator set can assume the full load] shall be provided by an uninterruptible power supply (UPS). The UPS shall consist of a rectifier, battery and support racks, a static inverter, static switch transfer, and a manual bypass switch. The UPS shall have a continuous output to supply the maximum load requirements of the ESS. Size battery to sustain the UPS at full rated load [for 4 hours] [for 15 minutes] [until diesel engine generator set can assume the load] [_____].

b. Batteries: Provide [further] backup by dedicated batteries in remotely located system elements such as individual sensors or control units. When radio frequency (RF) operation is required, batteries shall be an integral part of dispersed system elements. Batteries shall be capable of operation in any position and shall be protected against venting caustic chemicals or fumes within an equipment cabinet. Batteries shall be capable of continuous operation for up to [4] [_____] hours without recharge or replacement.

2.4 SYSTEM PERFORMANCE REQUIREMENTS

Design system components to operate as described herein within the context of the overall system performance previously described. Perceived inconsistencies between the following component performance specifications and overall system level performance descriptions shall be decided in favor of the former.

2.4.1 Modularity

Provide components designed for modular increase or decrease of system capability by installation or removal of plug-in modules. Design system

components to facilitate modular subassembly and part replacement.

2.4.2 Reliability

Provide only new components in current manufacturing production, manufactured to meet requirements specified herein, and free from characteristics and defects which affect appearance, or serviceability or render equipment unsuitable for the intended purpose. MTBF for component shall not be less than [5000] [_____] hours. [Provide only ESS components which meet requirements of DIA DCID 6/9.]

2.4.3 Maintainability

Components shall be capable of being maintained using commercially available standard tools and equipment. Components shall be arranged and assembled to be readily accessible to maintenance personnel without compromising defeat resistance of ESS.

2.4.4 Availability

Provide components designed for continuous operation. Provide solid-state electronic components, mounted on printed circuit boards conforming to UL 796. Boards shall be plug-in, quick-disconnect type. Circuitry shall not be so densely placed as to impede maintenance. Power-dissipating components shall incorporate safety margins of not less than 25 percent with respect to dissipation ratings, maximum voltages, and current-carrying capacity. Light duty relays and similar switching devices shall be solid-state type or hermetically sealed electromechanical. Electrical indicating instruments incorporated into system components shall conform to applicable provisions of ANSI C39.1.

2.4.5 Environmental Conditions

2.4.5.1 Interior Conditions

Equipment installed in environmentally protected interior areas shall meet performance requirements specified for the following ambient conditions:

a. Temperature: 0 to 50 degrees C 32 to 120 degrees F. Components installed in unheated security protected areas shall meet performance requirements for temperatures as low as minus 17 degrees C zero degrees F;

b. Pressure: Sea level to 4,573 meters 15,000 feet above sea level;

c. Relative humidity: 5 to 95 percent;

d. Fungus: Components shall be constructed of nonfungus nutrient materials or shall be treated to inhibit fungus growth; and

e. Acoustical noise: Components shall be suitable for use in high noise areas above 100 dB, such as boiler rooms, power plants, and foundries without adversely affecting their performance.

2.4.5.2 Exterior Conditions

Components mounted in locations exposed to weather shall be housed in corrosion-resistant enclosures with appropriate environmental protection. Component performance shall not degrade because of improper housing design.

Components in enclosures shall meet performance requirements when exposed to the following ambient conditions:

a. Temperature: Minus 32 to 60 degrees C Minus 25 to 140 degrees F;

b. Pressure: Sea level to 4,573 meters 15,000 feet above sea level;

c. Solar radiation: Six hours of solar radiation at dry bulb temperature of 60 degrees C 120 degrees F including 4 hours of solar radiation at 0.00112 watts per square millimeter 104 watts per square foot;

d. Sand and dust: Wind driven for up to [9.6] [_____] km per hour [6] [_____] miles per hour;

e. Rain: 50 mm 2 inches per hour and 125 mm 5 inchesper hour cyclic with wind plus one period of 300 mm 12 inches per hour;

f. Humidity: 5 to 95 percent;

g. Fungus: Warm, humid atmosphere conducive to the growth of heterotropic plants;

h. Salt fog: Salt atmosphere with 5 percent salinity;

i. Snow: Snow loading of 234 kg per square meter 48 pounds per square foot (psf) per hour; blowing snow of 22.5 kg per square meter 4.6 psf per hour;

j. Ice accretion: Up to 12.7 mm 1/2 inch of radial ice;

k. Wind: Up to 80 km/h 50 mph with gusts to 106 km/h 66 mph, except that fence sensors shall detect intrusions up to 56 km/h 35 mph; and

l. Acoustical noise: Components shall be suitable for use in high noise areas above 110 dB, such as flight lines, runup pads, and generator sites without adversely affecting their performance.

2.4.5.3 Transient voltage surge suppression

Intrusion detection, Automated Access Control, CCTV video circuitry, and communication circuits that lead to the SCC shall be protected at both ends against transient voltage surges. Transient voltage surge suppressors (TVSS) or surge protection devices (SPD) are required for the protection, within specified limits, of AC electrical circuits and electronic equipment from the effects of lightning induced voltages, external switching transients and internally generated switching transients. Individual suppressors shall be installed where shown on the drawings.

****

NOTE: Line Items a thru e should be part of building construction UFGS specifications.

****

a. Main service and distribution equipment suppressors: The AC voltage SPD's shall be a high speed, high current device designed to protect electrical systems and electronic equipment from transient over-voltage. The SPD shall provide continuous bi-polar, bi-directional, non-interrupting protection and be capable of instant reset with no degradation in protection. Gas tubes are not acceptable.

The SPD shall utilize SAD or MOV technology. It shall start to suppress at a minimum of 115 percent of the peak voltage of the sine wave. At maximum surge current dissipation, the device shall not exceed the maximum voltage protection level. The SPD shall be installed in parallel with the service main disconnect, distribution or branch panel main lugs as shown on drawings. Connect SPD to over current protection sized as shown with an AIC rating equal to panel rating. The suppressor shall have status indicator lights, dry contacts with remote alarm capabilities and an audible alarm. Suppressors shall be assembled as modular units to permit quick, easy replacement of failed components.

(1) Electrical Service

(a) Voltage shall be as indicated on drawings.
(b) Frequency -- 50/60 Hz
(c) Phases -- 3 phase
(d) Wiring configuration -- as indicated

(2) IEEE 62.41 Categories unless otherwise indicated on drawings:
Service entrance sizes

<600A	B3/C1
<600A to 1.2 KA	C2
>1.2KA	C3
Distribution or sub-panels	B2

(3) Electrical Performance
Response time < 5 nanoseconds
MCOV 115 percent minimum
Shortwave test- surge current
(6kv, 1.2/50usec; 3ka 8/20µsec) 5000 surges
Minimum surge current:

(a) Service Entrance 410,000 Amps/Phase
(b) Distribution and Sub-panels 210,000 Amps/Phase

(4) Suppression system protected modes shall be L-N, L-G, N-G for Wye Systems and L-L, L-G for ungrounded Delta Systems.

(5) Power on indicators and failure detection: A lighted panel on the cover shall provide indication that the suppressor is properly activated and shall also indicate mode failure. If the suppressor fails, an isolated contact shall close. In addition, an audible alarm shall be provided with manual reset.

(6) Failure mode - SPD's shall be designed to fail shorted. Any fuses in series with the SPD's shall not open during a surge event.

b. Disconnect: Main service suppressors shall be provided with an integral fused disconnect switch or dedicated circuit breaker as shown or required by UL. Breakers and suppressors shall have an AIC fault withstand rating equal or greater than the AIC rating of the equipment to which it is connected. The length of wiring from the tap at the service conductors to the suppressor being protected, however, shall not exceed the maximum length permitted by manufacturer, to maintain the maximum voltage protection level. Suppressors may be installed within switchgear or panel boards where UL label or listing is not affected, suppressors are completely and easily accessible, indicator lights are visible and audible alarm can be easily heard.

c. Enclosures: Enclosures for main service suppressors shall be as follows;

Minimum, 14 gauge painted steel or suitable enclosure to meet the NEMA selected requirements as listed.

d. Operation Status Indicator: Audible Remote Signaling and Visual Systems

(1) Visual System
(a) Protection: Suppressor Working - Green LED's
(b) Warning/Fault: Suppressor Failure - Red LED's
(c) LED's shall be field replaceable
(d) Other visual indicators where approved.

(2) Remote Signaling
Relay with Auxiliary for C contacts: Two sets at 2 ampere, 120 volts each. 1 Set N.O. and 1 set N.C. to operate upon failure of suppression module, blown fuse or tripped circuit breaker in suppressor module or in disconnect switch for alarm connection to remote location.

(3) Audible
The audible alarm shall activate upon a fault condition within the suppressor. An alarm silence/reset switch and push-to-test switch shall be provided.

e. Bonding and Grounding Conductors and Materials for Main Service Suppressors:

(1) Size: Conductors utilized for surge suppressor connections to service conductors shall be a minimum of #6 AWG stranded insulated copper unless otherwise specified.

(2) Bus: Ground bus or strip material where used shall be copper, a minimum of 1/4 inch thickness and two inches wide unless otherwise specified. Bus materials shall be secured to surfaces with appropriate insulators and mechanical fasteners. Bus connections shall be bolted and reinforced as necessary to provide a permanent and secure connection.

(3) Connections Compliance: Connectors, splices, and other fitting used to interconnect grounding conductors, bonding to equipment or ground bars, shall comply with requirements of the National Electric Code and be accepted by Underwriters' Laboratories for the purpose.

(4) Connectors: Connectors and fitting for grounding and bonding conductors shall be of the compression type in above grade locations. Connections below grade shall be exothermically welded.

(5) Dissimilar Materials: Bonding connections between electrically dissimilar metals shall be made using exothermic welds or using bi-metal connectors designed to prevent galvanic corrosion.

f. Communication Lines: The following standard for separately mounted telephone and signal line suppressors shall apply. All protectors shall be securely mounted at protected equipment location. All suppressors shall provide common (L-G) mode protection on all lines. Suppressors shall be tested in accordance with IEEE C62.36-1994 as a minimum. Protective interfacing with the telephone wire pairs shall be

listed to UL 497B.

g. Data Line Protection: Solid state, silicon avalanche diode or metal oxide varistor circuitry for protection from over voltages on long cable runs employing standard RS-232, RS422, or RS485. Appropriate connectors shall be utilized to interface a remote station with a host CPU.

h. Signal Line Protection: Solid state, silicon avalanche diode and metal oxide varistor hybrid circuitry for protection from over voltages on 2 or 4 wire signal lines such as balanced pair telephone, metallic pair telephone, buried and overhead field cable, remote radio equipment, and control systems. Unit shall have an LED diagnostic lamp that lights if unit needs replacement. Unit shall be listed UL 497B.

i. Modular, Twisted Pair Protection: Solid state, silicon avalanche diode or metal oxide varistor circuitry for protection from over voltages on twisted pair data or audio lines. Protectors shall clip mount on 66 punch down blocks furnished with grounding bar or studs and shall be totally enclosed. Units shall be securely mounted at terminal locations where shown and shall be grounded to the main building ground with a minimum No.12 stranded copper green insulated ground conductor kept as short as possible. Ground terminals shall be screw insertion lug type. No crimp, fork or ring type permitted. Unit shall have a multi-function diagnostic LED that shows continuity, ground present, unit function and line status.

j. Coaxial Cable Protectors: Solid state, silicon avalanche diode, metal oxide varistor and/or gas tube circuitry for non-interrupting over voltage protection of coaxial cable. Unit shall be provided with one female input connector and one female output connector. Securely mount adjacent to protection equipment and ground to equipment or local building ground if an equipment ground is not available.

2.4.6 Electromagnetic Interference (EMI)

ESS components employing electromagnetic radiation shall be designed and constructed to provide maximum practical invulnerability to electronic countermeasures.

2.4.7 Electromagnetic Radiation (EMR)

****

NOTE: National Post Telephone and Telegraph is normally the approving authority for EMR components overseas.

****

Provide only ESS communication components which are [Federal Communications Commission (FCC)] [_____] licensed and approved. Provide system components which are electromagnetically compatible.

2.4.8 Interchangeability

Like components shall be physically and functionally interchangeable as complete items, without modification of either the original items or of other components with which the items are used.

2.4.9 Safety

ESS components shall conform to application rules and requirements of NFPA 70 and applicable UL publications.

2.4.10 Human Engineering

Displays, other than wall-mount LCD, Plasma or DLP displays, shall be housed in standard [desk-type consoles] [480 mm 19 inch racks]. Central alarm reporting and display shall be designed for operation by one or more individual(s). Aural considerations shall include location of annunciators, tone pitch, quality, and intensity. Number of different audible signals shall not exceed four. Component design shall provide for ease of accessibility for maintenance.

2.4.10.1 Visual Annunciators

Annunciators shall be either liquid crystal displays (LCDs), Plasma Display, DLP projection Display or light emitting diodes (LEDs). Annunciators shall be so connected in the circuit that a failure of the annunciator, socket, or protective circuitry shall not result in an improper or indeterminate signal. LCD Displays, Plasma Display, DLP projection Display and LEDs shall be compatible with standby power supplies. LCDs shall be back-lit with a minimum 800:1 contrast ratio. Plasma and DLP projection shall produce no less than a 3000:1 Contrast ratio.LEDs shall be brightly lit and visible from a distance of 9 meters 30 feet in an area illuminated at 805 lux 75 footcandles. Use LEDs in outdoor applications or in the presence of sunlight. Signals shall be clearly visible from a distance of 9 meters 30 feet in an area illuminated at 805 lux 75 footcandles. LCDs and LEDs shall be used for remote display to provide status indications within a secured area. LCDs, Plasma Displays and DLP projection Displays shall be used in Central monitoring Stations and interfaced to the ESS Servers, and workstations.

2.4.10.2 Controls

Provide to ensure ease of operation of specified characteristics. Where applicable, clockwise rotation of controls shall result in an increasing function. Controls, switches, visual signals and indicating devices, input and output connectors, terminals, and test points shall be clearly marked or labeled on the hardware to permit quick identification, intended use, and location. Terminal markings and labels shall be of a permanent and legible type and located to be visible when associated system wiring is in place. Identification markings shall be associated with each adjustment device or item requiring periodic maintenance. Safety warning or cautions shall be marked in conspicuous red letters. Control and indicator identifications that are exposed outside enclosures shall be permanent, machine-engraved letters, painted to contrast with background color. Controls not required for system operation shall be inaccessible to the system operator.

2.4.11 Computer Software

Software shall be comprised of computer programs and computer data bases as required. Software shall be categorized as mission software and support software.

2.4.11.1 Mission Software

Mission software shall consist of software implemented to provide complete operation of the ESS.

2.4.11.2 Support Software

Support software shall consist of software implemented to support system operation, such as system setup and off-line maintenance routines.

2.4.11.3 Software Performance Requirements

Provide software in modules to meet application requirements of this section. Software shall include the operating system (OS), be complete off-the-shelf, modifiable for specific ESS application specified herein, and be a product of and supported by the ESS central processor manufacturer. OS executive shall accomplish in real time the scheduling and sequencing of programs for execution. Each program shall be assigned a priority level. Provide priority levels in sufficient number to provide total functional operation as specified. Software shall be menu-driven. Menu, reconfiguration, and other actions which could in any way compromise the security and integrity of the ESS shall be password controlled. A minimum of [eight] [_____] password levels shall be provided. Software provided shall be documented in a user's manual which shall be approved by the Government prior to system implementation.

2.4.12 Test Points

Test points, controls, and other adjustments inside enclosures shall be readily visible and accessible with minimum disassembly of equipment. Test points and other maintenance controls shall not be readily accessible to operator personnel.

2.4.13 Component Enclosures

Consoles, annunciator housings, power supply enclosures, sensor control and terminal cabinets, control units, wiring gutters, and other component housings, collectively referred to as enclosures, shall be formed and assembled to be sturdy and rigid.

2.4.13.1 Metal Thickness

Thicknesses of metal in cast and sheet metal enclosures of all types shall be not less than those listed in Tables 8.1, 8.2, and 8.3 of UL 1610for alarm components, and NEMA ICS 2 and NEMA ICS 6 for other enclosures. Sheet steel used in fabrication of enclosures shall be not less than 16 gage, except consoles may be 18 gage.

2.4.13.2 Doors and Covers

Doors and covers shall be flanged. Where doors are mounted on hinges with exposed pins, the hinges shall be of the tight pin type, or the ends of hinge pins shall be tack welded to prevent ready removal. Provide doors having a latch edge length of less than 600 mm 24 inches with a single lock. Where latch edge of a hinged door is 600 mm 24 inchesor more in length, provide the door with a three-point latching device with lock; or alternatively with two locks, one located near each end. Covers of junction boxes provided to facilitate initial installation of the system shall be held in place by tack welding, brazing, or one-way screws.

