****
USACE / NAVFAC / AFCEC **UFGS-28 10 05 (May 2024)**

Preparing Activity: USACE **Superseding**
UFGS-28 10 05 (May 2016)

UNIFIED FACILITIES GUIDE SPECIFICATIONS

References are in agreement with UMRL dated January 2025
****

SECTION TABLE OF CONTENTS

DIVISION 28 - ELECTRONIC SAFETY AND SECURITY

SECTION 28 10 05

ELECTRONIC SECURITY SYSTEMS (ESS)

05/24

2.3.7.2.5 Dual Technology Sensors
2.3.7.2.6 Bistatic Microwave Sensor
2.3.7.2.7 Monostatic Microwave Sensor
2.3.7.2.8 Passive Infrared Sensor (Exterior)
2.3.7.2.9 Buried Ported Cable
2.3.7.2.10 Active Infrared Sensor (Exterior)
2.3.7.2.11 Video Motion Sensor (Exterior)
2.3.7.2.12 Radar
2.3.7.3 Duress Alarms (Hold Up Switch)
2.3.7.3.1 Hardwire Duress Alarms
2.3.7.3.2 Wireless Duress Alarms
2.3.7.4 Tamper Switches
2.3.7.4.1 Tamper Switch Performance Requirements
2.3.8 Intrusion Detection System Date and Time
2.4 ACCESS CONTROL SYSTEM (ACS)
2.4.1 ACS Badging Requirements
2.4.2 ACS Programming
2.4.2.1 Time Schedules
2.4.2.2 Special Days
2.4.2.3 ACU Daylight Savings Time Adjustment
2.4.2.4 Scheduled Events
2.4.2.5 Maximum User Capability
2.4.2.6 Access Groups
2.4.2.7 Active and Expire Dates
2.4.2.8 Maximum Use Settings
2.4.2.9 Door Outputs
2.4.2.10 Anti-Passback
2.4.2.11 Two Person Rule
2.4.2.12 User List or Who's In (Muster Reports)
2.4.2.13 Crisis Mode
2.4.2.14 Door Groups
2.4.2.15 Door Interlocking
2.4.2.16 PIN Required
2.4.2.17 Remote Door Control
2.4.2.18 Key Control
2.4.2.19 Guard Tour
2.4.2.20 Reader Disable
2.4.2.21 Disable Event Messages
2.4.2.22 Input and Output Groups
2.4.2.23 Delays
2.4.2.24 Remote Input Control
2.4.2.25 Output Configuration
2.4.2.26 Remote Output Control
2.4.2.27 Remote Reset Command
2.4.2.28 Time Zone
2.4.2.29 User-Selected LED Behavior
2.4.2.30 Traced Cards
2.4.2.31 Badge Print Tracking
2.4.3 Error and Throughput Rates
2.4.4 Access Control System Central Processing
2.4.5 Access Control Unit(ACU)
2.4.6 Access Control Devices
2.4.6.1 Card Readers
2.4.6.1.1 Contact Card Readers
2.4.6.1.2 Contactless Card Readers
2.4.6.1.3 Card Readers With Integral Keypad and Biometric Reader
2.4.6.1.4 Card Readers with Integral Keypad
2.4.6.1.5 Card Reader Display
2.4.6.1.6 Card Reader Response Time

2.4.6.1.7 Card Reader Power
2.4.6.1.8 Card Reader Mounting Method
2.4.6.2 Keypads
2.4.6.2.1 Keypad Display
2.4.6.2.2 Keypad Response Time
2.4.6.2.3 Keypad Power
2.4.6.2.4 Keypad Mounting Method
2.4.6.2.5 Keypad Duress Codes
2.4.6.3 Access Control Cards
2.4.6.3.1 Credential Card Modification
2.4.6.3.2 Card Size and Dimensional Stability
2.4.6.3.3 Card Materials and Physical Characteristics
2.4.6.3.4 Card Construction
2.4.6.3.5 Card Durability and Maintainability
2.4.6.3.6 Warranty
2.4.6.4 Personal Identity Verification Equipment
2.4.6.4.1 Hand Geometry
2.4.6.4.1.1 Template Update and Acceptance Tolerances
2.4.6.4.1.2 Average Verification Time
2.4.6.4.1.3 Modes
2.4.6.4.1.4 Reports
2.4.6.4.1.5 Electrical
2.4.6.4.1.6 Mounting Method
2.4.6.4.1.7 Communications Protocol
2.4.6.4.2 Fingerprint Analysis Scanner
2.4.6.4.2.1 Template Update and Acceptance Tolerances
2.4.6.4.2.2 Average Verification Time
2.4.6.4.2.3 Modes
2.4.6.4.2.4 Reports
2.4.6.4.2.5 Electrical
2.4.6.4.2.6 Mounting Method
2.4.6.4.2.7 Communications Protocol
2.4.6.4.3 Iris Scan Device
2.4.6.4.3.1 Display Type
2.4.6.4.3.2 Template Update and Acceptance Tolerances
2.4.6.4.3.3 Average Verification Time
2.4.6.4.3.4 Modes
2.4.6.4.3.5 Reports
2.4.6.4.3.6 Electrical
2.4.6.4.3.7 Mounting Method
2.4.6.4.4 Facial Scanner
2.4.6.4.4.1 Template Update and Acceptance Tolerances
2.4.6.4.4.2 Average Verification Time
2.4.6.4.4.3 Modes
2.4.6.4.4.4 Reports
2.4.6.4.4.5 Electrical
2.4.6.4.4.6 Mounting Method
2.4.6.4.4.7 Communications Protocol
2.4.6.4.5 Palm Scanner
2.4.6.4.5.1 Template Update and Acceptance Tolerances
2.4.6.4.5.2 Average Verification Time
2.4.6.4.5.3 Modes
2.4.6.4.5.4 Reports
2.4.6.4.5.5 Electrical
2.4.6.4.5.6 Mounting Method
2.4.6.4.5.7 Communications Protocol
2.4.6.5 Portal Control Devices
2.4.6.5.1 Push-Button Switches
2.4.6.5.2 Panic Bar

2.4.6.5.2.1 Emergency Egress With Alarm
2.4.6.5.2.2 Normal Egress
2.4.6.5.2.3 Delay Egress With Alarm
2.4.6.5.3 Electric Door Strikes and Bolts
2.4.6.5.3.1 Solenoid
2.4.6.5.3.2 Signal Switches
2.4.6.5.3.3 Tamper Resistance
2.4.6.5.3.4 Size and Weight
2.4.6.5.3.5 Mounting Method
2.4.6.5.3.6 Astragals
2.4.6.5.4 Electrified Mortise Lock
2.4.6.5.4.1 Solenoid
2.4.6.5.4.2 Signal Switches
2.4.6.5.4.3 Power Transfer
2.4.6.5.4.4 Size and Weight
2.4.6.5.4.5 Mounting Method
2.4.6.5.5 Electromagnetic Lock
2.4.6.5.5.1 Armature
2.4.6.5.5.2 Tamper Resistance
2.4.6.5.5.3 Mounting Method
2.4.6.5.6 Entry Booth
2.4.6.5.6.1 Local Alarm Annunciation
2.4.6.5.6.2 Terminal and Facility Interface Device Support
2.4.6.5.6.3 Response Times
2.4.6.5.6.4 Autonomous Local Control
2.4.6.5.6.5 Entry Booth Local Processor Subsystem Capacities
2.4.6.5.6.6 Diagnostics
2.4.6.5.6.7 Memory Type and Size
2.4.6.5.6.8 Tamper Protection
2.4.6.5.6.9 Entry Booth Configuration
2.4.6.5.6.10 Entry Booth Operation
2.4.6.5.6.11 Display Type
2.4.6.5.6.12 Lighting
2.4.6.5.6.13 Heating and Ventilation Equipment
2.4.6.5.6.14 Entry Booth Wall and Frame Construction
2.4.6.5.6.15 Entry Booth Doors
2.4.6.5.6.16 Entry Booth Floor Construction
2.4.6.5.6.17 Electrical Requirements
2.4.6.5.6.18 VSS Camera
2.4.6.5.6.19 Weight Check Monitor
2.4.6.5.6.20 Double Occupancy Sensor
2.4.6.5.6.21 Intercom
2.4.6.5.6.22 Voice Prompts
2.4.6.5.7 Vehicle Gate Operator
2.4.6.5.7.1 Input Power
2.4.6.5.7.2 Audible Warning
2.4.6.5.7.3 Maximum Run Timer
2.4.6.5.7.4 Adjustable Load Monitor for Obstruction Sensing
2.4.6.5.7.5 Operator Override Controls
2.4.6.5.7.6 Limit Switches
2.4.6.5.7.7 Type of Gate
2.4.6.5.7.8 Safety
2.4.6.6 Active Barrier Interface
2.4.7 Elevator Control
2.4.7.1 Control Elevator Operation with Entry Control Terminal Devices
2.4.7.2 Floor Tracking
2.4.8 Access Control System Date and Time
2.5 VIDEO SURVEILLANCE SYSTEM (VSS)