2.4.13.3 Ventilation

Ventilation openings in enclosures and cabinets shall conform to requirements of UL 1610.

2.4.13.4 Mounting

Unless otherwise indicated, sheet metal enclosures shall be designed for wall mounting with top hole slotted. Mounting holes shall be in positions which remain accessible when major operating components are in place and door is open, but shall be inaccessible when door is closed.

2.4.13.5 Labels

Labels shall be affixed to such boxes indicating they contain no connections. These labels shall not indicate that the box is part of the intrusion detection system.

2.4.13.6 Enclosure Locks

Locks and key-lock-operated switches required to be installed on component enclosures shall be UL listed, round-key type with three dual, one mushroom, and three plain pin tumblers, or shall have a pick resistance equal to a lock having a combination of five cylinder pin and five-point three-position side bar in the same lock. Keys shall be stamped "U.S. GOVT. DO NOT DUP." Key-lock-operated switches shall be keyed differently and shall be two-position, with the key retractable from either position. Furnish two keys for each switch. Maintenance locks shall be of the one-way key-pull type arranged so that the key can be withdrawn only when the lock is in the locked position. Locks on components for maintenance access shall be keyed alike; only two keys shall be furnished for such locks. Deliver keys, tagged with metal tags, accompanied by a manufacturer's certificate which records the number of each key made.

2.4.14 Detection Sensors

Sensors shall detect penetration of the facility perimeter and protected zones by unauthorized personnel or intruders with a probability of detection (pd) of 0.9 with a 95 percent confidence level and, as applicable, shall conform to UL 639. Unless otherwise specified, required sensor power is plus 12 volts dc.

2.4.14.1 Interior Point Sensors

****

NOTE: Balanced magnetic switches (BMS) as specified in (a), (b) and (c) are for High security applications, refer to DCID 6/9. Use of recessed BMS is recommended during new installations. For non-high security applications, the use of magnetic switches is recommended as specified in (d). Coordinate with Architect to ensure proper door hardware (elect strike, hinges, etc.) are provided.

****

a. Door and window protection: Accomplish by one or more of the following:

(1) Magnetic Switches: Magnetic switches shall be [surface mounted],

[recessed], [_____]. Magnetic switches shall have a magnetic field with a high probability of alarm if an external magnet is introduced in defeat attempts. Provide each magnetic switch with an overcurrent protective device, rated to limit current to 80 percent of switch capacity. The magnetic switch housing shall be protected from unauthorized access by encapsulating reed switches in a polyurethane potting compound. Magnetic switch shall be rated for a minimum lifetime of one million operations. House magnetic switch components in enclosures made of nonferrous materials. Balanced Magnetic Switches shall be used for high security application and Standard Magnetic switches for all other applications

(a) Balanced magnetic switches (BMS): Switches shall be [surface mounted] [and] [recessed] [as indicated] and shall have a minimum of three encapsulated reed switches. Switches shall activate when a disturbance in the balanced magnetic field occurs. Provide each BMS with an overcurrent protective device, rated to limit current to 80 percent of the switch capacity. BMS shall be rated for a minimum lifetime of one million operations. House the BMS components in nonferrous enclosure materials.

(b) Surface mount BMS: House components used in outdoor applications in weatherproof enclosures. Switch mechanism shall be internally adjustable so the operating gap between faces of the switch housing and the magnet housing may be adjusted from 6 to [13] [50] mm 1/4 to [1/2] [2] inch[es] to accommodate installation variances. Surface mount BMS housing for the switch element shall have the capability to receive threaded conduit. Housing cover for surface mounted BMS, if made of cast aluminum, shall be secured by stainless steel screws. Magnet housing cover shall not be readily removable. Protect BMS housing from unauthorized access by a cover operated, corrosion-resistant tamper device. Device shall initiate an alarm when cover is opened as little as 3 mm 1/8 inch and shall be inaccessible until actuated. BMS shall have a minimum of three preadjusted reed switches and three preadjusted magnets. Field adjustments in the fixed space between magnet and switch housing shall not be possible. Attempts to adjust or disturb the magnetic field shall cause a tamper alarm. [Conductors running from the door to alarm circuits shall be jumpered within a flexible armored cord constructed from corrosion-resistant metal. Each end of the armored cord shall terminate in a junction box or other enclosure. Armored cord ends shall be mechanically secured to the junction boxes by clamps or bushings. Conductors within the armored cord shall be provided with lug terminals at each end. Jumpered conductors and the armored cord shall experience no mechanical strain as the door is removed from fully open to closed. Switch circuit shall initiate an alarm if a short circuit is applied to the door cord.]

****

NOTE: Regarding the text below, show a junction box above each door so that slack in conductors serving switches cannot be accessed when switch mounting screws are removed. If building construction does not permit junction box location above doors, specify switches to be epoxy glued in place after preliminary testing.

****

(c) Recessed BMS: The recessed BMS shall have a minimum three preadjusted reed switches and [two] [three] preadjusted magnets. Field adjustments in the fixed space between magnet and switch housing shall not be possible. Attempts to adjust or disturb the magnetic field shall cause a tamper alarm. [Ball bearing door trips shall be mounted within vault door headers such that when the locking mechanism is secured, the door bolt engages an actuator, mechanically closing the switch. Door bolt locking mechanism shall be completely engaged before the ball bearing door trip is activated. Provide circuit jumpers from the door.]

(d) Standard magnetic switch: The magnetic switch shall be of the design specifically for use in either steel or wooden doors commonly found in commercial building applications. The magnetic switch shall allow for flush recessed or surface mounting. The magnetic switch shall allow for a gap distance not less than 6 to [13] [50] mm 1/4 to [1/2] [2] inch[es] when installed in metal or wood framed door(s).

(2) Glass breakage detection: Glassbreak sensors shall be [Glass Mounted], [Wall Mounted], [Ceiling Mounted], [_____]. Sensors shall detect window breakage by responding to acoustic or vibration frequencies that accompany breaking glass. Sensors shall selectively filter input to minimize false alarms.

(a) Window Mounted Glassbreak Sensor: Sensors shall detect window breakage by responding to acoustic or vibration frequencies that accompany breaking glass. Sensors shall selectively filter input to minimize false alarms. Sensors shall be contained in a fire-resistant ABS plastic housing and shall be mounted in contact with the window. Glass breakage sensors shall initiate alarm when glass they protect is cracked or broken. Sensing shall be accomplished through the use of a mechanical filtered piezoelectric element. Sensor shall have a sensitivity adjustment controlling output voltage from the piezoelectric element which triggers a solid-state latching device. Provide sensor with an LED for adjusting sensitivity. Supply sensor with a two-sided polyurethane tape with acrylic adhesive. Provide sensor with an exterior label to protect tape from direct sunlight. Sensor shall not initiate alarm in response to seismic vibrations or other ambient stimuli. [Test glass breakage sensors by using test units supplied by the manufacturer which simulate glass breakage.]

(b) Ceiling or Wall Mounted Dual technology glassbreak sensor: Sensor shall detect window breakage by responding to acoustic frequencies that accompany breaking glass. The sensor shall be combined with a passive infrared motion detector (PIR) for the purpose of eliminating occupant-generated false alarms. It will extend coverage to occupied areas, allowing the sensors to be armed while people are present.

(c) Ceiling or Wall Mounted Recessed glassbreak sensor: A recessed glassbreak sensor is to be used when appearance is a consideration. Recessed models can be mounted directly to the wall or ceiling or can be installed on a single gang box. The sensor shall employ pattern recognition technology that listens for the actual pattern of breaking glass. The sensor shall be able to detect the difference from breaking glass and normal room sounds

by listening across the glassbreak frequency spectrum. The sensor shall provide a 7.6 meters 25 feet 360 degree coverage of the area to be protected.

b. Object Protection

(1) Capacitance proximity sensor: Capacitance proximity sensor shall detect changes in the established capacitance to ground of a protected object. When the protected object is touched and a ± 20 pf - (variable) change in the capacitance is detected an alarm shall be generated. Circuits measure the ratio between the charging current and the resultant rate of change of voltage with time. Sensor shall protect objects up to a [50,000] [_____] picofarad capacitive load. System shall provide means of indicating an alarm condition at protected objects during installation and calibration. Provide indicator with a disabling device within a tamperproof enclosure. The number of objects protected by a single capacitance detector shall not exceed the unit's maximum capacitance at the desired sensitivity. Protected objects shall be insulated from ground by insulating pads which shall have a dielectric constant such as glass or thermoplastic materials. [If screen grids or radiators are employed as antennas, they shall be insulated from ground. Wires used for grid shall be larger than No. 14 AWG, 30 percent copper-clad steel covered with a minimum of 0.794 mm 1/32-inchvinyl coating. Space grid elements at 150 mm 6 inchesmaximum, and construct in a symmetrical manner.] Provide sensor with sensitivity controls inaccessible to operating personnel. Sensor shall be insensitive to human body movements in excess of 915 mm 36 inches from the antenna circuit. Sensor sensitivity to alarm-producing stimuli shall be readily adjustable from contact to 915 mm 36 inches with a heavily gloved hand. Sensor shall not initiate nuisance alarms in response to normal ambient conditions. [Provide sensors with tamper switches. Constantly supervise interconnecting lines and tamper switches even when system is set for authorized access.] Sensor shall not reset upon restoration of SECURE mode if antennas were altered during authorized entry to disable detection capability.

(2) Vibration vault sensor: Sensor shall sense short duration, large amplitude signals like those produced in attacks from explosions, hammering or chiseling. It shall also detect long duration, small amplitude signals like those produced in attacks from torches, thermic lances, drills, grinders or cutting discs. The sensor enclosure base shall be constructed of die-cast aluminum with a stamped 22 gauge steel cover.

c. Floor, wall, and ceiling protection

(1) Vibration sensors: Sensors shall sense and selectively amplify signals generated by forced penetration of a protective structure. Sensors shall initiate alarms upon detecting drilling, cutting, or other methods of forced entry through a structure. Mount vibration sensors directly contacting the surface to be protected. Sensors shall be designed to give peak response to structurally conveyed vibrations associated with forcible attack on the protected surface. Provide [1] [_____]sensor(s) on each monolithic slab or wall section, even though spacing closer than that required for midrange sensitivity may result. House sensors

in protective mountings and fasten to surface with concealed mounting screws or an epoxy. [Provide sensors with tamper switches.] Removal of a sensor from the surface shall initiate an alarm. An adjustable alarm discriminator shall function to prevent incidental vibrations which may occur from triggering the alarm circuit. Adjust discriminator on the job to precise needs of application. Connect sensors to an electronic control unit by means of wiring or fiber optics cable run in [rigid steel conduit] [electrical metallic tubing (EMT)]. Sensor sensitivity shall be individually adjustable unless sensor is designed to accommodate vibration ranges of specific surface type on which it will be mounted. Sensitivity adjustments shall not be accessible without removing the sensor cover. Sensor shall not be responsive to airborne sound.

(2) Fiber Optic mesh sensors: Provide fiber optic woven nets which form an alarmed sensor barrier in walls, doors, floor or ceiling. Fiber optic mesh sensors are made up of a web of optical fiber cables which are deployed within building walls, stores, partitions or mobile container shells. External applications for fiber optic mesh sensors, configured from an appropriate form of fibre-optic cable, include attachment to flexible structures, water-side installations and mobile facilities.

****

NOTE: Utility inlet openings are protected in a variety of methods, the correct one being dependent on two variables: the nature of the intrusion threat (i.e., physical penetration, electrical, electro-optical, etc.) and the characteristics of the utility inlet opening (i.e., discharge water from a nuclear plant, office air duct, electric conduit, etc.). Subsequent to such analysis, almost any of the intrusion detection sensors described herein could provide the necessary protection. Normally a breakwire trap sensor is used for this application.

****

(3) Protection of utility inlet openings: Provide protection by a sensor of the [breakwire] [wire trap] type consisting of up to 26 AWG hard-drawn copper wire with a tensile strength of 17.8 N 4 pounds maximum interlaced throughout the opening such that no opening between wires shall be larger than 100 mm 4 inches on center. Terminate sensor so that attempts to cut the wire or otherwise enlarge openings between wires shall cause an alarm. Sensor termination shall be [concealed] [tamper protected].

2.4.14.2 Interior Volumetric Sensors

a. Passive infrared sensors: Sensors shall detect intruder presence by monitoring the level of infrared energy emitted by objects within a protected zone. Sensor shall initiate an alarm upon observing increased or fluctuating infrared energy caused by the presence and motion of an intruder whose temperature is as little as 1 1/2 degrees C 3 degrees F different from the background temperature. Sensor shall be passive in nature; no transmitted energy shall be required for detection. Sensor shall be sensitive to infrared energy emitted at wavelengths corresponding to human body and other objects at ambient

temperatures. Sensor detection pattern shall be 3.14 rad 180 degrees for volumetric units, unless otherwise indicated[, and shall be housed in a tamper-alarmed enclosure]. Sensor shall provide some means of indicating an alarm condition during installation and calibration. A means of disabling the indication shall be provided within the sensor enclosure. Sensor shall alarm when an intruder moves within the area of protection more than 1500 mm 5 feet at a velocity of 30 mm 0.1 foot per second, and one step per second, assuming 150 mm 6 inchesper step. Detection sensitivity shall be irrespective of direction of motion. Sensor shall also alarm at velocities faster than 30 mm 0.1 foot per second, up to 3000 mm 10 feetper second. Sensor maximum detection range shall be [a minimum of 10.6 meters 35 feet] [as indicated]. Sensor shall not alarm in response to general area thermal variations.

b. Dual technology sensors: Provide sensor combining passive infrared and microwave sensors designed and manufactured specifically to be mounted in a single enclosure.

(1) Passive infrared (PIR) sensor section: Sensor shall detect intruder presence by monitoring the level of infrared energy emitted by objects within a protected zone. Sensor shall initiate an alarm upon observing increased or fluctuating infrared energy caused by the presence and motion of an intruder whose temperature is as little as 1.5 degrees C 3 degrees F different from the background temperature. Sensor shall be passive in nature; no transmitting energy shall be required for detection. Sensor shall be sensitive to infrared energy emitted at wavelengths corresponding to human body or other objects at ambient temperatures. Sensor detection pattern shall be 3.14 rad 180 degrees for volumetric units, unless otherwise indicated.

(2) Microwave sensor section: Sensor shall detect intruder presence by transmitting electromagnetic energy into a protected zone, receiving the direct and reflected energy, and monitoring the frequency shift between transmitted and received signals. If more than one device is used in an area, devices shall operate on different frequencies. Provide for selective filtering by sensor to minimize nuisance alarms due to moving metal objects such as fan blades and venetian blinds, interference from radar, or other sources of electronic interference. Transceivers shall consist of a combined transmit/receive antenna and an adjustable-gain preamplifier in a single housing. Provide transceivers with sensitivity adjustments. Transceiver controls shall permit adjustment of transmission range and alarm signal threshold. Sensitivity controls shall be inaccessible to operating personnel. Sensitivity requirements shall be met with sensitivity controls set approximately at midrange.