2.5.1 Cameras
2.5.1.1 VSS Camera
2.5.1.1.1 Sensitivity
2.5.1.1.2 Signal-To-Noise Ratio
2.5.1.1.3 Resolution
2.5.1.1.4 Synchronization
2.5.1.1.5 Low Light Level
2.5.1.2 Camera Lenses
2.5.1.3 Camera Housing and Mounts
2.5.1.3.1 Environmentally Sealed Camera Housing
2.5.1.3.2 Indoor Camera Housing
2.5.1.3.3 Interior Mount
2.5.1.3.4 Low Profile Ceiling Mount
2.5.1.3.5 Interior Dome Housing
2.5.1.3.6 Exterior Dome Housing
2.5.1.3.7 Exterior Wall Mount
2.5.1.3.8 Pan-Tilt Mount
2.5.1.3.9 Explosion Proof Housing
2.5.2 Thermal Imaging System
2.5.3 Video Analytics (VA)
2.5.3.1 Software
2.5.3.1.1 Basic Motion Detection
2.5.3.1.2 Advanced VA
2.5.3.1.2.1 Intruder Identification
2.5.3.1.2.2 Environmental Compensation
2.5.3.1.2.3 Counting
2.5.3.1.2.4 Directional Identification
2.5.3.1.2.5 Item Recognition
2.5.3.1.2.6 Subject Tracking
2.5.3.1.2.7 Multiple Subject Tracking
2.5.3.1.2.8 Object Left Behind
2.5.3.2 Embedded VA
2.5.3.2.1 Intelligent Video Analysis
2.5.3.2.2 Motion Tracking with PTZ Cameras
2.5.4 Color Computer Monitors
2.5.4.1 Mounting
2.5.4.2 Video and Signal Input
2.5.5 Ancillary Equipment
2.5.5.1 Video System Date and Time
2.5.5.2 Camera Identifiers
2.5.5.3 Video Recording
2.5.5.3.1 Analog to IP Video Converter
2.5.5.3.2 IP Based Video Recording Device/System
2.5.5.3.3 Video Recording Performance
2.5.5.3.4 Recording Audio With Video
2.5.5.4 Camera Control
2.5.6 Camera Mounting Structures
2.5.7 Video Surveillance System (VSS) Schedule
2.6 SECURITY COMMAND CENTER (SCC)
2.6.1 ESS Software
2.6.1.1 Alarm Call up
2.6.1.2 Programming
2.6.1.2.1 Daylight Savings Time Adjustment
2.6.1.2.2 Operator Privileges
2.6.1.2.3 Alarm Priorities
2.6.1.2.4 Reports
2.6.1.2.5 User Interface
2.6.1.2.6 Messages
2.6.1.2.7 Graphics

2.6.1.2.8 Device Status
2.6.1.2.9 Diagnostics
2.6.1.2.10 Mandatory Data Fields
2.6.1.2.11 User Defined Data Fields
2.6.1.2.12 Archive Database
2.6.1.2.13 Programmable Database Backup
2.6.1.2.14 Programmable Database Purging
2.6.1.2.15 Database Importing
2.6.1.2.16 Data Exporting
2.6.1.2.17 Event Log Output
2.6.1.2.18 Data Audit Trail
2.6.1.2.19 Alarm Forwarding
2.6.2 ESS Monitor Display Software
2.6.3 Graphical Interactive Map Software
2.6.4 Printers
2.6.4.1 Report Printer
2.6.4.2 Alarm Printer
2.6.4.3 Badge Printer
2.6.5 Control and Display Integration
2.6.6 Enrollment Center Equipment
2.6.6.1 Enrollment Client Accessories
2.6.6.2 Enrollment Center I.D. Production
2.6.6.3 Enrollment Client Software
2.7 COMMUNICATIONS
2.7.1 Link Supervision
2.7.1.1 Hardwire Direct Current Line Supervision
2.7.1.2 Hardwire Alternating Current Supervision
2.7.1.3 Hardwire Digital Supervision
2.7.2 Hardwire
2.7.2.1 Electrical Conductor Lines
2.7.2.2 Communication Link
2.7.3 Radio Frequency Link
2.7.4 Data Encryption
2.7.5 Network Switch
2.7.5.1 Inside Plant
2.7.5.2 Outside Plant
2.7.6 Video and ESS Transmission
2.7.7 Wire and Cable
2.7.8 Digital Data Interconnection Wiring
2.7.9 Aboveground Sensor Wiring
2.7.10 Direct Burial Sensor Wiring
2.7.11 Local Area Network (LAN) Cabling
2.7.12 Cable Construction
2.8 SECURITY LIGHTING INTERFACE
2.9 MEDICAL FACILITY SYSTEM
2.9.1 Infant Protection Alarm System (IPAS) Performance Requirements
2.9.2 Infant Protection Alarm System (IPAS) Major Components
2.9.3 Infant Protection Operator Workstations
2.9.4 Remote Display Unit
2.9.5 Operator Interface
2.9.6 Alarm Management
2.9.6.1 Tamper Alarm
2.9.6.2 Near Exit Alarm
2.9.6.3 Battery Alarm
2.9.6.4 Failed Communications Alarm
2.9.6.5 Lost Alarm
2.9.7 IPAS Area Wireless Tag Readers
2.9.8 IPAS Door Wireless Reader
2.9.9 Infant Tags and Straps

-- End of Section Table of Contents --

****

USACE / NAVFAC / AFCEC | **UFGS-28 10 05 (May 2024)**

Preparing Activity: USACE | **Superseding**
UFGS-28 10 05 (May 2016)

UNIFIED FACILITIES GUIDE SPECIFICATIONS

References are in agreement with UMRL dated January 2025

****

SECTION 28 10 05

ELECTRONIC SECURITY SYSTEMS (ESS)
05/24

****

NOTE: This guide specification covers the requirements for Electronic Security Systems (ESS) consisting of commercial off-the-shelf equipment which is limited to:

1. Intrusion Detection System (IDS)
2. Access Control System (ACS)
3. Video Surveillance System (VSS)
4. Medical Facility System
5. Security Command Center
6. Security Lighting
7. Infant Protection Alarm System (IPAS)

System requirements must conform to UFC 4-021-02, "Electronic Security Systems". Consult the appropriate governing authority - the US Naval Facilities Engineering Command, the US Army Corps of Engineers, the US Air Force Civil Engineering Support Agency, or the National Aeronautics and Space Administration - for questions concerning system design. Coordinate requirements with the Project Manager, Base/Regional Security Personnel, and the Accrediting Official. ESS is typically provided for the protection of designated assets.

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 item(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).

****

PART 1 GENERAL

****

NOTE: This section will be used in conjunction with Sections: 26 20 00 INTERIOR DISTRIBUTION SYSTEM; 27 10 00 BUILDING TELECOMMUNICATIONS CABLING SYSTEM; 33 71 01 OVERHEAD TRANSMISSION AND DISTRIBUTION; 33 71 02 UNDERGROUND ELECTRICAL DISTRIBUTION; 33 82 00 TELECOMMUNICATIONS OUTSIDE PLANT (OSP); 28 08 10 ELECTRONIC SECURITY SYSTEM ACCEPTANCE TESTING; Section 34 75 13.13 CRASH RATED ACTIVE VEHICLE BARRIERS AND CONTROLS; and any other guide specification sections required by the design.

****

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 Reference Identifier (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)

ASC/X9 X9.52	(1998) Triple Data Encryption Algorithm Modes of Operation

ASTM INTERNATIONAL (ASTM)

ASTM A123/A123M	(2024) Standard Specification for Zinc (Hot-Dip Galvanized) Coatings on Iron and Steel Products
ASTM B32	(2020) Standard Specification for Solder Metal

ASTM D709	(2017) Standard Specification for Laminated Thermosetting Materials
ASTM E84	(2023) Standard Test Method for Surface Burning Characteristics of Building Materials

BUILDERS HARDWARE MANUFACTURERS ASSOCIATION (BHMA)

ANSI/BHMA A156.23	(2010) Electromagnetic Locks

ELECTRONIC COMPONENTS INDUSTRY ASSOCIATION (ECIA)

ECIA EIA/ECA 310-E	(2005) Cabinets, Racks, Panels, and Associated Equipment

INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS (IEEE)

IEEE 802.3	(2022) Ethernet
IEEE C62.41.1	(2002; R 2008) Guide on the Surges Environment in Low-Voltage (1000 V and Less) AC Power Circuits
IEEE C62.41.2	(2002) Recommended Practice on Characterization of Surges in Low-Voltage (1000 V and Less) AC Power Circuits

INTELLIGENCE COMMUNITY STANDARD (ICS)

ICS 705-1	(2010) Physical and Technical Security Standard for Sensitive Compartmented Information Facilities

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION (ISO)

ANSI ISO/IEC 7816	(R 2009) Identification Cards - Integrated Circuit Cards

NATIONAL ELECTRICAL MANUFACTURERS ASSOCIATION (NEMA)

NEMA 250	(2020) Enclosures for Electrical Equipment (1000 Volts Maximum)
NEMA ICS 1	(2022) Standard for Industrial Control and Systems: General Requirements
NEMA ICS 2	(2000; R 2020) Industrial Control and Systems Controllers, Contactors, and Overload Relays Rated 600 V
NEMA ICS 6	(1993; R 2016) Industrial Control and Systems: Enclosures

NATIONAL FIRE PROTECTION ASSOCIATION (NFPA)

NFPA 70	(2023; ERTA 1 2024; TIA 24-1) National Electrical Code

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST)

NIST FIPS 140-2	(2001) Security Requirements for Cryptographic Modules
NIST FIPS 197	(2001) Advance Encryption Standard
NIST FIPS 201-2	(2013) Personal Identity Verification (PIV) of Federal Employees and Contractors
NIST SP 800-116	(2018; Rev 1) Guidelines for the Use of PIV Credentials in Facility Access

OPEN NETWORK VIDEO INTERFACE FORUM (ONVIF)

ONVIF	(2017) Core Specification Version 17.06

TELECOMMUNICATIONS INDUSTRY ASSOCIATION (TIA)

TIA-222	(2018H; Add 1 2019) Structural Standard for Antenna Supporting Structures and Antennas and Small Wind Turbine Support Structures
TIA-568.2	(2024e) Balanced Twisted-Pair Telecommunications Cabling and Components Standards
TIA-606	(2021d) Administration Standard for Telecommunications Infrastructure
TIA-607	(2019d) Generic Telecommunications Bonding and Grounding (Earthing) for Customer Premises

U.S. DEPARTMENT OF DEFENSE (DOD)

MIL-HDBK-419	(1987; Rev A) Grounding, Bonding, and Shielding for Electronic Equipments and Facilities Volumes 1 of 2 Basic Theory
MIL-STD-188-124	(1998; Rev B; Notice 2 1998; Notice 3 2000; Notice 4 2013) Grounding, Bonding and Shielding for Common Long Haul/Tactical Communications Systems, Including Ground Based Communications - Electronics Facilities and Equipments

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

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

UL SOLUTIONS (UL)

UL 50	(2024) UL Standard for Safety Enclosures for Electrical Equipment,

	Non-Environmental Considerations
UL 294	(2023) UL Standard for Safety Access Control System Units
UL 437	(2013; Reprint Jan 2022) UL Standard for Safety Key Locks
UL 634	(2007; Reprint Mar 2015) Connectors and Switches for Use with Burglar-Alarm Systems
UL 636	(2018) UL Standard for Safety Holdup Alarm Units and Systems
UL 639	(2007; Reprint Jun 2024) Standard for Intrusion Detection Units
UL 681	(2014; Reprint Jan 2021) UL Standard for Safety Installation and Classification of Burglar and Holdup Alarm Systems
UL 796	(2020; Reprint Oct 2023) UL Standard for Safety Printed Wiring Boards
UL 969	(2017; Reprint May 2023) UL Standard for Safety Marking and Labeling Systems
UL 972	(2006; Reprint Nov 2020) UL Standard for Safety Burglary Resisting Glazing Material Type
UL 1037	(2016; Reprint Aug 2023) UL Standard for Safety Antitheft Alarms and Devices
UL 1076	(2018; Reprint Feb 2021) UL Standard for Safety Proprietary Burglar Alarm Units and Systems
UL 1610	(2016; Reprint Apr 2021) UL Standard for Safety Central-Station Burglar-Alarm Units
UL 2050	(2003; 4th Edition) Standard for National Industrial Security Systems for the Protection of Classified Materials (limited distribution publication, direct purchase request with justification to UL)
UL 2802	(2013; Reprint Apr 7 2020) UL Standard for Safety Performance Testing of Camera Image Quality
UL 62368-1	(2019) UL Standard for Audio/Video, Information, and Communication Technology Equipment - Part 1: Safety Requirements

1.2 SUBMITTALS

****
NOTE: Review submittal description (SD) definitions

in Section 01 33 00 SUBMITTAL PROCEDURES and edit the following list, and corresponding submittal items in the text, to reflect only the submittals required for the project. The Guide Specification technical editors have classified 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 Army projects, fill in the empty brackets following the "G" classification, with a code of up to three characters 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 and Air Force projects.

The "S" classification indicates submittals required as proof of compliance for sustainability Guiding Principles Validation or Third Party Certification and as described in Section 01 33 00 SUBMITTAL PROCEDURES.

****

Government approval is required for submittals with a "G" or "S" classification. Submittals not having a "G" or "S" classification are for Contractor Quality Control approval. Submittals not having a "G" or "S" classification are for information only. When used, a code following the "G" classification identifies the office that will review the submittal for the Government. 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.

] SD-02 Shop Drawings

ESS Components; G, [_____]

Access Control System (ACS); G, [_____]

Security Hardware Door Schedule; G, [_____]

Overall System Schematic; G, [_____]

Video Surveillance System (VSS) Schedule; G, [_____]

SD-03 Product Data

****

NOTE: The product data list is not all inclusive.

****

Premise Control Unit; G, [_____]

Detection Sensors; G, [_____]

Access Control Unit; G, [_____]

Access Control Devices; G, [_____]

Cameras; G, [_____]

Camera Lenses; G, [_____]

Camera Housing and Mounts; G, [_____]

Thermal Imaging System; G, [_____]

Video Recording; G, [_____]

Printers; G, [_____]

Communications Interface Devices; G, [_____]

Radio Frequency Link; G, [_____]

Network Switch; G, [_____]

Video and ESS Transmission; G, [_____]

Infant Protection Alarm System (IPAS) Major Components; G, [_____]

Uninterruptible Power Supply (UPS); G, [_____]

Batteries; G, [_____]

Component Enclosure; G, [_____]

Equipment Rack; G, [_____]

SD-05 Design Data

Backup Battery Capacity Calculations; G, [_____]

Video Surveillance System (VSS) Storage Calculations; G, [_____]

Error and Throughput Rates; G, [_____]

SD-07 Certificates

Contractor Qualifications; G, [_____]

Instructor Qualifications; G, [_____]

Contact Card Readers; G, [_____]

Contactless Card Readers; G, [_____]

Data Encryption; G, [_____]

Wire And Cable; G, [_____]

Bonding, Grounding, And Shielding; G, [_____]

SD-10 Operation and Maintenance Data

ESS Components; G, [_____]

ESS Software, Data Package 4; G, [_____]

ESS Training; G, [_____]

ESS Training Outline; G, [_____]

Submit data package in accordance with Section 01 78 23 OPERATION AND MAINTENANCE DATA

SD-11 Closeout Submittals

As-Built Drawings; G, [_____]

Warranty; G, [_____]

1.3 QUALITY ASSURANCE

1.3.1 Regulatory Requirements

The advisory provisions in each of the publications referred to in this specification are mandatory. Interpret these publications as though the word "must" has 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 must be in accordance with the mandatory and advisory provisions of NFPA 70 unless more stringent requirements are specified or indicated.

1.3.2 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 and:

a. Have been in satisfactory commercial or industrial use for 2 years prior to bid opening and have been utilized in applications of equipment and materials under similar circumstances and of similar size.

b. Have been available on the commercial market through advertisements, manufacturers' catalogs, or brochures during the 2-year period.

c. Where two or more items of the same class of equipment are required, provide products of a single manufacturer.

d. Provide commercial off-the-shelf (COTS) products in which the manufacturer allows a network of qualified distributors to sell, install, integrate, maintain, and repair the hardware and software

products that make up the system. All products are to be NDAA and FAR subpart 4.21 compliant.

1.3.2.1 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.

1.3.2.2 Material and Equipment Manufacturing Date

Products manufactured more than one year prior to date of delivery to the site are not acceptable.

1.3.2.3 Product Safety

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

1.3.3 Shop Drawings

1.3.3.1 ESS Components

Submit the ESS Components, Data Package 4 with the ESS Software submittal package in accordance with Section 01 78 23 OPERATION AND MAINTENANCE DATA. Submit drawings that clearly and completely indicate each ESS component function that includes:

a. Termination device points

b. Interconnections required for system operation

c. Interconnections between modules and devices

d. Component and device wiring diagrams.

e. Proposed wireway or conduit systems to be used including:

(1) Locations

(2) Sizes

(3) Types

f. Drawings showing:

(1) Device locations and spacing

(2) Mounting and positioning details

(3) Riser Diagrams with cable sizes and types

(4) Bill of Materials (Device make, model and quantities)

(5) Alarm and access control zones

(6) Video Surveillance System (VSS) and sensor coverage areas

(7) Spare capacity

(8) Tables with (Security Hardware Door Schedule) identifying security devices requirements per building, room, and door

(9) Overall system schematic diagram(s).

1.3.4 Evidence of Experience and Qualifications

1.3.4.1 Contractor Qualifications

Contractor or its subcontractor(s) must be a Value Added Resaler (VAR)/Authorized Dealer (AD) of the manufacturer line of products being installed. Provide manufacturer certificate showing current dealership status. Technicians working the project must provide certificates of training for the requirements of the manufacturer, and those certificates must be from the manufacturer or approved by the manufacturer.