(3) Additional dual technology sensor requirements: Enclosure containing the two sensor sections shall be tamper alarmed. Both the microwave and PIR sections shall activate simultaneously to generate an alarm. Only an intrusion characterized by volumetric motion and radiant body heat shall be detected. Sensor shall provide a means of indicating an alarm condition during installation and calibration. A means of disabling the indication shall be provided within the sensor enclosure. Sensor shall alarm when an intruder moves within the area of protection more than 1500 mm 5 feetat a velocity of 30 mm 0.1 foot per second, and one step per second, assuming 150 mm 6 inches per step. Detection

sensitivity shall be irrespective of direction of motion. Sensor shall also alarm at velocities faster than 30 mm 0.1 foot per second, up to 3000 mm 10 feet per second. Sensor shall not alarm in response to general area thermal variations. Mount sensors [near ceiling on vibration-free surfaces] [as indicated]. Electronic circuitry shall be solid state and mounted on printed circuit boards. Sensor elements shall contain circuitry for transmitter drive, signal processing, tamper circuitry, and power supplies. Circuitry shall provide an alarm relay with Form C contacts capable of carrying 2 amperes at 100 volts dc minimum.

c. Microwave sensors: Sensors shall detect intruder presence by transmitting electromagnetic energy into a protected zone, receiving direct and reflected energy, and monitoring frequency shift between transmitted and received signals. When more than one device is used in an area, devices shall operate on different frequencies. Provide for selective filtering by the sensor to minimize nuisance alarms due to moving metal objects such as fan blades, and venetian blinds, interference from radar, or other sources of electronic interference. Provide a means of indicating an alarm condition on the sensor at the protected zone during installation and calibration. Provide an indicator disabling device within sensor enclosure. Transceivers shall consist of a transmitting antenna and a receiving antenna, or a combined transmit/receive antenna, and an adjustable-gain preamplifier in a single housing. Provide transceivers with sensitivity adjustments. Transceiver controls shall permit adjustment of transmission range and alarm signal threshold. Sensitivity controls shall be inaccessible to operating personnel. Sensitivity requirements shall be met with sensitivity controls set approximately at midrange. System shall alarm when an intruder moves within the area of protection more than 1500 mm 5 feet at a velocity of 30 mm 0.1 foot per second and one step per second, assuming 150 mm 6 inches per step. Sensitivity shall be irrespective of direction of motion. Sensor shall be [installed to be self-protecting] [housed in a tamper-alarmed enclosure]. The number of transceivers chosen shall be adequate to completely cover the protected zone. In the event that dead spots cannot be overcome by adding sensors, the use of a different type sensor shall be employed. Power output from each transceiver shall be minimum level required for stable operation and adequate sensitivity. Maximum power density radiated from transmitters shall not exceed 0.2 mW per square centimeter at 30 meters 100 feet. Frequency of emissions and allowable power densities for each shall be governed by FCC 47 CFR 15. Mount transmitters near ceiling on vibration-free surfaces. Electronic circuitry shall be solid state, mounted on printed circuit boards. Sensor elements shall contain circuitry for transmitter drive, signal processing [, tamper circuitry,] and power supplies. Circuitry shall provide an alarm relay with contacts capable of carrying 2 amperes at 120 volts ac minimum.

d. Range Controlled Radar (RCR) sensor: Sensor shall detect intruder presence by transmitting radar signals that ping the coverage area then bounce back to the sensor on the same path. The sensor technology shall provide for longer-range applications, eliminating false alarms through exact control of the monitored space. The sensor shall allow the Installer to select the range (6, 9, 12, 15 meters) (20, 30, 40, 50 feet) to be protected with a jumper switch. Nothing beyond that range will cause a false alarm, and the measured radar signals shall distinguish and ignore signal reflections within the defined range. The sensor shall have a tamper and a Form C relay and can be used for

applications where longer range is required.

e. Audio sensors: Sensors shall consist of microphones which detect audio information and transmit signals to an audio amplifier in a central control unit. Multiple units may be connected to a central control unit. Audio sensors shall be designed to be especially sensitive to generic audio intrusion signature of [breaking glass] [splintering wood] [fracturing of cement block] [normal voice conversation]. Sensors shall have sensitivity adjustments which shall be inaccessible to operating personnel. Sensitivity adjustment shall permit operating ranges up to a maximum of [465] [_____] square meters [5000] [_____] square feet. Sensors shall have a detection sensitivity of [unidirectional design] [omnidirectional design]. [Audio assessment capability shall be provided.] Sensors shall be capable of installation in a concealed configuration and shall be inherently self-protecting.

f. Photoelectric sensors: Sensors shall detect intruder presence by establishing a series of infrared or ultraviolet beams and detecting beam disruptions. Beam transmitters shall be designed to emit [no perceptible] light. Beam may be reflected by one or more mirrors before being received and amplified. Disruption of the beam by an opaque body shall initiate an alarm. Transmitted beam shall be uniquely modulated to prohibit an intruder from shining another light source into the receiver to escape detection. Provide a means of local alarm indication on the sensor for use at the protected zone during installation and calibration. Provide with an indicator disabling device within the sensor enclosure. Sensor shall consist of modulating transmitter, focusing lenses, mirrors, demodulating receiver, power supply, and interconnecting lines. House elements in tamper-alarmed enclosure. Receiver unit shall provide an alarm relay with contacts capable of carrying 2 amperes at 120 volts ac minimum. Protective beam shall be focused in a straight line. Installed beam distance from transmitter to receiver shall not exceed 80 percent of the manufacturer's maximum recommended rating. Mirrors may be used to extend the beam or to establish a network of beams. Each mirror used shall derate the maximum system range by no more than 50 percent. Mirrors and photoelectric sources used in outdoor applications shall have self-heating capability to eliminate condensation and shall be housed in weatherproof enclosures. System shall utilize automatic gain control or be provided with sensitivity adjustments to allow for various beam lengths. Controls shall be inaccessible to operating personnel. With controls set at approximately midrange, system shall initiate an alarm when the beam is interrupted. Test system by walking through the beam. Systems that use multiple beams to establish a fence shall be tested by attempting to crawl under and jump through and over beams. Systems shall provide cutoffs of at least [90] [_____] percent to handle a high percentage of light cutoff prior to initiating an alarm.

****

NOTE: At the text below, the number of pixels digitized depends on the application. The designer should consider cost effectiveness as a factor since digitizing a large number of pixels could increase cost by a magnitude of 500 percent with little additional actual detection capability for a specific application.

****

g. Video motion detection System (VMD): Video motion detection capabilities range from basic activity detection to the search through massive databases to pre-empt serious incidents. VMD capabilities have become a standard feature of common DVR's. VMD algorithms are a software function, they are programmed into chips and boards that can be installed in IP cameras, stand-alone modules, digital video recorders and dedicated computer processors. VMD is also available as software for installation in off-the-shelf computers. The complexity of these products varies greatly. The IP cameras provide a separate output on basic activity detection, while the PC-based software and modules provide graphic identification of the identified movement, user-selectable monitored areas, compensation for environmental movement, and a host of other features.

(1) Basic motion detection: Basic motion Detection typically recognizes any type of motion in the video field. A single output then activates automatic call-up to the monitor screens of surveillance personnel or initiates automatic DVR recording. The video call-up is no longer limited to cabled CCTV systems, but can be transmitted via the network LAN or WAN. Many basic DVRs can search and retrieve records of movement or activity on their stored hard drives. These features are often found on off-the-shelf equipment, are economical, and have limited applications.

(2) Advanced VMD: Advanced VMD products enhance the concepts of basic motion detection and can, when properly applied and operated, provide innovative, effective solutions to security issues. Most of these features result from elaborate algorithms that search out detailed movement patterns and only activate a system response under very specific conditions. Capabilities include:

a. Intruder Identification: Identifying unauthorized humans in specified areas of the field of view.

b. Environmental Compensation: Recognizing and ignoring wind-blown debris, animals, background traffic, etc.

c. Counting: Recognizing a quantity of a particular object moving or activity performed.

d. Directional Identification: Ignoring objects moving in one direction, while alarming for objects moving in unauthorized directions.

e. Item Recognition: Activating when specific user-selected items are removed from, placed in, or passed through the field of view.

f. Subject Tracking: Highlighting and following a specific person or item as it moves about the field of view, or from the field of view of one camera to another.

g. Multiple Subject Tracking: Highlighting and following multiple persons or items simultaneously as they move about the field of view, or from the field of view of one camera to another.

2.4.14.3 Exterior Fence and Perimeter Sensors

a. Fiber Optic Fence Sensors: Sensors shall initiate an alarm when an intruder attempts scaling, cutting through or attempting to lift the fabric of a standard chain link fence or physical barrier. The sensor shall comprise of a weft-knitted single tactical fiber-optic cable structure, mounted under tension between upper and lower galvanized conduits, and also tensioned to the horizontal direction of the fence. The net is to be made of a fiber-optic cable formed into squares of16 by 16 cm 6.5 by 6.5 inches, which are crossed at each joint by a plastic crossover button bonded by ultra-sonic welding. Infrared light is pulsed through the fiber net. The upper part of the fence shall incorporate transducers and a tensioned heavy-duty fiber-optic cable, which is stretched between the transducers and inserted through the upper loops of the fiber-optic net. The upper part of the fence shall rest upon flexible fiberglass rods installed 2 meters 6 feet apart assuring structural flexibility. The folding fiber net can be attached parallel to a variety of existing perimeter barriers or installed as a free standing intruder detection system.

b. Electromechanical fence sensors: Sensors shall detect human presence by sensing mechanical vibrations or motion associated with an intruder scaling, cutting through a standard security chain link fence, or attempting to lift the fence fabric. Sensor shall fully protect fence installation. Dead zones shall not exist where an intruder can scale the fence or cut through the fence without detection. Length of fence protected shall be divided into [100 meter] [_____] zones. Sensors shall consist of individually electromechanical sensing units mounted every 3045 mm 10 feet on the fence [fabric] [posts] and shall be wired in series to a sensor zone control unit and associated power supply. Sensor zone control unit shall alarm when a sufficient number of sensing unit activations are sensed within a specified time period. Alarm threshold shall be field adjustable by zone and shall [in combination with adjustments to individual sensing units] permit compensation for winds up to [40] [56] [_____] km/h [25] [35] [_____] mph without increased nuisance alarms while maintaining specified sensor performance. With sensitivity controls set at approximately midrange, sensor shall alarm when an intruder attempts to scale the fence or to climb undetected in areas of reduced sensitivity, such as around poles and rigid supports. Sensor shall alarm for attempted fence liftings or scalings, including scalings assisted by climbing aids leaned against the fence. Sensors shall allow gradual changes in fence position, due to expansion, settling, and aging, without increased numbers of nuisance alarms. Sensors shall be either tamper alarmed or self-protecting. Exterior components shall be housed in rugged, corrosion-resistant enclosures, protected from environmental degradation. Provide sensor zone control unit housings with tamper alarms. Fence cable support hardware shall be weather-resistant. Interfacing between sensor zones and alarm annunciators shall be carried in underground cables.

c. Strain-sensitive cable sensors: Sensors shall detect movement on a standard security chain link fence associated with an intruder scaling, cutting through, or attempting to lift the fence fabric. Entire sensor system, including sensor zone electronics, shall be capable of mounting directly on the fence and exposed to the same environmental conditions as the fence. Length of fence protected shall have no dead zones where an intruder can penetrate the fence, and through sensor electronics, shall be divided into [100 meter] [_____] zones. Sensing unit of

sensor shall consist of transducer cable capable of achieving specified performance either by attachment directly to the fence fabric by plastic cable every 300 to 455 mm 12 to 18 inches or by installation inside EMT conduit mounted on the fence. Sensing unit shall have equal adjustable sensitivity throughout the entire length. To permit installation in extreme EMI environments with no loss of detection capability, only conventional waterproof coaxial cable connectors shall be used for connections of the sensing unit. Entire sensor system shall be capable of detecting tampering within each portion of the system by sensor zone. Sensor zone electronic circuitry shall provide capability for alarm threshold sensitivity adjustment to permit compensation by zone for winds up to [40] [56] [_____] km/h [25] [35] [_____] mph while maintaining the same level of detection performance as under ambient conditions. Sensor zone control unit shall provide an analog audio output for interface to an external audio amplifier to permit remote audio assessment regardless of sensor alarm status. Sensor zone control unit alarm output interface shall be a separately supervised relay contact normally open or normally closed, with [an adjustable intrusion alarm pulse width of 0.5 second adjustable and a] continuous (until corrected) tamper alarm.

d. Electrostatic field sensors: Sensors shall initiate an alarm when an intruder attempts to approach or scale a fence or physical barrier. Electrostatic field sensors shall detect human presence by generating an electric field around one or more horizontal wires and sensing the induced signal in parallel sensing wires. Sensor shall monitor the induced signal for changes that result from the presence of a conductive body, or a body with a high dielectric constant such as the human body, which distorts coupling between transmitting and sensor wires. Sensor components shall consist of one or more signal generator field wires and mounting hardware, sensing wires, an amplifier/signal processor, power supplies, and necessary circuitry hardware. Mounting and support hardware shall be provided by the equipment manufacturer. Wires shall be spring tension-mounted and provided with end-of-line terminators to detect cutting, shorting, or breaking of the wires. Sensor configuration shall be selected such that an intruder cannot crawl under the bottom wire, through the wires, or over the top wire without being detected and shall be divided into sensor zones. Sensors shall be capable of following irregular contours and barrier bends without degrading sensitivity below the specified detection level. In no case shall a single sensor zone exceed 100 meters or be long enough to significantly degrade sensitivity. Adjacent zones shall provide continuous coverage to avoid a dead zone. Adjacent zones shall be designed to prevent crosstalk interference. Signal processing circuitry shall provide filtering to distinguish nuisance alarms. Sensor configuration shall incorporate balanced, opposed field construction to eliminate far field noise. Exterior components shall be housed in rugged corrosion-resistant enclosures, protected from environmental degradation. Provide housing with tamper switches. Interfacing between exterior units shall be carried in underground cables. Exterior support hardware shall be stainless or galvanized to avoid tension degradation in the physical support system. Sense and field wires shall be stainless steel. Wire spacing for various configurations shall follow manufacturer's specifications. Spacing of wires shall be maintained constant throughout each zone and shall be uniform with respect to the ground. Signal processing equipment shall be separately mounted such that no desensitized zones are created within the zone of detection. Sensor sensitivity shall be adjustable. Adjustment controls shall be inaccessible to operating personnel. With

system sensitivity controls set at approximately midrange, system shall alarm when an intruder is within 915 mm 3 feet of a wire. Sensitivity shall be irrespective of direction of motion, or velocity in the range of 30 mm to 3000 mm 0.1 foot to 10 feet per second. Sensor shall detect intruder attempts to cross potential dead zones, such as between adjacent zones or in the vicinity of posts with the minimum specified performance or better. Sensor shall provide some means of indicating an alarm at the protected perimeter to facilitate installation and calibration. Provide an indicator disabling device within a tamperproof enclosure. Power required shall be 120 volts ac.

e. Taut-wire sensors: Sensors shall consist of a perimeter intrusion detection sensor incorporated into a barbed wire security fence. Intrusion detection shall be achieved by cutting of any single wire or the deflecting, as by climbing, of any wire by more than [_____]. Sensor zone shall include one or more [61] [_____] meters [200] [_____] foot maximum sections of [2100] [_____] mm [7] [_____] foot high parallel fence with each sector consisting of [13] [_____] horizontal barbed wires attached to the taut-wire fence posts, and three strands as outriggers, plus an "antiladder" trip wire supported by rods extending from the outriggers for a total vertical height of approximately [2440] [_____] mm [8] [_____] feet. Displacement switches for each horizontal wire shall be mounted within a prewired channel fastened to the fabric fence post at the midpoint of each section. Outrigger barbed wire and tripwire may share the same switch. Each taut-wire fence post shall mount to the normal security fence (chain link) fabric posts or other barrier via standoffs to position the taut-wire approximately 150 mm 6 inches from the fence fabric or other barrier. Mount freestanding taut-wire fence posts in concrete to support the taut-wire fence system. Each barbed wire strand shall be pretensioned and clamped to the lever arm of the displacement switch, such that the lever is in the neutral (off) position; therefore, the forces applied by the barbed wires are balanced equal in opposite directions. Tripwire shall be pretensioned in a like manner. Tripwire shall be linked to the top switch in the sensor switch channel by a special subassembly that includes a rod which shall serve as a lever to transfer movement of the tripwire to the end of the actuating lever arm of the sensor switch. Abnormal displacement of a switch lever resulting from cutting or deflecting its attached wire, as by climbing on or through fence strands, shall initiate an alarm condition. Damping mechanism in the sensor shall reduce alarm threshold due to slowly changing phenomena such as ground shifting, daily and seasonal temperature variations, and winds up to 56 km/h 35 mph. Sensor switch shall provide electrical contact closure as the means for initiating an alarm condition, whenever the wire clamped to the vertical center bolt is pulled laterally in any direction by an amount not over 19 mm 0.75 inch. Housing for switch assembly shall be covered by a neoprene cap to retain the center bolt (lever arm), which functions as a lever to translate movement of the attached horizontal wire into contact closure. When the neoprene cap is firmly seated on the cup-shaped polycarbonate housing, it shall function as the fulcrum for the lever (bolt). Upper exposed end of the lever shall be threaded to accommodate clamping to the horizontal wire. The lower end of the lever, which is fashioned to serve as the movable electrical contact, shall be held suspended in a small cup-shaped contact that floats in a plastic putty material. The plastic putty shall retain a degree of elasticity under varying temperature conditions and provide the sensor switch with a self-adjusting property. This provides the switch with a built-in compensating mechanism that ignores small, very slow changes

in lever alignment (which may result from environmental changes such as extreme temperature variations and ground creepage due to weather conditions) and to react to fast changes only, as caused by manual deflection or cutting of the wires. Provide metal slider strips having slots through which the barbed wires pass. Wires shall be prevented from leaving the slots by rivets. Purpose of the slider strip shall be to translate forces normal to the barbed wire to a horizontal displacement of the sensor. Install one slider strip pair, upper and lower, on every fence post except where sensor posts or anchor strips are installed. Separation between slider elements along the fence shall be [3000] [_____] mm [10] [_____] feet. Attach barbed wires of sensor to existing specially installed fence posts, called anchor posts, located equidistant on both sides of sensor posts and at ends of sensor zone run. Anchor strip shall be a strip of steel plate on which are installed fastening plates. Weld strip or otherwise attach the strip to anchor post and ends of tensed barbed wires wrapped around the fastening plates. Attempts to climb on fastening plates or on the attached barbed wires shall cause plates to break off, creating an alarm and making it impossible to defeat the system by climbing at the anchor post. Barbed wire used in the system shall be suitable for installation under a preload tension of approximately 392 N 88 pounds and be flexible enough for convenient manipulation during tensioning. Double-strand 15 1/2-gage barbed wire shall be the minimum acceptable. Sensor zone control unit shall monitor up to [10] [_____] zones. Provide relay outputs to interface alarm outputs with the overall ESS. Input power requirements shall be 120/208 volts ac.