Submit experience and certified qualifications data prior to installation. Show that specific installers who will perform the work have a minimum of [2] [_____] years of experience successfully installing ESS of the same type and similar design as specified. Include the names, locations, and points of contact of at least two installations of similar type and design as specified in this document where the installer has installed such systems. Indicate the type of each system installed. Certify that each system has performed satisfactorily in the manner intended for a period of at least [12] [_____] months.[Installation and maintenances of IDS for the protection of classified information to be performed by US citizens who have been subject to a trustworthiness determination.]

1.3.4.2 Instructor Qualifications

Submit the instructor's experience and certified qualifications data prior to installation. Show that the instructor has received a minimum of 24 hours of ESS training from the manufacturer of the product being installed, and 2 years experience in installing the specified ESS type.

1.4 ENVIRONMENTAL CONDITIONS

1.4.1 Interior Conditions

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

1.4.1.1 Temperature

0 to 50 degrees C.32 to 120 degrees F. Components installed in unheated security protected areas must meet performance requirements for temperatures as low as minus 17 degrees C 0 degrees F

1.4.1.2 Pressure

Sea level to 4573 m 15,000 feet above sea level

1.4.1.3 Relative Humidity

5 to 95 percent

1.4.1.4 Fungus

Components must be constructed of non-fungus nutrient materials or be treated to inhibit fungus growth

1.4.1.5 Acoustical Noise

Components must be suitable for use in high noise areas above 100 dB, without adversely affecting their performance

1.4.2 Exterior Conditions

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

1.4.2.1 Temperature

[Minus 32 to 60] [_____] degrees C [Minus 25 to 140] [_____] degrees F

1.4.2.2 Pressure

Sea level to [4573] [_____] m [15,000] [_____] feet above sea level

1.4.2.3 Solar Radiation

Six [_____] hours of solar radiation per day at dry bulb temperature of 60 [ ] degrees C 120 [_____] degrees F including 4 hours of solar radiation at 0.00112 [ ] watts per square mm 104 [_____] watts per square foot

[1.4.2.4 Sand and Dust

Wind driven for up to [9.6] [_____] km per hour (kmph) [6] [_____] miles per hour (mph) in accordance with UL 294 and UL 639.

]1.4.2.5 Rain

50 mm 2 inches per hour and 125 mm 5 inches per hour cyclic with wind plus one period of 300 mm 12 inches per hour in accordance with UL 294 and UL 639.

1.4.2.6 Humidity

5 to 95 percent

[1.4.2.7 Fungus

Warm, humid atmosphere conducive to the growth of heterotrophic plants

][1.4.2.8 Salt Fog

Salt atmosphere with [5] [_____] percent salinity

][1.4.2.9 Snow

Snow loading of 234 kg per square m 48 (psf) per hour; blowing snow of 22.5 kg per square m 4.6 psf per hour. Blowing snow from any angle (falling vertically to horizontal blowing from any azimuth) must not penetrate ESS equipment.

][1.4.2.10 Ice Accretion

Up to 12.7 mm 1/2 inches of radial ice

]1.4.2.11 Wind

Continual velocity up to 80 kmph 50 mph with gusts to 106 kmph 66 mph, except that fence sensors must detect intrusions up to 56 kmph 35 mph

1.4.2.12 Acoustical Noise

Visual alert device and components should be used in high noise areas above 110 dB without adversely affecting their performance. Examples areas include flight lines, run-up pads, and generator sites.

1.5 SYSTEM CALCULATIONS AND ANALYSIS

1.5.1 Backup Battery Capacity Calculations

Submit calculations showing that backup battery capacity exceeds sensor operation, communications supervision, and alarm annunciation power requirements for proposed equipment plus 25 percent spare capacity. In environments regularly exposed to conditions of 0 degrees C 32 degrees F provide 50 percent spare capacity. In environments regularly exposed to conditions of 49 degrees C 120 degrees F provide resistance to thermal runaway for lithium based batteries.

1.5.2 Video Surveillance System (VSS) Storage Calculations

Submit calculations showing the required storage capacity for each video storage device. Calculations must be based on the recording parameters specified by the end user/customers operational requirements.

1.6 ESS SOFTWARE, DATA PACKAGE 4

Submit the ESS software, Data Package 4 with the ESS Components submittal package in accordance with Section 01 78 23 OPERATION AND MAINTENANCE DATA. Describe the functions of all software in the software manual and include:

a. All information necessary to enable proper loading, testing, and operation

b. Terms and functions definitions

c. Use of system and application software

d. Procedures for system initialization, start-up and shutdown

e. Alarm reports

f. Reports generation

g. Database format and data entry requirements

h. Directory of all files

i. All communication protocol descriptions, including data formats, command characters, and a sample of each type of data transfer

j. Interface definition

k. List of software keys

l. Backup and restore procedures and instructions on how to archive reports and video footage on DVD for forensics investigations.

1.7 AS-BUILT DRAWINGS

****
NOTE: Designer must verify CAD version with Contracting Officer and clearly state the requirement.
****

Maintain a separate set of drawings, elementary diagrams, and wiring diagrams of the system to be used for as-built drawings. Keep this set accurately and neatly up to date with all changes and additions. This set is not to be used for installation purposes.

Finish the final drawings submitted with the endurance test report in accordance with Section 01 78 00 CLOSEOUT SUBMITTALS for as-built requirements.

PART 2 PRODUCTS

2.1 SYSTEM DESCRIPTION

****
NOTE: Use the following for ESS guidance as applicable:

For SCIF and SAPF fill in the first bracketed option with: Intelligence Community Standards (ICD/ICS) 705 Physical and Technical Security Standards for Sensitive Compartmented Information Facilities. (NOTE: Do not identify "SCIF" or SAPF in Request for Proposal (RFP) or construction drawings. With accrediting official's approval, areas may be identified as "secure area" or "controlled area.")

For Secret, Top Secret or Controlled Access Areas (CAA), fill in the first bracketed option with the appropriate Service instruction: SECNAV M-5510.36A Department of Navy Information Security Program; Army Regulation AR 380-5 Department of the Army Information Security Program; or Air Force Instruction AFI 31-401 Department of the Air Force Information Security Program.

For Arms, ammunition or explosives (arms rooms,

armories, and magazines), fill in the first bracketed option with the appropriate Service instruction: OPNAV Instruction 5530-13C Department of the Navy Physical Security Instruction for Conventional Arms, Ammunition, and Explosives; MCO 5530.14A Marine Corps Physical Security Program Manual; AR 190-11 Department of the Army Physical Security of Arms, Ammunition and Explosives; or AFMAN 91-201 Department of the Air Force Explosive Safety Standards

For Air Force non-nuclear assets, ensure system utilizes the Air Force Non-Nuclear IDS Approved Equipment List. Contact AFSFC/S5G at afsfc.ibdss@us.af.mil for a copy of the letter or with any questions concerning these items.

For Army projects, contact the Electronic Security System Mandatory Center of Expertise (ESS MCX) for assistance in specifying requirements for IDS zones that will connect to an existing Integrated Commercial Intrusion Detection System (ICIDS). ESS MCX e-mail address is AskESSMCX@usace.army.mil

****

Provide a complete and integrated electronic security system (ESS) that meets the requirements of [_____]. ESS must be compatible with the Installation's central monitoring system and monitored [within the secure/protected area] [_____] [and] [at the Installation central monitoring station]. [[Installation's][_____] central monitoring system is manufactured by [_____], model number [_____].] ESS consisting of the following subsystems and features:

a. Intrusion Detection System (IDS)

b. Access Control System (ACS)

c. Video Surveillance System (VSS)

d. Security Command Center (SCC)

e. Communications System

f. Security Lighting Systems

[g. Medical Facility Systems

] Include materials not normally furnished by the manufacturer with the ESS equipment as specified in:

[a. Section 33 71 02 UNDERGROUND ELECTRICAL DISTRIBUTION

]b. Section 33 71 01 OVERHEAD TRANSMISSION AND DISTRIBUTION

][c. Section 26 20 00 INTERIOR DISTRIBUTION SYSTEM

]2.2 PERFORMANCE REQUIREMENTS

Integrate the installed and operating subsystems into the overall ESS

system to detect intrusion, control access, video surveillance, visual verification, and perform as an entity, as specified below. Provide electronic equipment that complies with 47 CFR 15 and are suitable for the environment where they will be installed.

2.2.1 Growth Capability

Provide capability for modular ESS expansion of inputs, outputs, card readers, and remote-control stations with minimal equipment modification. Software must be able to handle design requirements plus 25 [_____] percent spare capacity. Growth capability is not to be limited by the provided products.

2.2.2 Hazardous Locations

****

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.

****

When located in areas where fire or explosion hazards exist, provide system components rated and installed according to Chapter 5 of NFPA 70.

2.2.3 Maintainability

Provide components that can be maintained using commercially available tools and equipment. Arrange and assemble components to be readily accessible to maintenance personnel without compromising system defeat resistance and with no degradation in tamper protection, structural integrity, EMI or RFI attenuation, or line supervision after maintenance when it is performed in accordance with manufacturer's instructions.

2.2.4 Availability

Provide components rated for continuous operation. Provide solid-state electronic components mounted on printed circuit boards, conforming to UL 796. Provide boards that are plug-in, quick-disconnect type. Do not impede maintenance with densely packed circuitry. Provide power-dissipating components with safety margins of not less than 25 percent with respect to dissipation ratings, maximum voltages, and current-carrying capacity. Provide heat sinks or other heat dissipation devices on appropriate components and assemblies. Provide solid-state type or hermetically sealed electromechanical type light duty relays and similar switching devices.

2.2.5 Fail-Safe Capability

Provide fail-safe capability in critical elements of the ESS including, but not be limited to, the capability to monitor communication link integrity and to provide self-test. Provide fault annunciation when diminished functional capabilities are detected. Annunciate fail-safe alarms to clearly distinguish from other types of alarms.

2.2.6 Line Supervision

Provide the same geographic resolution for fault isolation at the systems level as provided for intrusion detection. Provide either a static or dynamic system with active mode for line supervision of communication links of the ESS.

a. The static system must represent "no-alarm" always by the same signal, which is different than the originally transmitted signal.

b. The dynamic system must represent "no-alarm" with a signal which continually changes with time.

2.2.7 Power Loss Detection

****
NOTE: Verify if the Uninterruptible Power Supply (UPS) is detecting the loss of power to the critical component.
****

Detect AC and DC power loss and generate an alarm when a critical component of the system experiences temporary or permanent loss of power. Annunciate the alarm in [the Secured Area] [_____] [and] [the Security Command Center] to clearly identify the component experiencing power loss.

2.2.8 Controls and Designations

Provide controls and designations in accordance with NEMA ICS 1.

2.2.9 Special Test Equipment

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

2.2.10 Electromagnetic Interference (EMI)

Configure and provide ESS components employing electromagnetic radiation constructed to provide minimal vulnerability to electronic countermeasures.

2.2.11 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.

2.2.12 Interchangeability

Use off-the-shelf components which are physically, electrically, and functionally interchangeable with equivalent components as complete

items. Equivalent, replacement components must not require new or other component modification. Do not use custom designed or one-of-a-kind items. Interchangeable components or modules must not require trial and error matching in order to meet integrated system requirements, system accuracy, or restore complete system functionality.

2.2.13 Date and Time Generator

****
NOTE: Provide a time server for larger systems.
****

The ESS system date and time are to originate from [the ESS network time server] [GPS synchronization system with GPS satellite antenna][_____].

2.3 INTRUSION DETECTION SYSTEM (IDS)

The IDS primary function is to detect intrusion into secured areas. Utilize a single database for all IDS programming data that seamlessly integrates with the ESS under a single operating environment. The IDS events must be viewable as separate or as a combined list of all ESS events. Control the IDS alarm monitoring through software control from the ESS.

a. Provide both supervised and non-supervised alarm point monitoring.

b. [Arm or disarm] [Secure or access] alarm points both manually and automatically by time of day, day of week or by operator command.

[c. For classified assets, IDS installation related components and monitoring stations must comply with UL 2050.

]2.3.1 IDS Components

Provide components:

a. Premise Control Units (PCU)

b. Detection Sensors

c. Tamper Switches

d. Arm/Disarm Keypads

2.3.2 Detection Sensitivity

The sensitivity of the IDS must allow for the following:

a. Locating intrusions [within [100] [_____] meters 300 [_____] feet 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 the coverage on a single volumetric sensor

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 designer should select arming/disarming for Army projects and select secure/access for Air Force and Navy projects.
****

Collect, communicate, and display up to [12] [32] [64] [128] [256] [_____] sensor zone alarms [and to enable control of [one] [two] [_____] [card reader] [card reader with integral keypad] for [arming and disarming] [secure and access] [inside of the protected area with a delayed alarm] [outside of the protected area with instant alarm]].

Identify individual sensors in alarm if the sensor zone is a multiple alarm source combination. Annunciate a single alarm within [1] [2] [_____] seconds maximum, after sensor transducer or other detection device activation [except that alarms transmitted by radio frequency signaling must communicate in less than 3 seconds].

2.3.4 False Alarm Rate

The false alarm rate for each interior IDS zone must not exceed one false alarm per 30-day period. The false alarm rate for each exterior IDS zone must not exceed one false alarm per 24-hour period.

2.3.5 Nuisance Alarm Rate

The nuisance alarm rate for each interior IDS zone must not exceed three nuisance alarms per 30-day period. The nuisance alarm rate for each exterior IDS zone must not exceed three nuisance alarms per 24-hour period.

2.3.6 Premise Control Unit (PCU)

Install the PCU command processor in a tamper resistant enclosure that is specified in paragraph COMPONENT ENCLOSURE. Package the following with the PCU:

a. Power transformer

b. Battery(s)

c. Network connection cable

d. Keypad(s)

e. Keypad connection cable(s)

f. Additional components as required for full functionality

2.3.6.1 PCU Capabilities

Provide the PCU 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. Support [4] [8] [16] [_____] keypads with alphanumeric display. Each keypad must be capable of [arming and disarming] [securing and accessing] any system area based on a pass code or access control card and or key FOB authorization. Provide keypad alphanumeric display with 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.

****
NOTE: For installation where dial-up is the only feasible line, two lines of communication are to be used.
****

f. Data line supervision [or two separate lines of communication].

g. 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. Provide a minimum of a [4,000] [_____] event log buffer per PCU. Record and hold alarm activity information in the log buffer until the ESS is connected and receives the information. Provide a software-configurable warning log buffer filling notification for PCU(s) configured with network switch 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).

2.3.6.2 Overcurrent Protection and Indication

When overcurrent more than it is rated for is detected by the PCU, communication bus(es) and keypad(s) are to be shut down and an overcurrent notification LED lit to indicate the situation.

2.3.6.3 Manual and Self-Test

All alphanumeric keypad to include testing for: standby battery, alarm bell or siren, and communication to the Security Command Center (SCC). Include provisions for an automatic, daily, weekly, 30 day, or up to 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.

Include the following for internal monitoring points:

a. The bell circuit

b. AC power

c. Battery voltage level

d. Charging voltage

e. Panel box tamper

f. Phone trouble line 1

g. Phone trouble line 2

h. Transmit trouble

i. Network trouble

A battery test must be automatically performed to test the integrity of the standby battery by disconnecting the standby battery from the charging circuit and placing a load on the battery. Perform this test at an interval no greater than 180 days.

2.3.7 Detection Sensors

****

NOTE: Certain assets may require a higher probability of detection (Pd) than the 0.9 value provided below. Consult the applicable security policy for the asset being protected to determine the actual Pd value required. Remote test capability should be used only when required by governing regulations or when sensors are installed in hard to reach areas.

****

a. Sensors are to detect facility perimeter or protected zone penetrations by unauthorized personnel or intruders and transmit an alarm signal to the alarm annunciation system upon change detection. Accomplish this with a probability of detection (PD) of [[0.9], [0.95]] with a [[90], [95]] percent confidence level and conforming to UL 639 where applicable.

Probability of Detection	0.9	0.9	0.95	0.95	Number of Misses Allowed
Confidence Level	90 Percent	95 Percent	90 Percent	95 Percent	
Number of Intrusion Attempts	22	29	45	59	0
	38	46	77	93	1
	52	61	105	124	2
	65	76	132	153	3
	78	89	158	181	4
	91	103	184	208	5

b. Required sensor power is 12 VDC unless otherwise specified.

c. An interior IDS zone is a room or space within a building that can be [armed and disarmed] [secured and accessed] independently from all other zones.

d. Provide line supervision for all sensors with an end-of-line resistor at the sensor or within a tampered junction box with conduit from the junction box to the sensor.

e. Provide sensors and components rated for operation in the installed environment. The sensors must transmit an alarm signal to the alarm annunciation system upon change detection. Provide all sensors with a tamper switch and elements housed in a tamper-alarmed enclosure in accordance of paragraph COMPONENT ENCLOSURE.

2.3.7.1 Interior Sensors

2.3.7.1.1 High Security Switch (HSS)

****

NOTE: High security switch (HSS) as specified in (a) are for High security applications, refer to ICS 705-1. Use of recessed HSS is recommended during new installations. Coordinate with Architect to ensure proper door hardware (electric strike, hinges, etc.) is provided.

Use level 2 high security HSS in SCIF and SAPF areas. Use level 1 or level 2 in all other locations. The level required is dependent on the asset and risk level.

****

Mount the HSS inside the secure location and on the opening side of the door. HSS sensors do not have the capability to incorporate an end-of-line (EOL) resistor.

2.3.7.1.1.1 Level 1 Switch

UL 634. Level 1 High Security

2.3.7.1.1.2 Level 2 Switch

UL 634. Level 2 High Security

2.3.7.1.2 Glass Break Detection

UL 639.

2.3.7.1.2.1 Window-Mounted Glass Break Shock Sensor

Provide sensors with an LED for adjusting sensitivity.

Provide sensor with an exterior label to protect tape from direct sunlight. Seismic vibrations or other ambient stimuli are not to initiate an alarm. [Test glass breakage sensors by using test units supplied by the manufacturer which simulate glass breakage.]