f. Gate units: Provide in accordance with specific fence sensor manufacturer's recommendations to ensure continuous fence sensor zone protection for the entire protected perimeter. Provide gate unit for each fence portal. When gate units are not provided by the fence sensor manufacturer, provide separately zoned BMS gate sensors. Sensors shall perform as specified in paragraph entitled "Balanced Magnetic Switches (BMS)." In addition, for a double gate, since both BMS elements must be mounted on the gate, electrical connection shall be jumpered within a flexible armored cord constructed from corrosion-resistant metal. Each end of the armored cord shall terminate in a junction box or other enclosure. Secure armored cord ends mechanically to the junction boxes by clamps or bushings. Provide conductors within the armored cord with lug terminals at each end. Jumpered conductors and the armored cord shall experience no mechanical strain as gate is moved from fully open to closed.

g. Barrier protection: Provide for exterior facility barriers other than fences by the employment of [electrostatic field sensors] [taut-wire sensors] [mounted on the barrier] [in a stand-alone configuration]. Divide the facility barrier perimeter sensor length electronically into [100-meter] [four] [_____] zones. Install sensors [on the exterior side of the barrier] [and] [as recommended by the manufacturer]. Sensors shall be as specified in the paragraph entitled ["Electrostatic Field Sensors"] ["Taut-Wire Sensors"].

h. Laser Range finder Sensor: Sensors shall detect intruder presence on building roofs, perimeters and water ways by two rotating laser range finders. As the range finders rotate, the sensor sends out laser pulses which enable it to learn its surrounding environment. The sensor shall detect intruders in a specified area while disregarding useless clutter such as weather conditions, moving bushes and similar environmental anomalies. The sensor shall be able to track an intruder

for up to 140 meters 450 feet radius and display the alarm results at the ESS. The sensor shall be able to send alarm signal data to the ESS and a CCTV camera system for additional intruder tracking.

i. Triple Technology Sensors : sensor shall consist of triple technology that combines Microwave and Dual Horizontally Opposed Mirror Optic PIRs into one single all-weather detector. The sensor is to be used in extreme outdoor conditions to provide the maximum amount of coverage in a horizontal plane. It shall come mounted in an industrial grade housing with a pan/tilt swivel bracket that provides swivel within 100 degrees of range and tilt within 10 degrees. The swivel bracket shall allow for calibration into 1 degree segments for adjustment to any environment. The sensor shall be able to provide either wide angle or long range detection by change of optical mirrors. Wide angel coverage shall detect intrusion out to 15 meters [49] [_____] feet and long range coverage out to [40] [_____] meters [130] [_____] feet. The sensor shall allow adjustment masks for wildlife immunity for animals up to [10] [20] [30] [45] [_____] kilogram [22] [44] [66] [99] [_____] pounds.

2.4.14.4 Duress Alarms

UL 636.

a. Hardwire duress alarms: Provide at points within the protected area as indicated. Alarms shall be capable of being secretly activated by the foot or hand of an average adult in both standing and seated positions. Alarms shall not be visible or audible from the sensor. Alarm signal shall lock-in upon activation until manually reset with a key or similar device and shall be readily identifiable by the ESS. Sensors shall be easy to operate and designed to minimize the possibility of accidental activation. Hardwire duress alarms shall be rated for a minimum lifetime of 50,000 operations. Securely mount sensors in rugged, corrosion-resistant housing.

b. Radio frequency duress alarms: Duress alarms shall consist of a compact and lightweight transmitter enclosed in a case that can be easily worn at the waist on a belt. Each transmitter shall have a unique identification code. The transmitter shall be capable of transmitting 2 watts of RF power. Each transmitter shall transmit up to [500] [_____] times on the power provided by internal batteries. A small, flexible PVC-encased antenna shall be mounted 10 mm 1/2 inch away from the transmitter to ensure reliable propagation of the alarm signal and rotation of 6.28 rad 360 degrees without damage to the sensor. Provide a case to prevent corrosion in hostile environments. Transmitter shall be available in both the very high frequency (VHF) and ultrahigh frequency (UHF) radio bands. The transmitter shall be FM modulated to ensure reception and decoding of the alarm signal. Signal transmitted shall readily interface with the ESS communications subsystem as specified in paragraph entitled "Radio Frequency Link." Activation of the sensor shall be by hand-operated switch protected from accidental activation, yet easily activated by hand when worn at the waist on a belt. [Sensor activation shall be automatic when mounted on a belt and the wearer is in a horizontal position for longer than [one] [5] [15] [_____] minutes, adjustable. Adjustment of time interval activation shall not be accessible to operations personnel.]

2.4.15 Automated Access Control System (AACS)

Provide Automated access control system based upon a modular distributed microprocessor architecture complete with access control cards and ready for operation. [system shall interface with and provide alarm and other status to the overall ESS.] [system shall provide monitoring and control for the ESS.] System shall meet the Grade [AA] [_____] communications requirements of UL 1076 and UL 294 and shall have the capability of controlling up to [4] [8] [16][_____] card reader and keypad per card reader controller. System shall grant or deny access or exit based upon keypad identification data, card identification data, video, biometric iris scan, biometric finger print reader identification data, Smart card identification data or a combination of identification technologies, input through the access control devices compared to data stored within the system, as well as time of day and day of week. Decision to grant or deny access or exit shall be based upon authorization for such data to be input at a specific location for the current time period. [Access decisions for high security areas shall be based upon combination of two identification technologies, such as card and keypad or card and biometric.]

The AACS primary functions shall be to regulate access through specific doors or portals to secured areas, regulate elevator control and monitor alarm points at the facilities to be protected. [The AACS shall provide for a Photo Identification credential creation and production system integrated with the cardholder management system]. The AACS shall utilize a single database for both its access control and photo imaging functionality that shall seamlessly integrate with the ESS. The AACS shall be able to control [4] [8] [16] [_____], [128] [256] [512] [_____] alarm inputs, or [128] [256] [512] [_____] relay outputs or any combination of these components.

The AACS shall support configuration and simultaneous monitoring of multiple access control devices when TCP/IP communication interfaces are used between the ESS and the primary Access Control Units (ACU). The events of the AACS shall be viewable as separate or as a combined list of all ESS events. Overall control of the AACS, alarm monitoring, and photo identification shall be through software control of the ESS.

All AACS programming data shall reside on a single database and shall be instantly accessible to every networked PC workstation connected to the ESS.

AACS functions shall include validation based on time of day and day of week, special day/holiday scheduling with card validation override, video image storage and retrieval of cardholder photographs, access validation based on positive verification of card, card/PIN, card and video.

AACS shall provide both supervised and non-supervised alarm point monitoring. The system shall be capable of arming or disarming alarm points both manually and automatically by time of day, day of week or by operator command. The system shall be capable of disarming alarm points based on a valid access event.

AACS, when used for elevator control, shall grant access to elevator floors based on a valid credential, or by schedule.

The AACS shall provide programmable 'delay' setting for all alarm points. The alarm points shall not report an ENTRY type alarm condition until the delay setting has expired. The system shall not report a DWELL type alarm condition until the alarm has been active for the full delay period.

The AACS shall include fully integrated badging capabilities, including image capture, image editing, badge design, and badge printing. The system shall permit the storage of four different images: main photograph, alternate photograph, signature, and fingerprint. The AACS shall allow each cardholder to be assigned to both a badge design formatted for badge printing and a dossier design formatted for standard paper printing. The AACS shall provide for interfacing with external badge programs, in which stored photo images are displayed in cardholder information window but other badge features are supported by the external program. The Photo imaging components shall include one or more networked PC workstations at which all of the required image capture equipment has been installed.

The AACS shall provide capability to place ACU(s) in an off-line mode. In the off-line mode, the ACU(s) shall retain a historical summary of all ACU activity transactions, up to the maximum capacity of the ACU memory buffer. The system shall provide ability for manual operator control of system output relays. The manual functions shall include the ability to energize, de-energize, enable or disable.

The AACS shall provide ability to display stored 'video image' of cardholder based on card activity, and switch real-time CCTV camera to card reader location for specific card usage. The card reader shall not activate the door lock until positive operator acknowledgment from the SCC.

The AACS software shall be capable of, but not limited to, the following programming:

(1) Time Schedules: Up to [254] [_____] user-definable time schedules shall be provided. These time schedules shall determine the day(s) and times that access will be granted or a scheduled event shall occur. Any and all of the time schedules shall be available for defining access privileges and scheduled events. There shall be ALWAYS and NEVER schedules that cannot be altered or removed from the system. Each user-defined time schedule shall have the option of reacting or not reacting to user-defined special days, with the ability to react uniquely to each type of special day.

(2) Special Days: There shall be an unlimited number of user definable special days. These days shall be used for configuring exceptions to the normal operating rules, typically for specifying holiday operating rules. Each special day shall be assigned to a type, with each type defined by the user.

(3) ACU Daylight Savings Time Adjustment: There shall be a software-configurable, user defined adjustment for Daylight Savings Time. The ACU shall not need to be connected to a PC workstation in order for the adjustment to occur.

(4) Scheduled Events: Any access controlled reader shall be capable of scheduled unlock periods to allow for card-free access. The access controlled reader shall also be capable of requiring one valid access event before beginning a scheduled unlock period. Additionally, any access control point shall be capable of requiring a valid card as well as a PIN code via keypad on a scheduled basis for high security areas. The use of PIN via keypad functions shall not reduce the number of card reader or alarm points available in the ACU(s). Any designated alarm input shall be able to be scheduled Armed and Disarmed. Any relay output shall be capable of scheduled On and Off periods to allow for automatic I/O system control.

(5) Maximum User Capability: Up to [64,000] [_____] individual users may be given access cards or codes and have their access controlled and recorded.

(6) Access Groups: Each system user shall be assignable to a maximum of [4] [_____] of [256] [_____] possible access groups. An access group shall be defined as one or more people who are allowed access to the same areas at the same days and time periods.

(7) Active/Expire Dates: Any card/user may be configured with activation and expiration dates. The card can be assigned to any valid access group and will be activated and expired according to the specified dates.

(8) Maximum Use Settings: Any card/user may be configured with maximum number of uses for that card. The card can be assigned to any valid access group and will be expired according to the specified number of card uses.

(9) Door Outputs: Each access control reader shall have two dedicated relay outputs. Both relays shall provide Normally Open and Normally Closed contacts. The first relay shall be used for electric lock control. The second shall be software configurable to activate for door forced open, door left open too long, duress, passback violations, invalid access attempts and valid unlock conditions. Both relays shall be separately programmable for energize times from [1] [_____] second to [10] [_____] minutes. The second relay shall allow a delay time to be specified, causing its activation to be delayed after an activating condition occurs.

(10) Anti-Passback: The AACS shall have global anti-passback capability. Any door on the system can be linked to one of [254] [_____] user defined passback areas or two [2] [_____] pre-defined areas. Each door may be set up to automatically forgive passback entries at the following intervals: Never, at Midnight, every 12 hours (Midnight and Noon), every 6 hours, every 2 hours, each hour or every 30 minutes. Each door can be configured to deny or grant access for passback violations and individual users can be exempt to the passback rules. The anti-passback features shall be a global function and operate completely independent of the AACS software with the exception of configuring the passback rules. Additionally, the operator shall have the ability to manually forgive an individual user or all users by command from the AACS.

(11) Two Person Rule: Any access control reader on the system shall have the ability to require two valid cards for access. This feature shall be software programmable. Any access control reader on the system that includes a keypad shall also have the ability to require a valid PIN number associated with each of the two valid cards.

(12) User List/Who's In (Muster Reports): The AACS shall be capable of generating dynamic lists of users in certain access-controlled areas, based either upon selected users or selected areas. The lists shall have the option of automatically refreshing after a user-selected interval of time.

(13) Crisis Mode: The AACS shall support "crisis mode", in which the activation of user-selected alarm points causes changes to user access

privileges. The changes to user access privileges shall be configurable to restrict normal access to no access or limited access.

(14) Door Groups: The system shall allow up to [255] [_____] door groups to be configured. Doors belonging to the same group shall be able to be locked, unlocked, disabled and enabled on command from the AACS.

(15) Door Interlocking: The system shall allow a group of doors to be software configured so that if any door in the group is unsecure, all other doors shall be automatically disabled. This feature also known as "mantrap" configuration. The interlocking features shall not require the AACS to be on-line for proper operation.

(16) PIN Required: The AACS shall support the required use of a keypad code, in addition to a valid credential, at user-selected doors, during user-selected schedules.

(17) Remote door control: The SCC operator shall have the capability of manually controlling any access point by issuing a simple command from the AACS. The operator shall have the ability to lock, unlock, enable, disable and pulse any door in this manner. This activity shall cause an entry to be logged displaying the door name, number and time that it was performed. Additionally, the operator shall have the ability to lock, unlock, enable and disable any group of doors in a Door Group by a single command from the AACS.

(18) Key Control: When interfaced with an approved key-control system, the system shall allow users to deny access to certain doors to any users who have keys in their possession.

(19) Guard Tour: The AACS shall support user-defined guard tours. The tour may be configured in a set pattern of tour points, or may follow a mode in which all tour points can be visited in any order within an allotted time. The AACS shall allow a tour to be started by AACS-command, by use of a selected card at a selected reader, or by use of a selected keypad code at a selected keypad. The system shall detect guard late-to-point; point missed, and point out-of-sequence events. The system shall generate a report at the completion of a tour.

(20) Reader Disable: The AACS shall support disabling readers in reaction to a user-selected number of invalid access attempts.

(21) Disable Event Messages: The AACS shall allow users to disable user-selected event messages (Door Forced Open, Door Open Too Long, Door Closed, Request to Exit) for user-selected doors. The AACS shall allow users to disable certain messages (Door Forced Open, Door Open Too Long) according to a user-selected schedule.

(22) I/O Groups: The AACS shall allow up to [255] [_____] user-defined I/O (input-output) groups to be defined. Each Input device shall be able to be linked to these groups for arming, disarming, shunting and unshunting as well as output control.

(23) Delays: Each alarm device shall allow a delay to be specified. The delay shall be either an entry type or a dwell type. An entry-type delay shall prevent the input from issuing an alarm event until the delay elapses. If unarmed during the delay period, the alarm condition shall be ignored. A dwell-type delay shall require the input to remain in the alarm state for the full duration of the delay before issuing an

alarm condition.

(24) Remote Input control: The operator shall have the capability of manually controlling any alarm/input point by issuing a simple command from the AACS. The SCC operator shall have the ability to shunt, unshunt, disable and restore any input in this manner. This activity shall cause an entry to be logged displaying the input name and time that it was performed. Additionally, the operator shall have the ability to arm, disarm, shunt and unshunt any alarm partition/group by a single command from the SCC. The arm disarm, shunt and unshunt any alarm partition/group from the SCC shall not be permissible in DIA DCID 6/9 applications.

(25) Output Configuration: Each output relay shall be software configurable as a FOLLOWS, LATCH, TIMEOUT, SCHEDULED, TIMEOUT RETRIGGERABLE, LIMIT, or COUNTER type. The SCHEDULED type shall allow a time schedule to automatically control its activation and de-activation. The FOLLOWS, LATCH, TIMEOUT, TIMEOUT RETRIGGERABLE, LIMIT and COUNTER types shall be configured to activate based on the condition of I/O groups. Additionally, a time schedule shall be specified to configure when the output shall actively monitor the I/O groups.

(26) Remote Output control: The operator shall have the capability of manually controlling any output point by issuing a simple command from the SCC. The SCC operator shall have the ability to ENABLE, DISABLE, turn ON and turn OFF any output in this manner based on the output type. A FOLLOWS type output shall not be capable of being turned OFF or ON. This activity shall cause an entry to be logged displaying the output name and time that it was performed. manual control of outputs shall not be permissible in DIA DCID 6/9 applications.

(27) Remote Reset Command: Any ACU shall have the capability of being reset manually or by command issued from the AACS. This reset command shall have the option of simulating the ACU reset settings, or forcing a reset type as specified by the user. The remote reset command shall not cause the ACU to degrade its level of protection to any access points defined.

(28) Dial Out: The ACU shall have the capability of using a modem to automatically connect to the AACS when a critical alarm or service event occurs. The conditions triggering the dial out capability shall be user defined and software configurable.

(29) Time Zone: The AACS shall allow the user to select the time zone in which the ACU is located, so that event times displayed for that ACU will match the local time where the ACU is located.