2.3.7.1.2.2 Ceiling Or Wall-Mounted Dual Technology Glass Break Sensor

Provide a sensor that eliminates occupant-generated false alarms by combining a passive infrared motion detector (PIR) with glass break sensing. The combination will extend coverage to occupied areas, allowing the sensors to be armed while people are present.

2.3.7.1.2.3 Ceiling or Wall-Mounted Recessed Glass Break Sensor

Provide a sensor employing pattern recognition technology that listens for the actual pattern of breaking glass. The sensor is to be able to detect the difference from breaking glass and normal room sounds by listening across the glass break frequency spectrum. Provide a range of 7.6 meters 25 feet to cover the area to be protected.

2.3.7.1.3 Vibration Vault Sensor

Provide a sensor that senses short duration, large amplitude signals like those produced in attacks from explosions, hammering or chiseling and also detect long duration, small amplitude signals like those produced in attacks from torches, thermic lances, drills, grinders, or cutting discs.

Provide sensor equipped with a manual and an automatic test alarm output with test indicator not visible or audible during normal operations. The test indicator is to annunciate when the sensor detects an intruder when active. The alarm indication may be located within the sensor or as a separate device.

2.3.7.1.4 Fiber Optic Mesh Sensors

Fiber optic mesh sensors are to be comprised of a web of optical fiber cables which are deployed within:

a. Building walls

b. Partitions

c. Flexible structures

d. Water-side installations

e. Mobile facilities

f. Mobile container shells

2.3.7.1.5 Utility Inlet Opening Protection

****
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.
****

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 is larger than 100 mm 4 inches on center.

[Conceal] [Tamper protect] terminated sensors so that any attempts to cut the wire or enlarge openings between wires cause an alarm.

2.3.7.1.6 Passive Infrared Sensors

UL 639.

2.3.7.1.7 Microwave Sensors

UL 639.

2.3.7.1.8 Dual Technology Sensors

****
NOTE: In subparagraph, writer should specify whether the dual technology detection would require both phenomenological (i.e., "AND" mode) or a single phenomenology (i.e., "OR" mode) for reporting of an alarm. If dual technology sensors are placed in SCIF, SAPF, or classified open storage, then the sensor must be configured in the "OR" mode.
****

UL 639. Provide sensor combining passive infrared (PIR) and microwave sensors configured and manufactured specifically to be mounted in a single tamper alarmed enclosure. The sensor must provide ["AND" logic for alarm indication] [selectable "AND" logic or "OR" logic for alarm indication configured in the "OR" logic state]. Provide sensors that have a local means of indicating detection for use during installation and calibration

with a means of disabling the indication.

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

2.3.7.1.9 Photoelectric Sensors

UL 639. The sensor is to detect opaque bodies and not allow an intruder to disable detection by shining another light source into the receiver.

Provide sensor with a local means of indicating detection for use during installation and calibration with a means of disabling the indication.

2.3.7.2 Exterior Sensors

2.3.7.2.1 Wide Gap High Security Switch (HSS)

Provide UL 634 approved wide gap HSS for all exterior applications (gates, etc.) that cannot operate within the close tolerances of standard HSS sensors. Ensure the application tolerances are within the HSS limitations set by the manufacturer for optimum operation. Wide gap HSS should have a minimum gap tolerance of [_____] mm [_____] inches and a maximum gap tolerance of [_____] mm [_____] inches between switch and magnet.

2.3.7.2.2 Fence Mounted Sensors

Sensors are fiber optic or strain-sensitive cable sensors as indicated which initiate an alarm when an intruder attempts to scale, cut through, lift the fabric of, or lean climbing devices on to the entire length of a standard chain link fence or physical barrier. Provide sensors that are either tamper alarmed or self-protecting. House exterior components in rugged, corrosion-resistant enclosures, as specified in paragraph COMPONENT ENCLOSURE.

Provide fence cable support hardware that is weather-resistant.

2.3.7.2.2.1 Fiber Optic Sensor

The sensor consists of an ultraviolet resistant fiber optic transducer cable with a microprocessor based dual zone signal processor that is capable of monitoring different styles of metal fabric fencing including chain-link, expanded-metal or welded-mesh fence. The sensor detects intruders by utilizing signals generated by the minute flexing of the fiber optic transducer cable, caused by attempting to cut, climb, or raise the fence fabric.

The signal processor analyzes the signals from the fiber optic transducer cable and detects minute vibrations in the fabric of the fence. The signal processor supports [single] [dual] zones with each zone supporting a maximum 500 m 1640 feet of sensing cable. The processor utilizes adaptive algorithms, ambient signal compensation and selectable common-mode rejection, to discriminate between actual, false and nuisance alarms, without lowering the probability of detection. The processor identifies, by type, a cut intrusion and a climb intrusion. Provide

sensors with independent adjustments and thresholds for each type of intrusion and have the capability to completely mask climb or cut alarms. Alarms caused by power failure, low input voltage, cable fault (cable cut or high loss due to physical stress), or internal electronic fault are to be identified as supervisory alarms. Equip the sensor with a test indicator if it is an integral sensor signal processor function.

2.3.7.2.2.2 Strain-Sensitive

a. Provide a complete fence line protection with no dead zones where an intruder can penetrate the fence. Through sensor electronics the fence line protection must be divided into zones. Sensing unit of sensor must achieve specified performance with transducer cable either by attachment directly to the fence fabric by plastic cable every 300 to 455 mm 12 to 18 inches or by installation inside RGS conduit mounted on the fence. Provide sensing units with equal adjustable sensitivity throughout the entire length.

b. Use only conventional waterproof coaxial cable connectors for connections of the sensing unit to permit installation in extreme EMI environments with no loss of detection capability. Entire sensor system must be capable of detecting tampering within each system portion by sensor zone.

c. Provide capability for alarm threshold sensitivity adjustment to permit compensation by zone for winds up to [40] [56] [_____] kmph [25] [35] [_____] mph while maintaining the same level of detection performance as under ambient conditions.

d. Sensor zone control unit must 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 is to 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.

2.3.7.2.2.3 Gate Units

Provide gate units in accordance with specific fence sensor manufacturer's recommendations to ensure continuous fence sensor zone protection for the entire protected perimeter. Provide a gate unit for each fence portal.

Provide separately zoned HSS gate sensors when gate units are not provided by the fence sensor manufacturer. HSS sensors perform as specified in paragraph WIDE GAP BALANCED MAGNETIC SWITCH.

2.3.7.2.3 Electrostatic Field Sensors

a. Initiate an alarm when an intruder attempts to approach or scale a fence or physical barrier. Electrostatic field sensors generate an electric field around one or more horizontal wires and sense the induced signal in parallel sensing wires to detect human presence. Provide sensors that monitor the induced signal for changes that result from the presence of a conductive body or a body with a high dielectric constant.

b. Use mounting and support hardware as provided by the equipment manufacturer.

c. Provide spring tension-mounted wire on end-of-line terminators to detect cutting, shorting, or breaking of the wires. Select sensor configuration such that an intruder cannot crawl under the bottom wire, through the wires, or over the top wire without being detected and be divided into sensor zones.

d. Sensors must be capable of following irregular contours and barrier bends without degrading sensitivity below the specified detection level. Adjacent zones must provide continuous coverage to avoid a dead zone and be configured to prevent crosstalk interference.

e. Provide filtering on signal processing circuitry to distinguish nuisance alarms. Sensor configuration is to incorporate balanced, opposed field construction to eliminate far field noise.

f. House exterior components in rugged corrosion-resistant enclosures, protected from environmental degradation and provided with tamper switches. Use underground cables to interface between exterior units. Use stainless steel or galvanized exterior support hardware. Use stainless steel sensor and field wires.

g. Follow manufacturer's specifications for wire spacing of various configurations.

h. Provide adjustable sensor sensitivity which is inaccessible to operating personnel.