(30) User-Selected LED Behavior: The AACS shall allow the user to select different behaviors for the LEDs of each access controlled reader.

(31) Traced Cards: The AACS shall be capable of selecting any number of cardholders for the purpose of limiting reports to only traced users. The AACS shall be capable of displaying all traced cardholder events in a user-selected alternate color.

(32) Badge Print Tracking: The AACS shall support setting a print limit for any badge. The software will track the number of times any badge has been printed, as well as display the date and time of the most recent printing.

2.4.15.1 Error and Throughput Rates

Rates shall be portal to portal performance averages obtained when processing individuals one at a time. When serial verification techniques or multiple attempts are required to satisfy error performance requirements, features shall not reduce capability to meet throughput requirements. A Type I error denies access to an authorized enrolled individual. A Type II error grants access to an unauthorized individual. Subsystem Type I and Type II error rates shall be both less than [0.1] [_____] percent. At the error rates, subsystem access throughput rate shall be minimum of [12] [_____] individuals per minute through one card reader and keypad access control device.

2.4.15.2 Access Control Subsystem Central Processing

Provide serial management and control of subsystem. Provide a microprocessor control device designed to monitor and control units and up to [32] [_____] card reader and keypad access control devices. Central processor shall interrogate and receive responses from each ACU within 100 milliseconds. Failure to respond to an interrogation shall cause an alarm. Provide a printer with a minimum print rate of 30 characters per second to produce hard copy of subsystem events. Provide the central processor with an TIA-232 interface port to communicate with the printer. Provide an operator interface to control system operating functions. Provide the central processor with a facility-tailorable data base for a minimum of [1000] [_____] card holders with by-name alphanumeric printout, and for automated [subsystem] [IDS] monitoring, management, and control functions. Provide enrollment equipment to process access control cards and enroll personnel into and disenroll personnel from the subsystem data base. Enrollment equipment shall not be accessible to ESS operations personnel. Provide a minimum of [150 percent of the number of card holders specified above] [_____] access control cards with the enrollment equipment. Provide system configuration controls and electronic diagnostic aids for subsystem setup and troubleshooting with the central processor. Components shall not be accessible to operations personnel. Central processor components shall be tamper alarmed.

2.4.15.3 Access Control Unit (ACU)

The ACU shall be micro-processor based with all access and I/O decisions to be made by the individual ACU(s). The ACU shall be of modular design which will allow for present security requirements and the capability to expand. All field ACU panels shall be configured to intercommunicate via RS-422/485 or RS-232 hardwired, Dial-up, TCP/IP or fiber-optic communication. All field ACU(s) shall be equipped with a tamper contact. One ACU shall be designated a "Primary", responsible for all AACS-to-ACU communications. All other ACU(s) up to a maximum of [16] [32] [64] [254] [_____] shall be designated "Secondaries" and shall communicate with the "Primary" via an RS-422/485 hardwire, TCP/IP network or fiber-optic configuration. The ACU shall be capable of, but not limited to, the following:

(1) All ACU(s) shall have built-in surge suppression circuitry on plug-in modular circuit boards. The surge protection, designed as an integral component of the system, shall be self-sacrificing in the event of extreme surges or spikes.

(2) Each ACU shall be capable of supporting at least [2] [_____] ports and be expandable in increments of two ports up to a maximum of [4] [8]

[16] [_____] ports per ACU.

(4) Each ACU port shall be configured by AACS to support any one of the following peripheral devices: Card reader, Alarm Monitoring Module, Output Relay Module, Elevator Reader, or Elevator Output Module. Any combination of these devices can be supported on each ACU, up to a total of [2] [4] [8] [16] [_____] devices per ACU.

(5) Each ACU shall have the capability of supporting multiple card reader technologies simultaneously, including Transmissive Infrared, Wiegand, Magnetic stripe, Proximity, Barcode, Keypad, Card/Keypad, Smart Card, and Biometrics. This capability shall be an integral part of the ACU and will not require special external equipment.

(6) Each ACU shall have built-in battery back-up of programmed information and shall be sustainable for a period of not less than ninety days.

(7) Each ACU shall be powered by a [12] [24] [_____]VDC power source rated at a minimum of [2] [_____] amperes. The power supply shall have a battery back-up for complete system operation in the event of power failure. Provide battery backup for all ACU(s) to sufficiently power the ACU for 48 hours continuous service.

(8) Electric strikes, other locking devices and ancillary peripherals shall have a separate power supply. Battery back-up shall be utilized for continued operation in the event of power failure.

(9) There shall be a minimum of a [10,300] [_____] event log buffer per ACU. The log buffer shall be used to record and hold access and alarm activity information until the AACS is connected and receives the information. There shall be a software-configurable warning notification of log buffer filling for ACU(s) configured with modem capabilities.

2.4.15.4 Card Reader and Keypad Access Control Devices

****

NOTE: Specify only one type of access control card. Be sure card type and card readers are compatible with each other.

****

Devices shall be tamper alarmed, tamper and vandal resistant, and solid state, containing no electronics which could compromise the access control subsystem should the subsystem be attacked. Devices shall be surface, semiflush, pedestal, or weatherproof mountable as specified for each individual location. [Each device shall contain a visual display, either mounted on the face or an integral part, to indicate access or exit request processing, request approval, and request denial.] Card readers shall be the [proximity] [insertion] [swipe-through] type and shall be capable of reading [magnetic stripe] [high coercivity magnetic stripe] [Wiegand] [Hollerith] [proximity] [Transmissive Infrared] [Keypad] [[_____]/Keypad] [Smart Card] [Biometric][_____] type access control cards. Keypads shall contain an integral 12-digit tactile keyboard with digits[arranged in numerical order]. Keypad shall be [a stand-alone device] [or] [integrated into the card reader].

2.4.15.5 Access Control Cards

****

NOTE: Determine the format, logo, and wording for the cards from the using activity before final design. A unique facility code may only be available with the purchase of 5000 cards or more.

****

Cards shall be manufactured with capability of modification and lamination during enrollment process without reduction of readability for use as a picture and identification badge. Cards shall contain binary coded data arranged in a scrambled pattern as a unique identification code stored on or within the card and of the type readable by the subsystem card readers. Include within the card binary data a nonduplicated unique facility access control subsystem identification code common to access control cards provided. [Cards shall be designed for use as a photo identification card suitable for lamination.]

2.4.16 Communications

Communications shall link together subsystems of the ESS. ESS communications links shall be via hardwire (cable) [or radio frequency]. Communications links shall be supervised. Common communications interface devices shall be provided throughout the ESS. Sensor to control unit interface shall be by dry relay contact normally open or normally closed, except as specified otherwise. Control unit to central alarm reporting and display processor interface shall be digital, asynchronous, or multiplexed data. Individual data bits shall be grouped into word format and transmitted as coded messages. Interface shall be implemented by modems which function as a communications controller, perform data acquisition and distribution, buffering message handling, error checking, and signal regeneration as required to maintain communications.

2.4.16.1 Link Supervision

a. Hardwire direct current line supervision: Provide only for sensor to control unit links which are within ESS protected area. Circuit shall be supervised by monitoring changes in the current that flows through the detection circuit and a terminating resistor of at least 2.2 kohms. Supervision circuitry shall initiate an alarm in response to opening, closing, shorting, or grounding of conductors by employing Class C, standard line security. Class C circuit supervisor units shall provide an alarm response in the annunciator in not more than one second as a result of the following changes in normal transmission line current:

(1) Five percent or more in normal line signal when it consists of direct current from 0.5 through 30 milliamperes.

(2) Ten percent or more in normal line signal when it consists of direct current from 10 microamperes to 0.5 milliampere.

(3) Five percent or more of an element or elements of a complex signal upon which security integrity of the system is dependent. This tolerance will be applied for frequencies up to 100 Hz.

(4) Fifteen percent or more of an element or elements of a complex signal upon which the security integrity of the system is

dependent. This tolerance will be applicable for all frequencies above 100 Hz.

b. Hardwire alternating current supervision: Supervision shall not be capable of compromise by use of resistance, voltage, or current substitution techniques. The method shall be employed on circuits which employ a tone modulated frequency-shift keying (FSK), interrogate-and-reply communications method. Supervisory circuit shall be immune to transmission line noise, crosstalk, and transients. Detection circuit shall be terminated by a complex impedance. Supervision of the line shall be maintained by monitoring current amplitude and phase. Complex impedance shall be sized so that current leads or lags the driving voltage by 0.785 plus or minus 0.087 rad 45 plus or minus 5 degrees. For supervision currents of 0.5 to 30 milliamperes root mean square (rms), an alarm shall result when rms current changes by more than 5 percent, or phase changes by more than 0.087 rad 5 degrees. For lines with supervision currents of 0.01 to 0.5 milliampere, an alarm shall result when rms current changes by more than 10 percent, or phase changes by more than 0.139 rad 8 degrees. Identified line supervision alarm shall be communicated within one second of the alarm condition.

c. Hardwire digital supervision: Modems at both ends of circuit shall exchange digital data to indicate secure or alarm condition at least every 2 seconds. For passive supervisory circuits, an alarm shall sound if data is missed for more than one second. Coding used for data shall not be decipherable by merely viewing data on an oscilloscope. For transponder schemes, supervisory circuit shall asynchronously transmit bursts of digital data. Data pattern shall be random in nature. Remote detectors shall receive data and encode a response based on a proprietary coding scheme. Each ESS shall have a unique encoding scheme; an industry-wide or vendor standard is not acceptable. Encoded response shall be transmitted back to supervisory circuit. Supervisory circuit shall compare the response to an anticipated response. Failure of the detector to return a data burst, or return an incorrect response, shall initiate an alarm.

d. RF link supervision: System shall consist of link supervision components which provide a line supervision alarm declaration at the annunciation end of the link in approximately 2 seconds after the system has verified a problem by repeating the same signal no less than nine times during a period of 30 seconds or less.

2.4.16.2 Hardwire

a. Hardwire shall utilize electrical conductor lines. Alarm electrical lines shall not rely on current path except for electrical wires; neutral conductors of electrical distribution systems shall not be used as signal transmitters. Conductors outside the protected area shall be [shielded cable] [buried] [[installed in rigid galvanized steel conduit.] [installed in electrical metallic tubing (EMT)] as specified in Section 26 20 00 INTERIOR DISTRIBUTION SYSTEM]. Supervision circuitry shall not initiate nuisance alarms in response to normal line noise, transients, crosstalk, or in response to normal parametric changes in the line over a temperature range of minus 35 to 52 degrees C 30 to 125 degrees F. Ambient current levels chosen for line supervision shall be sufficient to detect tampering and shall be within the normal operating range of electrical components. Line supervision and tamper alarms shall be reported regardless of mode of operation.

Provide hardwire links as specified in UL 1076 and Section 26 20 00 INTERIOR DISTRIBUTION SYSTEM for interior applications with additions and modifications specified herein. Conductors shall be copper. Conductors for links which also carry ac voltage, shall be No. 12 AWG minimum; single conductors for low-voltage dc links shall be No. [14] [16] AWG minimum. Conductors shall be color coded. Conceal wiring in finished areas of new construction and wherever practical in existing construction if not otherwise precluded by the Government. Identify conductors within each enclosure where a tap, splice, or termination is made. Identify conductors by plastic-coated, self-sticking, printed markers or by heat-shrink type sleeves. Connect sensors, control units, and communication devices so that removal will cause a tamper alarm to sound. Pigtail or "T" tap connections are not acceptable. Each conductor used for identical functions shall be distinctively color coded. Each circuit color code wire shall remain uniform throughout circuit.

b. Communication link from sensor to control unit shall be by dedicated circuit. An alarm condition shall be indicated by the opening or closing of a relay contact. Analog signals shall be converted to digital values or a relay closure or opening within 76 meters 250 feet of the sensing point. Communications from control unit to central alarm reporting and display processor shall operate in a continuous interrogation and response mode, using time-multiplexed digital communications techniques at a data rate of [5.12] [10.24] [_____] kilobaud. Interrogation and response communications between the control unit and central processor shall be half-duplex, bidirectional on one dual twisted pair cable, one pair for interrogation, one for response, which may have one or more parallel branches. Individual control unit lines shall be 22 AWG or larger wire. Connect control wires in parallel to the hardwire link. Communications system shall provide for connection of as many as [255] [_____] control units. When operating without line repeaters or other signal regenerating or amplifying devices, communication system shall maintain specified performance over a link length of 2287 meters 7500 feet. When operating with signal-regenerating line repeaters, communications system shall maintain specified performance over a link length of 22 865 meters 75,000 feet. Control unit to central alarm reporting and display processor communications link shall also be capable of operating over a maximum of [two] [four] [_____] standard voice grade telephone leased or proprietary lines. Link shall be capable of operating half duplex over a Type 3002 data transmission pair and be capable of modular expansion. Telephone lines shall be provided by the Government. Coordinate and check out system operation. General characteristics and telephone line service shall be as follows:

(1) Connections: Two- or four-wire

(2) Impedance at 1000 Hz: 600 ohms

(3) Transmitting level: 0 to 12 dBm

(4) Transmitting level adjustment: 3 dB increments

(5) Type: Data

(6) Direction: Two-way alternate (half duplex)

(7) Maximum speed: [1.2] [5.12] [10.24] [_____] kilobaud

(8) Maximum loss at 1000 Hz: 33 dB.

c. Video hardwire links shall be as specified in paragraph entitled "Video Transmission."

2.4.16.3 Radio Frequency Link

****

NOTE: Radio frequency links may not be allowed on some Government facilities. Recommended usage for RF links is as backup to hardwire links or to a remote location lacking telephone lines. OPNAV Instruction 2400.20E requires that funds shall not be obligated for procurement of radio equipment until frequency allocation authority has been obtained. As soon as possible, but no later than schematic design, the designer shall contact the area radio frequency coordinator (usually the base radio officer) to determine the availability of radio frequencies and to ensure that the using activity submits a DD Form 1494, "Application for Frequency Allocation," for a Stage 1 ("Conceptual Development") allocation (see DD Form 1494 Preparation Guide). Stage 1 allocation authority (i.e., approval) must be obtained prior to advertisement of the contract.

The 138 to 150.8 MHz band is the preferred range since specific frequencies in this range are reserved for DOD use. Frequencies in the 162 to 174 MHz and 450 to 470 MHz bands are shared with other users on a first-come, first-served basis. In order to avoid potential contract delays, the frequency assignment should be included in the specification when possible. For additional information, contact the base radio officer or the Naval Electromagnetic Spectrum Center at (202) 433-0689, OPNAVINST 2400.20E issued by OPNAV Code N60 (previously Code OP941), telephone (703) 695-7284.

****

System shall be a full duplex supervised RF polling specifically designed for alarm data communications with components manufactured by one manufacturer. System shall operate in the VHF, 134 to 154 MHz band. System shall interface directly with ESS hardwire data link from control unit to central alarm reporting and display location and shall translate (reduce) the data rate for RF transmission, modulate and demodulate the data signal, and transmit and receive ESS data. Provide a factory-tested complete RF link which both automatically and upon operator command transmits a signal with a unique identification from the central alarm monitoring location to the control unit locations. Message receipt at control unit location shall be ignored by all units except the addressee. Unit with the correct address shall decode the interrogation signal and respond to the interrogation with the status of the reporting sensors. When the addressee fails to respond, reinterrogate. Failure to respond a second time shall cause a line supervision alarm. Remote units in the RF system shall be individually polled in turn. Polling response time and transmission data rate, data error rate, and equipment reliability shall ensure that overall ESS alarm

annunciation time reliability and Ps is not degraded. Provide RF transmitters, receivers, or transceivers in sufficient quantities to meet specified requirements. RF link transmissions shall be on one or more of the frequencies within the specified band as required to meet specified requirements and shall neither interfere with other ESS components nor any facility electronic components. Provide transmitters which are in accordance with applicable requirements of 47 CFR 15. Message types and content shall be identical to those transmitted by other portions of the ESS data communications subsystem. ESS alarms sent by RF link shall not fail to be transmitted by the RF link due to event occurrence during "off air" periods. RF link shall provide message transmission priority in the following order:

a. Intrusion alarms

b. Tamper alarms

c. Access denial alarms

d. Other alarms on a first-in, first-out basis including loss of communication signal, fail-safe, low battery, and power loss.

Provide [omnidirectional, coaxial, half-wave dipole] [_____] antennas for alarm transmitters and transceivers with a driving point impedance to match transmission output. Antennas and antenna mounts shall be corrosion resistant and designed to withstand wind velocities of [160] [_____] km/h [100] [_____] mph and physical damage caused by vandalism. Antennas shall not be mounted to any portion of the facility fence or roofing system. Antennas shall be furnished by the same manufacturer as the rest of the RF link. Provide coaxial cable in lengths as required. Cable shall use PL-type fittings or connectors, properly protected against moisture. Cables shall match output impedance of transmitters.

2.4.17 Closed-Circuit Television (CCTV) System

****

NOTE: Scene illumination shall be even across the field of view of the camera, with a maximum light to dark ratio of 8 to 1. Minimum illumination level shall be 11 lux one footcandle.

****

****

NOTE: For visual assessment of alarms, specify the optimum number of monitors for the number of cameras required. It is difficult to view and respond to too many monitors. Typically, for six cameras or less, use one monitor per camera. For a larger number of cameras, consider sequential switchers, four quadrant multiplexers, or a combination of both.

****

Provide UL Listed CCTV components to provide visual assessment of ESS alarms. Subsystem shall continuously view remote areas with video cameras and display the areas automatically upon ESS alarm, or upon SCC operator selection. Provide the number of alarm monitors as required. Video systems shall be capable of automatic and manual operation. In systems where monitors may display more than one camera scene, provide on-screen camera identification. Subsystem shall be composed of components which are

integrated to provide a quality video surveillance system. The scene from each camera shall appear clear, crisp, and stable on the respective monitor during both daytime and nighttime operation. Component equipment shall minimize both preventive and corrective maintenance. Components shall be compatible with other components and with system as a whole and shall, to the greatest extent possible, be supplied by the same manufacturer.

2.4.17.1 Cameras

a. Except as specified herein, CCTV camera shall comply with SMPTE 170M for standard monochrome or color camera and shall:

(1) Camera: shall utilize digital signal processing (DSP) to produce a high picture quality. Day/Night (Color/B&W) fixed or pan-tilt-zoom (PTZ) cameras are to be used in all outdoor environments. Standard DSP fixed or PTZ cameras are to be used for all indoor applications except when backlighting issues are observed. For backlighting or high contrast applications, use Day/Night cameras or standard cameras with backlighting compensation.

(2) All PTZ cameras shall feature a direct drive motor assembly. Belt driven PTZ camera units are not acceptable. All PTZ cameras shall be equipped with a slip ring assembly having an optical interface and be rated for continuous duty. PTZ cameras shall be fully integrated units. The pan-tilt mechanism shall be an integral part of the camera.

(3) Be identified with the manufacturer's part number, model number, lens installed, and a serial number;

(4) Operate over a voltage range of 105 to 130 volts ac or low voltage 12 to 24 volts ac at 60 Hz;

(5) Have electronic circuits which use solid-state devices.

(6) Be constructed to provide rigid support for electrical and optical systems so that unintentional changes in alignment or microphonic effects will not occur during operation, movement, or lens adjustments;

(7) Have standard C or CS lens mount;

(8) Be designed to protect personnel from exposure to high voltage during operation and adjustment; and

(9) Meet requirements specified herein with either side of the power source line grounded. Minimum essential requirements shall include the following:

(a) Sensitivity: Minimum Illumination: 0.8 lux (0.08 fc) at F1.4 color mode; 0.1 lux (0.01 fc) at F1.4 in the B&W mode.

(b) Signal-to-noise ratio: Show a signal-to-noise ratio of not less than 50decibels (dB) at AGC "Off", weight "On".

(c) Resolution: Provide a horizontal resolution of at least 480 lines in color and 570 line in B&W with automatic gain and bandwidth at the specified sensitivity.

(d) Digital Signal Processing: Cameras shall have Digital Signal Processing (DSP) technology to produce clear, high quality video images.

(e) Synchronization: Internal, line lock or multiplexed Vertical Drive Selectable.

(f) Day/Night cameras shall feature a B/W mode that may be automatically engaged on low light level and permit the use of an external infrared illuminator. Removal electronically of the color signal is not acceptable. The camera shall feature an infrared cut filter capable of being removed automatically upon low light threshold or manually.

(g) Geometric distortion: Camera shall be accurate to within a maximum 1.5 percent geometric distortion in Zone 1 and to within 2 percent in Zones 2 and 3.

b. Camera signals: CCTV camera vertical sync signal shall be phase-locked to the ac power line frequency and shall remain line locked at 60 Hz, plus or minus 0.3 Hz. Synchronization at the video output shall conform to the timing specified by SMPTE 170M. Camera shall operate on internally generated sync automatically upon loss of external sync.

c. Camera resolution

(1) Exterior: Horizontal resolution shall be 480 TV lines in the center in the color mode and 570 lines in the black & white mode, Vertical resolution shall be 350 TV lines in the center. Resolution shall be maintained over the specified input voltage and frequency range, and shall not vary more than 100 TV lines from minimum specification over the specified operating temperature range. Composite video output level shall be automatically maintained to within plus or minus 0.1 volt over scene changes of 2.69 lux to 107,600 lux 0.25 footcandle to 1 by 104 footcandles with lenses of f/1.4 and greater.

(2) Interior: Horizontal resolution shall be at least TV lines. Vertical resolution shall be at least 350 TV lines. 480Resolution shall be maintained over the specified input voltage and frequency range.

d. CCTV lenses: Provide lenses with automated light level metering device and an auto-iris. Provide each lens with a metal density spot filter. Light adjustment by the automatic metering device shall be a weighted average rather than a simple average or a peak response. Provide lenses for 1/3 and 1/4 inch format cameras. Provide lenses which are mountable with standard C or CS mounts.

e. Auxiliary CCTV camera equipment: Equipment shall consist of camera mounts and housings with environmental protection as applicable for each camera. Camera mounts shall be heavy duty industrial type, shall provide stable support for the camera, and shall be the configuration specified for each individual camera location. Housing shall protect the camera to ensure continuous 24-hour per day operation under specified environmental conditions. Housing shall be constructed of a durable material. Access to housing shall allow for camera and auto-iris removal and replacement within plus or minus 0.0087 rad 0.5

degree, both vertical and horizontal centerline alignment. Sealed housings shall be pressurized with dry nitrogen, or contain two units of desiccant in the camera body area. Install a 10, 20, and 30 percent humidity level indicator strip in a position that allows inspection through the enclosure faceplate. Where used, thermostatically controlled heaters shall be located near the auto-iris and faceplate and near the midsection of the camera body. Where ventilation blower is used in housing to prevent high temperature, it shall be thermostatically controlled. Hinged louvers shall close over blower exhaust when blower is off. For exterior cameras, video, sync, tamper, and power cables shall enter camera housing via weatherproof fittings. Entry into housing shall not interfere with housing heaters or blower operation. Provide terminal strips for power inside environmental housings to distribute 120 volts ac for the camera, heater, and blower, as applicable. [Provide enclosure sunshade as indicated for exterior camera location.] [Provide indoor environmental enclosures which are lockable and dustproof.] [Enclosures shall be tamper alarmed.]

2.4.17.2 Video Signal

Requirements apply to the video signal present at the video monitor input. Standard system video level shall be one volt peak-to-peak (Vp-p) composite video and sync. Standard system impedance shall be 75 ohms over the frequency range 0 to 5 MHz. System timing and synchronizing waveform shall be according to SMPTE 170M. Peak-to-peak amplitude of the composite TV waveform shall be one volt and shall be referred to as standard system video level. Waveform shall be measured in IRE units on the IRE scale graticule where 140 IRE units represent one volt. Synchronizing pulse amplitude of a composite video signal of standard system video level shall be measured from blanking level to negative peak of the sync pulse and shall be 40 IRE units, 0.3 volt nominal. Video amplitude of a composite video signal of standard system video level shall be measured from blanking level to reference white level and shall be 100 IRE units, 0.7 volt nominal. Picture setup of a composite video signal of standard system video level shall be 7.5 IRE units, 7.5 percent of the video amplitude. Pulse overshoot shall be less than 2 percent of the pulse amplitude. Video signal voltage frequency response shall be measured from camera output to video monitor input. It shall be plus or minus 2 dB from 60 Hz to 5 MHz and not more than 3 dB down at 6 MHz. The low frequency distortion shall be measured for every camera output over every normal program path to the input of the associated monitor. Distortion shall be less than 2 percent at line and field rates. Peak-to-peak signal-to-rms noise ratio shall be measured for every camera output via the normal program path at input of the associated monitor. Terminate circuits, except the one under test, at inputs and outputs. Hum and noise shall be 60 dB below 1.0 Vp-p.

2.4.17.3 Video Matrix Switchers

Switching shall interface multiple video signals, cameras, with one or more monitors. Switching shall be timed to occur during the video signal blanking period, vertical interval switching. When an ESS zone goes into alarm, a signal shall be sent from the alarm reporting and display processor to the switcher. When the zone is covered by CCTV cameras, switcher shall call up the camera views for display on one or more of the dedicated video monitors wired to the switcher. In the case of multiple alarms, applicable camera numbers shall be stored in an alarm queue until zones are manually called up for viewing. First video display out of the queue shall be from the last reported alarm. Active alarms shall cycle between the alarm queue and video monitors as various zones are called up

for viewing. Alarms shall not leave the cycle until secured, reset or placed in access at the alarm reporting and display processor. Additionally, a sequential monitoring capability shall permit alarm reporting and display subsystem operation to view zones in numerical order at an operator adjustable scan rate. Individual cameras shall be capable of being called up to display zones on the video monitors. Manual controls for camera switching shall be from any remote controller connected to the Matrix switcher. Switcher shall be configured [to fit in a standard 480 mm 19 inch rack] [for desk top console operation]. [Switcher shall be tamper alarmed.] Performance requirements shall be as follows:

a. Modular construction shall enable [16] [32] [64] [_____] camera inputs and [4] [8] [16] [_____] monitor outputs.

b. Matrix switcher shall provide optional alarm and communication boards.

c. The Matrix switcher shall allow [1] [_____] remote controllers for system control and operation.

d. Alarm modes shall be automatically enabled or disabled by time of day and day of the week.

e. Operator Registration and System Partitioning: Up to [8] [16] [_____] operator(s) can be registered in a system with different operator access levels. Password protection shall be available to limit operator access. Operator priority shall be available to lock out lower priority operators and to limit operator access to specific cameras and controls.

f. Video connectors: BNC.

2.4.17.4 Video Transmission

Transmission shall be by 75-ohm coaxial cable , twisted pair or fiber optics dedicated to the associated circuit.

Interior cable shall be installed in conduit unless indicated otherwise. Cable shall be designed for the installation method intended. Exterior cable runs shall be underground.

a. Coaxial cable: Coaxial cable used shall provide a DC resistance rating of less than 15 ohm/1000', solid copper center conductor and 95 percent braided, pure copper shield.

b. Twisted pair wire: Use point to point unshielded twisted pair wire, 24-16 AWG, stranded or solid, Category 2 or better. The video signal may co-exist in the same wire bundle as other video, telephone, data, control or low voltage power. The wire shall be installed with no bridge-taps, loading coils, talk-battery or MOV type protectors. The high bandwidth signal will not pass through a telephone switching system, however multiple punch-blocks are okay.

c. Twisted pair wire distance: Distance includes any coax in the path. Wire distance shall be measured to ensure the capability of the product is not exceeded. Wire resistance may be measured with an ohm meter by shorting the two conductors together at the far end and measuring the loop resistance out and back.

d. Twisted pair wire with DVR: When using a digital video recorder, reduce

distance by 25 percent due to lower tolerance of the digital video recorder to synch level and overall video signal quality.

2.4.17.5 Color Video Monitors

a. Except as specified herein, design video monitors to comply with SMPTE 170M for distribution monitors and:

(1) Video monitors shall be designed for continuous operation and shall incorporate printed circuit modular construction.

(2) Monitor design shall provide for easy replacement of printed circuit modules.

(3) Electronic circuits shall use solid-state devices with the exception of the cathode ray tube (CRT).

(4) Each monitor shall be constructed to provide rigid support for electrical systems so that unintentional changes in alignment or microphonic effects will not occur during operation or movement.

(5) Circuit design shall incorporate safety margins of not less than 25 percent where possible, with respect to power dissipation ratings, voltage ratings, and current carrying capacity.

(6) Provide monitors, LCD's or Plasma Displays with a diagonal viewing angle that nominally measures [380][432][508][1067][1270][_____] mm [15] [17] [20][42] [50] [_____] inches.

(7) Provide adequate safeguards to protect personnel from exposure to high voltage during operation or adjustment.

(8) Front panel controls shall include a monitor power switch, horizontal hold, vertical hold, height, contrast, brightness, and focus.

(9) Monitors shall have the following minimum essential requirements:

(a) Resolution: Horizontal resolution for CRT monitors shall not be less than the following: 22.86 centimeter 9 inch monitors - 350 lines; 35.56 centimeter 14 inch monitors - 750 lines; 38.1 centimeter15 inch monitors - 750 lines; 43.18 centimeter 17 inch monitors - 700 lines; 50.8 centimeter 20 inch monitors - 500 lines.

Horizontal resolution for TFT LCD Monitors shall not be less than the following: 26.41 centimeter 10.4 inch monitors - 640 lines; 30.73 centimeter 12.1 inch, monitors - 800 lines; 38.1 centimeter 15 inch monitors - 1024 lines; 43.18 centimeter 17 inch monitors - 1280 lines; 51.05 centimeter 20.1 inch monitors - 800 lines.

(b) Geometry: No point in the active raster shall deviate from its correct position by more than 2 percent of raster height.

b. Mounting and identification

(1) Mount the monitor and other devices subject to burnout or short operating life to facilitate easy replacement.

(2) Label the printed circuit board's function and provide component numbers or markings.

(3) To maintain a standard quality and reliability, components shall be conservatively rated.

(4) Mount TV monitors in a frame for mounting in a [480 mm 19 inch rack] [desk top console].

(5) Two [228] [_____] mm [9] [_____] inch diagonal TV monitors shall be dually mounted in the [rack] [console]. Protect monitors from circuit overloads by fuse or fuses in the power source line. Power source line fuses shall be mounted in finger-operated extractor fuseposts. Fuseholders shall be located in a readily accessible position.

c. Video and signal input

(1) Monitors shall operate with video input requiring a one Vp-p nominal composite video signal switchable to either loop-through or internal 75-ohm terminating impedance.

(2) Signal input shall be BNC connectors.

2.4.17.6 Ancillary Equipment

Equipment shall consist of the items specified below.

a. Video date/time generator: The video time/date shall originate from either the camera, switcher, video, digital video recorder (DVR) or the video matrix switcher.

b. Camera identifiers: Video signal from each camera shall be identified by alpha numeric identifiers. Camera alpha numeric identifiers may originate from either the camera, switcher, digital video recorder or Video Matrix Switcher.

****

NOTE: Digital Video Records are preferred over Video Tape Recorders. DVR's provide larger storage capabilities and faster retrieval of stored data.

****

c. Digital Video Recorder (DVR): The DVR shall provide [4] [9] or [16] [_____]video channels. The DVR will record all cameras onto a hard drive and shall allow remote network viewing via [internet] [intranet] browser. Hard drive capability shall be sized to store all cameras recording 24/7 at [3] [6] [9] [15] [_____] images per second per camera for [1] [2] [4] [_____] weeks. DVR performance shall be as follows:

(1) The DVR shall use modular hard disk media, with a digital format capacity of [160GB] [250GB] [_____]per module.

(2) Include a [4] [9] [16] [_____]channel triplex video multiplexer capable of performing encoding, recording and multiscreen viewing modes simultaneously. Provide [4] [9] [16] channels of live, simultaneous video images in which all 16 channels are refreshed at 60 frames per second.

(3) Furnish 10-100base-T connection for record review and camera view and control on a PC workstation equipped with Microsoft Windows XP Professional operating system software, Microsoft Internet Explorer version 6 or greater Internet Browser Software.

(4) PC workstation Viewing: Each of the ESS PC workstations shall include direct access to each DVR via a Microsoft Internet Explorer Web Browser. All necessary descriptive bookmarks and shortcuts shall be prepared on each PC workstation to allow this direct access. All functions shall be accessible through html commands from a user's web browser interface. Pictures shall be available for attachment via a user-provided SMTP-based email transport system, and included capability for 16 users and 3 user access levels (admin, control and user).

(5) Include 720(H) by 480(V) (Pixel Memory) sampling and 3-D scan conversion to enable jitter-free stabilized pictures in a single frame. Include 720(H) by 240(V) and 320(H) by 240(V) (Pixel Memory) sampling, with 120 Images per second system recording rate. Include Emergency, Event, Schedule and Manual Recording Modes.

(6) Each camera shall support individual Recording Rate and Image Quality settings for each of Emergency, Event, Schedule and Manual Recording Modes. This array of Camera Recording Rate and Image Quality settings by the Recording Modes shall form one of 4 Program Actions. The Program Action shall be assignable to a Time Table to form one of 16 Independent Recording Profiles. Each Recording Profile shall be able to be manually activated, activated via RS-232C interface, automatically activated by Time Table, or activated by separate alarm or emergency inputs.

(7) Furnish digital display on the monitor and also recording of the following information: year, month, day, hour, minute and second, as well as alphanumeric camera location ID up to 8 characters. In addition to monitor display, the date and time shall be recorded on the hard disk. The digital video recorder shall also feature video loss detection on all channels.