2.3.7.2.4 Taut-Wire Sensors

a. Incorporate perimeter intrusion detection sensors into a [barbed] [barbless] wire security fence. Detect intrusion of cutting of any single wire or the deflecting, as by climbing, of any wire by more than 80 mm 3.1 inches. A sensor zone includes one or more [61] [_____] m [200] [_____] feet maximum sections of [2100] [_____] mm [7] [_____] foot high parallel fence with each sector consisting of [13] [_____] horizontal tensioned wires attached to the taut-wire fence posts, and three strands as outriggers, plus an "anti-ladder" trip wire supported by rods extending from the outriggers for a total vertical height of approximately [2440] [_____] mm [8] [_____] feet.

b. Mount displacement switches for each horizontal wire within a prewired channel fastened to the fence post at the midpoint of each section. Outrigger barbed wire and tripwire may share the same switch. Mount each taut-wire fence post 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.

c. Mount freestanding taut-wire fence posts in concrete to support the taut-wire fence system. Pretension and clamp each [barbed] [barbless] wire strand 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] [barbless] wires are balanced equal in opposite directions. Pretension tripwires in a like manner. Line tripwires to the top switch in the sensor switch channel by a special subassembly that includes a rod which transfers tripwire movement as a lever to the end of the actuating sensor switch's lever arm.

d. Initiate an alarm upon abnormal switch lever displacement. This would

result from cutting or deflecting its attached wire, as by climbing on or through fence strands. Provide sensor with a damping mechanism which reduces alarm threshold due to slowly changing phenomena including ground shifting, daily and seasonal temperature variations, and winds up to 56 kmph 35 mph.

e. Sensor switch must provide electrical contact closure as the means for initiating an alarm, 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.

f. Housing for switch assembly must be covered by a neoprene cap to retain the center bolt (lever arm). This bolt translates attached horizontal wire movement into the contact closure. The bolt functions as the fulcrum for the lever when the neoprene cap is firmly seated on the cup-shaped polycarbonate housing.

g. Provide threaded upper exposed end of the lever to accommodate clamping to the horizontal wire. The lower end of the lever, which is fashioned to serve as the movable electrical contact, must be held suspended in a small cup-shaped contact that floats in a plastic putty material. The plastic putty is to 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 including 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.

h. Provide metal slider strips having slots through which the barbed wires pass with rivets that prevent the wires from leaving the slots. The slider strip must translate horizontal displacement forces normal to the barbed wire to the sensor. Install one slider strip pair, upper and lower, on every fence post except where sensor posts or anchor strips are installed. Provide maximum separation between slider elements along the fence of [3000] [_____] mm [10] [_____] feet.

i. Attach [barbed] [barbless] wires to installed fence anchor posts, located equidistant on both sides of sensor posts and at ends of sensor zone run. Install fastening plates on an anchor strip. Weld strip or otherwise attach the strip to anchor post and ends of tensed barbed wires wrapped around the fastening plates. Fastening plates are to break off when climbed upon or on the attached [barbed] [barbless] wires creating an alarm and making it impossible to defeat the system by climbing at the anchor post.

j. Use [barbed] [barbless] wire suitable for installation under a preload of approximately 392 N 88 pounds tension and be flexible enough for convenient manipulation during tensioning. The minimum acceptable double-strand barbed wire gage is 15-1/2.

k. Sensor zone control unit must monitor up to [10] [_____] zones.

l. Provide sensor with relay outputs to interface alarm outputs with the overall ESS. Input power is [120] [230] VAC.

2.3.7.2.5 Dual Technology Sensors

a. Provide dual technology sensor that combines Microwave and Dual PIR into one single all-weather detector. Use the sensor in extreme outdoor conditions to provide the maximum amount of coverage in a horizontal plane.

b. The sensor must come mounted in an industrial-grade housing as specified in paragraph COMPONENT ENCLOSURE. Provide pan-tilt swivel bracket with swivel within 100 degrees of range and tilt within 10 degrees. The swivel bracket is to allow for calibration into 1-degree segments for adjustment to any environment.

c. The sensor must provide either wide angle or long-range detection by change of optical mirrors. Wide angle coverage must detect intrusion out to 15 [_____] m [49] [_____] feet and long-range coverage out to [40] [_____] m [130] [_____] feet. Provide sensors that allow adjustment masks for wildlife immunity for animals up to [10] [20] [30] [45] [_____] kg [22] [44] [66] [99] [_____] pounds.

2.3.7.2.6 Bistatic Microwave Sensor

****

NOTE: Within the U.S., the FCC regulates the operating frequencies of all microwave sensors. Other countries have their own frequencies. The designer must request approval from U.S Government agency or country agency having authority for approval of the frequency of the product selected in the design.

****

a. Provide sensor equipped with circuitry that produces an alarm signal when the sensor's receiver is captured by another microwave transmitter. Multiple sensors must be able to operate in adjacent zones without interfering with each other. Provide sensors with adjustable sensitivity controls within the sensor that are not accessible when the sensor housing is in place. Provide sensors that can be adjusted in order to obtain the designed coverage pattern.

b. The bistatic microwave sensor is to consist of a separate transmitter and receiver. The sensor detects changes from a standard intruder's movement in the received microwave signal sensor's detection pattern. The sensor transmits an alarm signal to the alarm annunciation system upon detecting such changes. The sensor must detect a standard intruder moving perpendicular through the sensor's detection pattern at a speed of 0.06 to 7.6 m per second 0.2 to 25 fps.

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

2.3.7.2.7 Monostatic Microwave Sensor

a. Multiple sensors must be able to operate in adjacent zones without

interfering with each other. Provide sensors with adjustable sensitivity controls within the sensor that are not accessible when the sensor housing is in place. The sensor must be adjustable to obtain the coverage pattern shown and have range cut off capabilities of field selected distance 30 to 122 m 100 to 400 feet.

b. The monostatic microwave sensor must consist of an integrated transceiver. The sensor detects changes from a standard intruder in the received microwave signal sensor's detection pattern. The sensor must transmit an alarm signal to the alarm annunciation system upon detecting such changes. The sensor must detect a standard intruder moving perpendicular through the sensor's detection pattern at a speed of 0.06 to 7.6 m per second 0.2 to 25 fps.

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

2.3.7.2.8 Passive Infrared Sensor (Exterior)

a. UL 639. The passive infrared sensor must detect movement from a standard intruder in the ambient level of infrared emissions within the sensors' field of view.

b. The sensor is to detect a change in temperature of at least 1.1 degrees C 2 degrees F and detect an intruder traveling within the sensor's detection pattern at a speed of 0.2 to 15 m per second 0.6 to 50 fps across 2 adjacent segments of the field of view. The sensor must have a detection range of at least 92 m 300 feet. Emissions monitored by the sensor must be in the 8 to 14 micron range.

c. Provide sensors that can be adjusted to obtain the designed coverage pattern. The sensor is to be equipped with a temperature compensation circuit.

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

2.3.7.2.9 Buried Ported Cable

The buried ported cable to monitor for changes in the electromagnetic field between the leaky coax transmit and receive cables within the sensor's detection pattern to detect standard intruder movement. The sensor must transmit an alarm signal to the alarm annunciation system upon detecting such changes. Provide sensors that detect a standard intruder moving through the sensor detection pattern at a speed of 0.06 to 7.6 m per second 0.2 to 25 fps.

Provide ported coaxial transmission and receive cables rated for direct burial. Provide sensors to obtain the designed coverage pattern with

adjustable sensitivity to 1 m 3 feet length by controls within the sensor signal processor. Controls must not be accessible when the sensor signal processor's housing is in place. Equip the sensor with a test indicator if it is an integral sensor signal processor function.

2.3.7.2.10 Active Infrared Sensor (Exterior)

a. The active infrared sensor detects a light beam interruption that links the transmitter and receiver caused by an intruder moving at a speed of less than 2.92 m per second 7.5 fps through the beam. The sensor must transmit an alarm signal to the alarm annunciation system upon detecting such an interruption.

b. The sensor must use a pulsed infrared light source. Multiple sensors must be able to operate within the same zone without interfering with each other. Provide sensors to obtain the designed coverage pattern with adjustable sensitivity with controls located within the sensor signal processor and not accessible when the sensor signal processor's housing is in place.

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

d. The sensor may incorporate remote test if it is an integral sensor function.

2.3.7.2.11 Video Motion Sensor (Exterior)

Provide a video motion sensor to detect changes in the video signal within a user defined detection zone as described in paragraph VIDEO ANALYTICS (VA). The system must detect changes in the video signal corresponding to a standard intruder moving within the defined detection zone and wearing clothing with a reflectivity that differs from that of the background scene by a factor of 2. Provide signal processing techniques to eliminate non-alarm background motion including light changes, trees blowing, and birds. Provide sensor with controls and method needed by the operator to define and adjust the sensor detection zone within the video picture.

Video motion sensor system must operate using [digital cameras] [thermal cameras] [or digital and thermal cameras]. The number of detection zones, the size of the detection zones, and the sensitivity of the detection zones are to be user definable. Provide sensors that accommodate multiple video inputs and have the capability of modular growth. The video inputs must accept composite video. The sensor must not require external sync for operation. Provide one alarm output for each video input. Provide number of video inputs and alarm outputs as required for an operable system. Rack-mount sensor equipment in a standard rack as described in paragraph EQUIPMENT RACK with hardware includes as required to mount the sensor components.

2.3.7.2.12 Radar

****

NOTE: Radar should be used in conjunction with

other detection and assessment systems such as VSS, to provide capability to extend the zone of protection to maximum standoff distances. The designer should contact the manufacturer of the product to determine that product's particular capabilities during design.

****

The radar system must provide intruder detection to [700] [_____] m [2300] [_____] feet. Provide monostatic type unit in which the transmitter and receiver are encased within a single housing unit (transceiver). The radar is to be equipped with a signal processor that is programmed to recognize reflected energy from the normal environmental surroundings and eliminate those objects relative to alarm. Provide unit with the capability of preprogramming specific parameters, size and speed, above which an alarm signal is generated.