(8) Pre-event recording: For all individual camera channels, up to 20 seconds of pre-event pictures shall be buffered simultaneously.

(9) Motion-based Recording: Advanced integrated VMD shall be used to detect a specific area, direction and duration of motion for each camera channel, independently and simultaneously. Motion Search may be executed for a single camera channel for a selected area on the image.

(10) Disk Partitioning: Furnish automated disk management and a RTOS (real-time operating system) platform to include up to [4.8] [_____]TB of digital video storage on a single partition within the DVR. The DVR System shall provide a choice of Physical Partitioning as RAID5 or Disk Mirroring redundant array recording. The operator shall be able to partition the available recording areas in a Virtual Partition by Regular, Event, and Copy Partitions. Manually and Scheduled recorded video information shall be assigned to a Regular Recording Partition, which may be overwritten. Event and Emergency Recording Data shall be

assignable to an Event Partition, where image overwriting shall be prohibited. Any copied data shall be able to be assigned to the Copy Partition, which may be overwritten or saved as required.

(11) Permit direct camera selection for recording playback of any of [4] [9] [16] [_____] video sources at the same time as multiscreen viewing and multiplexed camera encoding (triplex multiplexer capability).

(12) Multiplexer Functions: Built-in programmable switcher with dwell time and camera order programming. The unit shall automatically switch multiple camera images to enable sequential spot monitoring and simultaneous field recording. Separate spot, multiscreen, multiscreen/RGB and cascaded video monitor outputs. The unit shall offer full screen, 4, 7, 9, 10, 13 and 16 multiscreen monitoring modes.

(13) Camera Control: Camera functions and control shall be accessible for all cameras. The multiplexer shall furnish access to all camera control, set-up and alarm functions, including preset sequence, digital motion detector mask set, and back light compensation set-up. Controllable camera functions shall be accessible via front panel controls or the optional system controller. These functions shall include direct access of preset position, zoom (near/far), focus (near/far), iris (open/close) and pan (left/right). Camera functions and control shall be accessible for all cameras through the use of the optional control unit. These functions shall include direct access of preset position, zoom (near/far), focus (near/far), iris (open/close) and pan (left/right).

(14) Outputs: Furnish [4] [9] [16] [_____] looping outputs for connection of all video sources to external monitoring systems including multiscreen and spot monitor video outputs, via BNC female connections. Furnish [4] [_____] channels of audio connection, including audio loop through via RCA phono jacks. Furnish [1] [_____] External Storage connection via High Speed (480 Mbps) Serial Interface. Furnish One [1] [_____] External Copy connection via High Speed (480 Mbps) Serial Interface. Furnish [2] [_____] independent Video Outputs assignable to Multiscreen or Spot functions (both/either). Furnish one [1] [_____] Cascade output for connecting [3] [_____] additional digital video recorder for centralized control using a single video monitor. Furnish virtual camera number programming capability to support 64 camera channels on a single system. Furnish [1] [_____] independent RGB Video output, capable of monitoring all DVR functions.

(15) Indicators: Furnish Alarm, Alarm Suspend, Operate, HDD1, Hard drive identifier, Timer and Error indicators. Furnish Camera Selection, Iris, Preset and Camera Automatic Mode, Pan/Tilt, Set, Jog Dial, Shuttle Dial, Setup/Esc, Record, Search, Play/Pause, Pan/Tilt Slow, Stop, Pan/Tilt Go to Last, Zoom/Focus, A-B, Repeat, Shift, Alarm Reset Buttons. All Camera selection buttons shall have Tri-State Indication, corresponding to Recording, Viewing and Control functions on actual DVR hardware. PC emulation shall not be an acceptable alternative.

(16) Networking: All DVR recording, review, playback, camera control

and setup shall be available via the internally mounted Network Interface. Equip with 10-100base-T connection for record review and camera view and control on a personal computer equipped with Internet Browser Software and an Ethernet 100Base-T connection. Feature shall permit direct camera selection for recording playback of any of [4] [9] [16] [_____] video sources at the same time as multiscreen viewing and multiplexed camera encoding (triplex multiplexer mode). Up to eight [8] [_____] simultaneous clients viewing and [2] [_____] simultaneous FTP sessions shall be supported.

(17) Power: The DVR shall have a power source of [120VAC (50/60 Hz)] [_____].

d. Video tape recorder: Recorder shall be of the helical scan format and shall accept standard 12.7 mm 1/2 inch VHS video cassettes. Time for a stable picture lock from the standby mode shall be 2 seconds or less. Recorder shall provide continuous recording times of 2 hours per cassette. Time lapse recording up to 24 hours selectable shall be possible. Tape motion controls shall be pushbuttons. Provide for remote starting and stopping of video recorder. Recorder shall be capable of stop motion and slow motion. Provide a tracking control to ensure precise tracking of playback. Provide 10 standard 12.7 mm 1/2 inch VHS video cassettes. Mount recorder in a [standard 480 mm 19 inch equipment rack] [desk top console].

(1) Video performance requirements shall be as follows:

(a) Bandwidth: 30 Hz to 3.5 MHz plus or minus one dB, down no more than 4 dB at 5 MHz;

(b) Signal-to-noise ratio: 46 dB peak-to-peak composite signal to rms noise with high energy tape;

(c) Differential gain: 10 IRE units maximum deviation (10 to 90 percent APL);

(d) Input level: 0.5 to 2.0 Vp-p, 1.0 Vp-p nominal;

(e) Output level: One Vp-p composite video into 75 ohms;

(f) Horizontal tilt: Less than plus or minus one percent;

(g) Vertical tilt: Less than plus or minus 5 percent.

(2) Audio performance requirements shall be as follows:

(a) Number of channels: One minimum;

(b) Bandwidth: Audio one 75 Hz to 10 kHz plus or minus 4 dB, audio two 250 Hz to 7.5 kHz plus or minus 4 dB;

(c) Signal-to-noise ratio: 40 dB relative to 3 percent total harmonic distortion (THD) level at one kHz;

(d) Flutter: Less than 0.25 percent rms 0.5 to 250 Hz;

(e) Input: Microphone: 0.4 mV minimum, 200 ohms. Line: minus 20 to 16 dBm, 600 ohms unbalanced or balanced;

(f) Output: Balanced or unbalanced into 600 ohms.

e. Four quadrant multiplexer: Unit shall digitally capture full video from four unsynchronized sources and reduce these images to quarter screen size and combine images to provide a real time video output for display of the four inputs in four quadrants of a single monitor.

(1) Video performance requirements shall be as follows:

(a) Input level: One Vp-p nominal into 75 ohms from a 525 line, 60 fields per second source;

(b) Output level: One Vp-p nominal into 75 ohms;

(c) Alarm inputs: Four, rear panel mounted;

(d) Alarm outputs: Relay contacts, rear panel mounted;

(e) Video inputs: Four, looping;

(f) Switching: Five position, front panel mounted;

(g) Memory: 512 by 512 pixels, minimum, digital; and

(h) Gray scale: 64-level.

2.4.18 Security Command Center (SCC)

The Security Command Center shall integrate all sub systems and communications from and provide operator control interface to ESS. Major components shall be as follows:

a. ESS Software

b. Digital Receiver

c. Monitoring Display Software

2.4.18.1 ESS Software

The ESS software shall utilize a single database for the integration of all sub systems. The integration shall be provided under one operating environment. The System shall archive all events in a database stored either on a local hard drive or a networked database server. The software shall support configuration and simultaneous monitoring of all sub systems.

The software shall allow the configuration of networked PC workstations. The PC workstations and file server shall be connected via a TCP/IP network. Administrative tasks such as configuration, monitoring, schedules, report generation and graphic map display shall be provided from any PC workstation on the network. All system programming data shall reside on the single database and shall be instantly accessible to every PC Workstation connected to the network. The system shall utilize a non-proprietary SQL-based, ODBC-compliant database, managed by Sybase Adaptive Server Anywhere, Microsoft SQL Server, or Oracle.

The ESS shall utilize a preemptive multi-tasking operating system: Microsoft Windows 2000, 2003 or Windows XP Professional environment. The

System shall be designed to utilize the capabilities of multitasking operation, with many processes running at the same time without interference with each other and with higher priority tasks taking precedence over lower priority tasks.

The ESS software shall support responses to alarms entering the system. Each alarm shall be capable of initiating one or more of the following actions: sending alarm commands to a CCTV system interface, triggering DVR event recording, activating output devices, playing PC audio files, controlling doors, and displaying floor-plan graphical maps associated with the alarm device. The system shall provide mode of system operation that requires operator acknowledgment of any alarm.

The ESS software shall be capable of, but not limited to, the following programming and functionality:

a. Daylight Savings Time Adjustment: There shall be a software-configurable, user defined adjustment for Daylight Savings Time. The ACU(s) and PCU(s) shall not need to be connected to the ESS in order for the adjustment to occur.

b. Operator Privileges: An unlimited number of system operators shall be supported, each with a unique login and password combination. Operators shall be assigned privileges based on the loops, commands, or programming features that are available to each individual operator.

c. Alarm Priorities: Each alarm device shall have the ability to be user configured to belong to one of [10,000] [_____] priority levels. Priority levels are numbers assigned to an alarm based on the importance of the alarm. [9,999] [_____] is the highest and most critical level of alarms. [0] [_____] is the least significant. These priorities shall define which alarm events to display on individually specified ESS workstations.

d. Reports: The ESS shall include integrated reporting capabilities as well as the ability to run Crystal Report templates.

e. User Interface: The ESS programming shall be menu-driven, with "wizards" to assist with software configuration, and shall include on-line 'Help' information.

f. Messages: The ESS shall permit the use of user-selected colors for event messages.

g. Graphics: The ESS shall be capable of displaying a floor-plan graphic for card activity and alarm events as part of the ESS integration.

h. Device Status: The ESS shall be capable of displaying the dynamic status of a user-selected list of devices, including doors, inputs, and outputs.

i. Diagnostics: The ESS shall include diagnostic software tools that interface and query the hardware for information and to issue commands.

j. Mandatory Data Fields: The ESS shall require any cardholder data field to be selected by the user as mandatory. Mandatory data fields are to force ESS operators to input data that is required for proper system configuration.

k. User Defined Data Fields: The ESS shall provide [20] [_____] unassigned data fields for storing user-defined data. The data fields shall support user-defined labels, and shall be user-configurable as plain text fields or drop-down selection lists.

l. Archive Database: The ESS shall include a connection to an archive database, which stores purged events and deleted programming, and which can be accessed for reporting.

m. Programmable Database Backup: The ESS shall include the capability of performing user-scheduled database backups, without the use of third-party backup software.

n. Programmable Database Purging: The ESS shall include the capability of performing user-scheduled database purging, moving selected events to an archive database when the events have aged a user-specified number of days.

o. Database Importing: The ESS shall include the capacity to import user data from an ODBC datasource (Access, Excel, text).

p. Data Exporting: The ESS shall include the capacity to export data from any table in the database to either a text or HTML file, in any user-selected order.

q. Event Log Output: The ESS shall include the capacity to send a continuous stream of user-selected types of event messages to a text file, serial port, or TCP/IP address.

r. Data Audit Trail: The ESS shall record changes to programming, recording the date/time stamp of the change, the name of the operator making the change, and the nature of the change. This data audit shall be available in history for reporting.

2.4.18.2 Digital Receiver

The digital receiver system shall be capable of monitoring PCU digital dialers, data networks and TCP/IP network communications of IDS account zones on the same receiver. The digital receiver enclosure shall house the processor card rack, modem rack, data rack and convenience panel. Built into the front of the digital receiver enclosure shall be an LCD display for viewing incoming reports with a keypad for acknowledging reports and configuring the system and its components. The digital receiver enclosure shall contain internal cards consisting of a processor board, [3] [_____] line cards, modem power supply card, multibus power supply card, and transformer card.

The digital receiver shall be capable of, but not limited to, the following programming and functionality:

a. The digital receiver shall provide SCC with computerized monitoring of PCU communication format of Synchronous Data Link Control (SDLC). Digital receiver features shall include automatic logging of alarm, trouble, and supervisory account reports on a local printer with date and time of their occurrence. Capacity of up to [65,535] [_____] digital dialer or direct dedicated account zones for alarm, trouble, user and system reports.

b. The Digital receiver shall provide SCC with computerized monitoring of

PCU communication format of Host asynchronous (HOST). Digital receiver features shall include automatic logging of alarm, trouble, and supervisory account reports on a local printer with date and time of their occurrence. Capacity for alarm, trouble, user and system reports up to [65,535] [_____] host account zones that do not check in and [2,500] [_____] accounts that do check in.

c. LCD Display and Keypad: The LCD display shall allow the SCC operator to view alarm reports before acknowledging the alarms using the system keypad. The LCD and keypad shall be built-in to the front of the digital receiver enclosure. The LCD and Keypad are used as a backup when the ESS is not available during maintenance or unplanned system outages.

d. Printer: Routine reports shall be logged on an optional printer without need of operator response. Supervisory and alarm reports shall be logged on the printer and displayed on the LCD for operator acknowledgement. Report capability shall be the over all role of the ESS.

(1) Additional Reports: Receiver shall be able to process additional reports transmitted to it by PCU(s):

(a) Addition and deletion of code numbers including user number of the person making the change.

(b) Bypassing and resetting of zones by number and name including the user number of the person making the change.

(c) Schedule changes including user number of the person making the change.

(d) Trouble and Restoral report by zone name and number.

(e) Door access reports including user number and number of the door being accessed.

e. Communication and Line Capacity:

(1) The digital receiver shall be capable of communication using the IBM Synchronous Data Link Control format.

(2) The digital receiver shall accommodate up to [5] [_____] incoming lines.

(3) Digital receiver shall have the ability to be configured with PCU(s) digital dialer, data network and TCP/IP network communication receiving lines.

(4) PCU(s) digital dialer lines shall have a capacity of [65,535] [_____] separate accounts.

(5) Data TCP/IP network lines shall have a capacity of [65,535] [_____] separate accounts that do not check in or [2,500] [_____] separate accounts that do check in.

f. Digital Receiver Enclosure:

(1) Digital receiver enclosure shall provide housing for the

processor, power supply, line cards, and associated cables. The enclosure shall measure 22.22 centimeter 8.75 inches high, 48.22 centimeters 19 inches wide and 30.48 centimeters 12 inches deep. (2) Contained in the top of the system enclosure is the modem rack. The rack shall hold the modem power supply card and up to [5] [_____] line cards. The transformer card for connecting the [120] [_____] VAC shall be mounted on the rear of the rack modem. (3) Contained in the bottom of the system enclosure is the multibus rack with cooling fan. The multibus rack holds the processor card and the multibus power supply card.

g. Processor Card: The main system processor shall control the line cards, the LCD display, the built-in keypad, and the printer. The processor shall contain the firmware for system operation, the EEPROM memory of operator codes, line configuration, and perform all time keeping functions.

h. Line Card:

(1) Line card shall provide for [1] [_____] incoming line of PCU digital dialer, data network or TCP/IP network communication to PCU(s). Each line card shall have one 10-position flat cable for connection to the processor card and one connector for a phone line or data network line from an RJ11X connection block.

(2) When the line card is configured for PCU digital dialer operation, the line card shall monitor the incoming phone line voltage. During a loss of phone line voltage, a red Phone Line Fail LED shall light and an alert sound. The alert shall be silenced by pressing the silence switch on the card or software control from ESS. The LED shall remain lit until the phone line is restored.

(3) Line card shall have a green LED labeled PWR to be lit when the power supply on the line card is in a good condition.

(4) Line card shall have six yellow LEDs indicating the condition of the line card during various stages of communication. Stages indicated shall be: Transmit Data, Receive Data, Carrier Detect, On Line, Ring Detect, and Data Terminal Ready.

(5) A Network Interface Card (NIC) shall be integral to the digital receiver with a built in TCP/IP network router. External network routers are not acceptable for Ethernet and Internet/Intranet monitoring.

(6) A Network Interface Card (NIC) shall be integral to the receiver with built in network router capable of 128 Bit AES Rijndael Encryption process certified by NIST (National Institute of Standards and Technology).

i. Modem Power Supply Card:

(1) Modem power supply card shall provide power for up to [5] [_____] line cards. Power shall be supplied through the modem rack backplane connectors without additional cabling. The modem power supply card shall also provide monitoring for the LCD connection, UPS system status and [120] [_____] VAC input to the digital receiver.

(2) Modem power supply card shall have a green LED labeled PWR. The PWR LED will light when the power supply to the modem power supply card is in good condition. There shall also be a red LED labeled PWR TRBL, which will light when there is a power problem on the modem power supply card along with sounding an alert. The alert shall be able to be silenced by pressing a silence switch on the modem power supply card or software control from ESS. The red LED shall remain lit until power problem is corrected.

(3) Modem power supply card shall have a trouble LED for the LCD that lights and sounds an alert when the LCD is unplugged. The alert shall be able to be silenced by pressing a silence button on the modem power supply card or software control form ESS.

(4) Modem power supply card shall have a trouble LED for the UPS that lights and sounds an alert when the UPS Brownout input is opened. The alert shall be able to be silenced by pressing a silence button on the modem power supply card or software control form ESS.

(5) Modem power supply card shall have a trouble LED for the AC power to the transformer card that lights and sounds an alert when the AC power to the transformer card fails. The alert shall be able to be silenced by pressing a silence button on the modem power supply card or software control form ESS.

j. Special Applications Features: Receiver shall be able to act as a communications path to panels for "Trapping" of PCU(s) for Remote Programming/Interrogation processes. Receiver shall work in conjunction with the ESS in pass thru configuration with an Automation System to "Trap" a PCU and send notification for the panel to contact the remote link Programming Software for remote interrogation in a Network Application. (TCP/IP Network Trapping).

k. Multibus Power Supply Card

(1) Multibus power supply card shall provide power to the processor card through the multibus backplane. It also shall be able to monitor the condition of the processor card, the voltage output of the modem power supply card and its own internal voltages.

(2) Multibus power supply card shall monitor the processor through the multibus backplane. There shall be a green OK LED that will light when the processor is operating normally. If the processor stops operating, the red FAIL LED will light and failure buzzer shall sound. The system shall restart after the restart button on the multibus power supply card is pressed. System restart button shall not change system configuration.

(3) Multibus power supply card shall monitor three different system voltages, +5, +12, -12 and the modem power supply. Four LEDs shall be located on the multibus power supply card to display any voltage failures.

l. Transformer Card: Transformer card shall provide power to the modem power supply card and the multibus power supply card. It shall also have a power cord for connecting to the multibus rack-cooling fan.

m. Power Cable: Power cable shall be 61 centimeters 2 feet long and connect the different system voltages the transformer card and the

multibus power supply card.

n. Convenience Panel: Convenience panel shall provide cabling for [2] [_____] RS-232 ports. The ports shall be for the host output, activity log printer(s) and auxiliary communications.

o. Printer and Cable:

(1) Printer shall be an 80-column serial printer with a 10-foot RS-232 cable. The printer can be connected to the all events output connector or the alarm only output connector.

(2) Printer shall be configured to 1200 baud, 8 data bits, 1 stop bit and even parity.

p. LCD Display and Keypad

(1) LCD display shall be a 32-character LCD display with a keypad for entry of information and acknowledgment of alarm signals.

(2) LCD display shall be built-in to the front of the system enclosure.

(3) Power shall be provided from the multibus power supply card.

2.4.18.3 Printer Requirements

a. Report Printer: A laser text printer shall be provided for the purpose of generating reports. The printer shall be a parallel or USB interface dry-type laser process printer. The unit shall print a minimum of 8 pages per minute at 600 dpi resolution.

b. Badge Printer: A dye-sublimation/resin thermal transfer type image printer shall be provided for Badge Identification credentials. The printer shall be capable of printing two sides, edge to edge, directly onto a white-unfinished 0.030 PVC, PVH or PVCH card a rate of approximately 80 seconds per card. An encoder is available to be an integral part of the printer. The unit shall be capable of providing magnetic stripe encoding of all credentials utilizing an on-line magnetic stripe encoder device. The magstripe fields shall be sent to the encoder automatically from the System. The encoding shall conform to ABA Track II and ANSI specifications.

2.4.18.4 ESS Monitor Display Software

ESS Monitor display software shall provide for text and graphics map displays that include zone and device 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.

2.4.18.5 Graphical Map Software

ESS graphical map software shall show the [graphic and] visual data of all subsystem devices. A [19][21][30][42] [_____] color-graphic CRT, LCD flat screen or plasma display shall be used with messages displayed in the English language. Graphical maps shall be provided showing a layout of all the protected facilities. Zones corresponding to those monitored by the ESS shall be highlighted on the graphical maps. Status of each zone shall be displayed using graphical icons as required within each designated zone. Graphical maps shall have the capability of be linked together using a layered tree structure. For example, a top-level map might be a top view of the site and its buildings, the next level the individual buildings floor, followed by a map of the area on a floor containing the device in alarm. The graphical map software shall allow for [3] [6] [_____] layers of maps to be defined for any given ESS device. To speed the location of an incident, each map level contains a clearly visible indicator as to which sub map the operator should select next to find the device that is in alarm.

The ESS may also be configured to display a map automatically on presentation of a new alarm, providing the operator with prompt visual indication that an alarm condition has occurred.

The status of intrusion devices, access control readers, doors, auxiliary monitor points and auxiliary outputs can be requested from any map by simply selecting the icon representing the device and its current state will be displayed. With the associated management module installed, CCTV camera control, Digital video review, alarm panel transactions and Intercom requests are all available for inclusion on the map.

SCC operators shall be able to change a current setting by pressing the right mouse button anywhere on the screen or on a specific system device icon. Pressing the right mouse button will cause the appropriate command options list to appear for selection. Having selected a command, confirmation is provided by reflecting the change in status on the display.

The display of intrusion or auxiliary door alarms may be automatically enabled or disabled by the use of timed commands, either by device or by a group of devices. This may be used, for example, to disable all door alarms on internal doors, during normal office hours.

Maps may be created using standard office tools such as Paint® or drawing packages such as AutoCAD®. Drawings shall be able to be imported in Jpeg, Bitmap, Windows metafile or DXF file formats to provide maximum flexibility.

2.4.18.6 Control and Display Integration

Accomplish so that SCC controls are human engineered as specified in paragraph entitled "Human Engineering" so the entire SCC can be operated by a single or multiple operator(s). In addition, switching and monitoring components of the assessment subsystem shall also be integrated with the SCC so that SCC operator(s) can effectively monitor, assess alarms and control the ESS. [Method of system integration shall be as a single console. Provide chassis, modules, and furniture required for console configuration of SCC.]

2.5 FIELD FABRICATED NAMEPLATES

ASTM D709. Provide laminated plastic nameplates for each equipment enclosure, relay, switch, and device; as specified or as indicated on the drawings. Each nameplate inscription shall identify the function and, when applicable, the position. Nameplates shall be melamine plastic,3 mm (0.125 inch) 0.125 inch thick, white with [black] [_____] center core. Surface shall be matte finish. Corners shall be square. Accurately align lettering and engrave into the core. Minimum size of nameplates shall be 25 by 65 mm (one by 2.5 inches) one by 2.5 inches. Lettering shall be a minimum of 6.35 mm (0.25 inch) 0.25 inch high normal block style.

2.5.1 Manufacturer's Nameplate

Each item of equipment shall have a nameplate bearing the manufacturer's name, address, model number, and serial number securely affixed in a conspicuous place; the nameplate of the distributing agent will not be acceptable.

2.6 FACTORY APPLIED FINISH

Electrical equipment shall have factory-applied painting systems which shall, as a minimum, meet the requirements of NEMA 250 corrosion-resistance test

PART 3 EXECUTION

3.1 EQUIPMENT INSTALLATION

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.

3.1.1 Cable and Wire Runs

****

NOTE: Where design requirements must conform to NACSIM 5203, "Guidelines for Facility Design and RED/BLACK Installation," refer to Military Handbook MIL-HDBK-232.

****

NFPA 70 [and] [Section 26 20 00 INTERIOR DISTRIBUTION SYSTEM,] [applicable DOD directives] [, DIA DCID 6/9], and as specified herein. Conduits including flexible metal and armored cable shall terminate in the sensor or device enclosure. Ends of conduit shall be fitted with insulated bushings. Exposed conductors at ends of conduits external to sensors and devices are not acceptable.

3.1.2 Soldering

ASTM B32. For soldering electrical connections, use composition Sn60, Type AR or S, for general purposes; use composition Sn62 or Sn63, Type AR or S, for special purposes. When Type S solder is used for soldering electrical connections, flux shall conform to ASTM B32.

3.1.3 Galvanizing

Ferrous metal shall be hot-dip galvanized in accordance with ASTM A123/A123M. Screws, bolts, nuts, and other fastenings and supports shall be corrosion resistant.

3.1.4 Fungus Treatment

Completely treat system components for fungus resistance. Do not use treated materials containing mercury-bearing fungicide. Treating materials shall not increase flammability of material or surface being treated. Treating materials shall not cause skin irritation or other personnel injury during fabrication, transportation, operation, or maintenance of equipment, or during use of finished items when used for the purpose intended.

3.1.5 Conduit

****

NOTE: Where design requirements must conform to NACSIM 5203, "Guidelines for Facility Design and RED/BLACK Installation," refer to Military Handbook MIL-HDBK-232.

****

Install in accordance with NFPA 70 and Section 26 20 00 INTERIOR DISTRIBUTION SYSTEM.

3.1.6 Underground Cable Installation

Underground conductors connecting protected structures and objects to the central alarm updating and display unit shall be run direct burial or in conduit as specified in Section 33 71 02 UNDERGROUND ELECTRICAL DISTRIBUTION. Coaxial cable shall not be spliced. If permitted, cables connecting protected structures and objects to the security control console shall be sized such that initially only approximately 60 percent of the circuit pairs will be used. Cable pairs not used shall be reserved for future use of additional detection circuits.

3.1.7 Exterior Fences

****

NOTE: Coordinate this requirement with requirements of Section 32 31 13 CHAIN LINK FENCES AND GATES.

****

Preparation of existing fences [or installation of new fences] shall ensure a rigid fence system for installation of fence-mounted detection systems or a detection system where loose fence fabric might prove troublesome. A rigid fence and fence fabric shall be ensured to minimize nuisance alarms. Fences shall be additionally braced, provided with fabric ground anchors or curbs, tensioning devices, top and/or bottom rails, soft-seated gate latches, and reanchored outriggers for barbed wire to ensure a vibration-free installation. Relocate large signs which are fence supported to separate support posts to preclude interference with fence detection systems.

3.2 ADJUSTMENT, ALIGNMENT, SYNCHRONIZATION, AND CLEANING

Subsequent to installation, clean each system component of dust, dirt, grease, or oil incurred during installation or accrued subsequent to installation from other project activities, and prepared for system activation by manufacturer's recommended procedures for adjustment, alignment, or synchronization. Prepare each component in accordance with appropriate provisions of component installation, operations, and maintenance manuals. Remove large vegetation that may sway in the wind and touch fencing.

3.3 ESS System Acceptance and Training

3.3.1 ESS System Acceptance Test

ESS System Acceptance testing shall be performed as follows;

a. The NAVFAC and NAVFAC Engineer will conduct final acceptance testing of the system.

b. Prior to the final acceptance test, security contractor shall conduct a complete test of the entire ESS including subsystems and provide the NAVFAC and NAVFAC Engineer with a written report.

c. Following completion of the initial testing and correction of any noted deficiencies, conduct a five-day burn-in test, intent of the burn-in test shall be to prove the ESS by placing it in near real operating conditions. During this period the ESS shall be fully functional and programmed such that all points, interfaces, controls, reports, messages, prompts, etc. can be exercised and validated. Record and correct any system anomaly, deficiency, or failure noted during this period. Scheduling of the final acceptance test shall be based on a review of the results of this burn-in test.

d. Deliver a report describing the results of the functional tests, burn-in tests, diagnostics, calibrations, corrections, and repairs including written certification to the NAVFAC and NAVFAC Engineer that the installed complete ESS has been calibrated, tested, and is fully functional as specified herein.

e. Prior to the final acceptance test, complete all clean-up and patch work requirements. Security equipment closets and similar areas shall be free of accumulation of waste materials or rubbish caused by operations under the Contract At completion of the Work, remove all waste materials, rubbish, contractor tools, construction equipment, machinery and all surplus materials.

f. Upon written notification from the Contractor that the ESS is completely installed, integrated and operational, and the burn-in testing completed, the NAVFAC and NAVFAC Engineer will conduct a final acceptance test of the entire system at a mutually acceptable time.

g. During the final acceptance test, no adjustments, repairs or modifications to the system shall be conducted without the permission of the NAVFAC.

h. During the course of the final acceptance test by the NAVFAC and NAVFAC Engineer, the Contractor shall be responsible for demonstrating that, without exception, the completed and integrated ESS complies with the

contract requirements. Physical and functional requirements of the project shall be demonstrated and shown. This demonstration will begin by comparing as-built drawings conditions of the ESS to requirements outlined in this Section, item by item. Following the Section compliance review, ESS and SCCd equipment will be evaluated.

i. The functionality of the various interfaces between systems will be tested.

j. The installation of all field devices will be inspected. This field inspection will weigh heavily on the general neatness and quality of installation, complete functionality of each device, and compliance with mounting, back box and conduit requirements.

k. All equipment shall be on and fully operational during any and all testing procedures. Provide personnel, equipment, and supplies necessary to perform all site testing. Provide a minimum of two Contractor employees familiar with the ESS for the final acceptance test. One contractor employee shall be responsible for monitoring and verifying alarms while the other will be required to demonstrate the function of each device. Supply at least two radios or portable telephones for use during the test.

l. The NAVFAC and NAVFAC Engineer retain the right to suspend, terminate or reschedule testing at any time when the ESS is found to be incomplete or fails to perform as specified. In the event that it becomes necessary to suspend, terminate or reschedule the test, all of the NAVFAC and NAVFAC Engineers fees and expenses related to the test shall be deducted from the Contractor's retainage. In the event it becomes necessary to suspend, terminate or reschedule the test, the Contractor shall work diligently to complete and/or repair all outstanding items as required by the Contract Documents. The Contractor shall supply the NAVFAC and NAVFAC Engineer with a detailed punch list completion schedule outlining task-by-task completion dates and a tentative date for a subsequent retest. During the final acceptance test, no adjustments, repairs or modifications to the system shall be conducted without the permission of the NAVFAC Engineer and NAVFAC.

3.3.2 ESS Training Outline

Provide training as coordinated with the NAVFAC. The following training program is intended to identify typical training requirements and may be modified and/or amended to meet specific NAVFAC training requirements.

3.3.2.1 ESS Administrator Training

****

NOTE: For NAVFAC ML and other EFD's with a designated IDS engineer, select the first bracketed option for all projects. In all other areas, select the second bracketed option for all projects.

****

a. ACS and IDS Administrator Training shall include:

(1) [two] [_____] eight-hour on-site training sessions.
(2) Operating system procedures and configuration.
(3) Operator functions.
(4) Database functions and setup.

(5) Cardholder input and deletion procedures.
(6) Report generation.
(7) Applications programs (as applicable).
(8) Graphics generation and manipulation.
(9) Items unique to the ACS and IDS interfaces with other systems

b. CCTV System Administrator Training shall include:

(1) [One] [_____] eight-hour session on site.

(2) Training shall include all administrator and operator functions, and items unique to the installed CCTV System and the interfaces with other systems.

3.3.2.2 ESS Operator Training

Coordinate the operator training syllabus with NAVFAC prior to conducting operator training.

a. ACS and IDS Operator Training shall include:

(1) [Four] [_____] (one-day) [8] [_____] hours on-site training sessions.
(2) System operating procedures.
(3) System configuration orientation.
(4) Alarm acknowledgment.
(5) Alarm response logging.
(6) Graphics functionality.
(7) Items unique to the ACS and IDS interfaces with other systems.

b. CCTV Operator Training shall include:

(1) [Two] [_____] (one-day) [8] [_____] on-site training sessions.
(2) Training shall include:
(3) Operating procedures.
(4) System configuration.
(5) Video call-up.
(6) Camera and monitor control.
(7) Graphics functionality.
(8) Basic device terminology and troubleshooting.

3.3.3 Follow-up Training

a. [One] [_____], [two] [_____] hour training session each month for [two] [_____] months after initial training.

b. Follow-up training shall begin one month after initial training.

c. Training shall include testing for system competence.

3.3.4 Training Operating and Maintenance Personnel

Furnish instruction for operating staff in system operation and operator troubleshooting and preventive maintenance procedures. Instruction shall consist of [3] [_____] man-days, 8 hours per day, and shall be held during normal duty hours. Commence instruction after system is fully operational, and complete instruction prior to system acceptance and turnover to the Government. [Furnish maintenance instruction for Government maintenance personnel in adjustment, operation, and maintenance of [each system

equipment] [_____]. Attendance at equipment manufacturer's recommended maintenance training schools may be substituted for this training. Costs associated with such schooling, less travel and per diem, shall be borne by the Contractor. Complete maintenance instruction prior to system acceptance and turnover to the Government.]

3.4 FIELD APPLIED PAINTING

Paint electrical equipment as required to match finish of adjacent surfaces or to meet the indicated or specified safety criteria. Painting shall be as specified in Section 09 90 00 PAINTS AND COATINGS

3.5 NAMEPLATE MOUNTING

Provide number, location, and letter designation of nameplates as indicated. Fasten nameplates to the device with a minimum of two sheet-metal screws or two rivets.

-- End of Section --