The system is to provide alarm information to the ESS to identify specific zones of concern to include range and azimuth information, as a minimum. The information must have the capability of integrating with [VSS] [video motion sensor] systems, to "call" the cameras to a particular view for alarm verification. The system is to be able to retrofit with existing VSS or other detection systems. After radar system installation, post warning signs indicating radiation hazard as recommended by the manufacturer.

2.3.7.3 Duress Alarms (Hold Up Switch)

****

NOTE: The designer will show type and location of duress alarm switches. Duress alarm switches must meet requirements in UL 636.

****

UL 636. Duress alarm switches must provide the means for an individual to covertly notify the alarm annunciation system that a duress situation exists with no visible or audible signal in the secure area.

2.3.7.3.1 Hardwire Duress Alarms

Alarms must be capable of being secretly activated by the foot or hand of an average adult in both standing and seated positions. Upon activation the alarm signal is to lock-in until manually reset with a key or similar device and be readily identifiable by the ESS.

Provide sensors that are easy to operate and configured to minimize the possibility of accidental activation. Hardwire duress alarms must be rated for a minimum lifetime of 50,000 operations. Securely mount sensors in rugged, corrosion-resistant housing.

2.3.7.3.2 Wireless Duress Alarms

Wireless duress alarm switches to consist of portable alarm transmitters easily worn on the body or clothing. Alarm activation is to be by hand-operated switch protected from accidental activation, yet easily activated by hand when worn at the waist on body or clothing which transmits a unique identification code to one or more receivers located within a protected zone. The receivers, in-turn, are to transmit an alarm signal to the ESS system. [Sensor activation is to be automatic when

mounted on a body or clothing and the wearer is in a horizontal position for longer than [one] [5] [15] [_____] minutes, adjustable. Operations personnel must not be able to adjust time interval activation.]

Provide switches rated for a minimum lifetime of 50,000 operations and have a range of at least 762 m 2500 feet. Wireless switches must be fully supervised, where the transmitter automatically transmits (checks in) to the receiver on a regular basis to test the system for low battery, tamper, and inactive status.

2.3.7.4 Tamper Switches

****

NOTE: For Army projects, the designer should confirm with USACE Electronic Security Systems Mandatory Center of Expertise if the maintenance position is required. For Air Force and NAVFAC projects, include the requirement for a maintenance position switch.

****

a. Corrosion-resistant tamper switches are required for the following IDS and VSS equipment with hinged doors or removable covers that contain open circuits:

(1) Enclosures

(2) Cabinets

(3) Housings

(4) Boxes

(5) Raceways

(6) Fittings

(7) Sensors

b. Tamper switches are 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. One second is the minimum amount of time required to depress or defeat the tamper switch after opening or removing the cover. Enclosure and tamper switch must 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.

c. Tamper switches on doors which are opened to make normal maintenance adjustments to the system and to service power supplies must [not] have a maintenance position. [Provide two positions tamper switches.]

2.3.7.4.1 Tamper Switch Performance Requirements

Tamper switches are to 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. Annunciated to be clearly distinguishable from intrusion detection alarms and exempt from being disarmed, shunted, or silenced.

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

e. Wired to break the circuit when the door or cover is disturbed.

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

2.3.8 Intrusion Detection System Date and Time

Provide system date and time per paragraph DATE AND TIME GENERATOR.

2.4 ACCESS CONTROL SYSTEM (ACS)

****

NOTE: The designer must ensure that the Access Control System components are compatible with Common Access Cards (CAC). CAC is the principal identity credential of the Government.

Obtain clear requirements for separate and stand-alone ACS and separate and stand-alone IDS or a system that is capable of both ACS and IDS capability.

For HSPD-12 access control projects, ensure system utilizes the GSA FIPS 201 Evaluation Program Approved Products List.

****

Provide an access control system based upon a modular distributed microprocessor architecture complete with access control cards and ready for operation.

a. The ACS card credentials are required to be Common Access Cards (CAC), and CAC cards are being provided by the Government. [Interface system with and provide alarm and other status to the overall ESS.] [Provide system monitoring and control for the ESS.] Provide ACS that meets the communications requirements of UL 1076 and UL 294 and has the capability of controlling up to [4] [8] [16] [_____] card readers and keypads per card reader controller, [128] [256] [512] [_____] alarm inputs, or [128] [256] [512] [_____] relay outputs or any components combination.

b. System is to grant or deny access or exit based upon:

(1) Keypad identification data

(2) [Common Access Card (CAC)] [Personal Identity Verification (PIV)] card identification data

(3) Video

(4) Biometric reader identification data

(5) Smart card identification data

(6) Identification technologies combination

(7) Input through the access control devices compared to data stored within the system

(8) Time of day, day of week, and special day and holiday scheduling with card validation override.

c. Decision to grant or deny access or exit is to be based upon authorization for such data to be input at a specific location for the current duration. [Access decisions for high security areas are to be based upon two identification technology combinations: card and keypad or card and biometric.]

d. Provide ACS that supports the configuration and simultaneous monitoring of multiple access control devices when TCP/IP communication interfaces are used between the ESS and the primary Access Control Unit (ACU). The events of the ACS are to be viewable as separate or as a combined list of all ESS events. Provide overall control of the ACS, alarm monitoring, and photo identification through software control of the ESS.

e. Access control, photo imaging, and programming data must reside on a single database and instantly accessible to every networked PC workstation connected to the ESS.

f. Provide both supervised and non-supervised alarm point monitoring.

g. Provide the capability to arm or disarm alarm points both manually and automatically by time of day, day of week or by operator command and the capability to disarm alarm points based on a valid access event.

[h. When used for elevator control, the ACS is to grant access to elevator floors based on a valid credential, or by schedule.]

i. Provide programmable 'delay' setting for all alarm points. The alarm points are not to report an ENTRY type alarm until the delay setting has expired and not report a dwell type alarm condition until the alarm has been active for the full delay period.

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

[k. Provide the ability to display a stored 'video image' of the cardholder based on card activity and switch real-time VSS camera to the card reader location for specific card usage. The card reader must not activate the door lock until positive operator acknowledgment from the SCC.]

[2.4.1 ACS Badging Requirements

****
NOTE: The designer must show justification for including badging. CAC cards will be provided offsite and are not part of this contract.
****

Include fully integrated badging capabilities, including image capture, image editing, badge design, and badge printing. Allow for each cardholder to be assigned to both a badge design formatted for badge printing and a dossier design formatted for standard paper printing. The system must permit the storage of four different images:

a. Main photograph

b. Alternate photograph

c. Signature

d. Fingerprint

Provide for interfacing with external badge programs, in which stored photo images are displayed in a cardholder information window, but other badge features are supported by the external program. Include one or more networked PC workstations with the photo imaging components at which all the required image capture equipment has been installed.

]2.4.2 ACS Programming

Provide software capable of, but not limited to, the following programming:

2.4.2.1 Time Schedules

Provide up to [256] [_____] user-definable time schedules. These time schedules are to determine the day(s) and times that access will be granted, or a scheduled event is to occur. Any and all of the time schedules are to be available for defining access privileges and scheduled events. Provide ALWAYS and NEVER schedules that cannot be altered or removed from the system. Each user-defined time schedule must 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.

2.4.2.2 Special Days

Provide an unlimited number of user definable special days to be used for configuring exceptions to the normal operating rules, typically for specifying holiday operating rules. Allow for each special day to be assigned to a user-defined type.

2.4.2.3 ACU Daylight Savings Time Adjustment

Provide a software-configurable, user defined adjustment for Daylight Savings Time. The ACU must not need to be connected to a PC workstation for the adjustment to occur.

2.4.2.4 Scheduled Events

Any access-controlled reader is to be capable of scheduled unlock periods

to allow for card-free access. The access-controlled reader is to also be capable of requiring one valid access event before beginning a scheduled unlock period.

Any access control point is to 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 must not reduce the number of card readers or alarm points available in the ACU(s). Any designated alarm input must be able to be scheduled [Armed and Disarmed] [Secured and Accessed]. Any relay output must be capable of scheduled ON and OFF periods to allow for automatic input and output system control.

2.4.2.5 Maximum User Capability

Up to [64,000] [_____] individual users may be given access cards or codes and have their access controlled and recorded.

2.4.2.6 Access Groups

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

2.4.2.7 Active and Expire Dates

Any card or 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.

2.4.2.8 Maximum Use Settings

Any card or 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.

2.4.2.9 Door Outputs

Provide each access control reader with [one] [two] [_____] dedicated relay outputs. Both relays are to provide Normally Open and Normally Closed contacts. Use the first relay for electric lock control while the second is software configurable to activate for door forced open, door left open too long, duress, passback violations, invalid access attempts and valid unlock conditions. Allow for both relays to be separately programmable for energize times from [1] [_____] second to [10] [_____] minutes. The second relay must allow a delay time to be specified, causing its activation to be delayed after an activating condition occurs.

[2.4.2.10 Anti-Passback

Provide global anti-passback capability. Any door on the system can be linked to one of [256] [_____] user defined passback areas or two [2] [_____] pre-defined areas. Each door may be set up to automatically forgive passback entries at one of the following intervals:

(1) Never

(2) Midnight

(3) Every 12 hours (Midnight and Noon)

(4) Every 6 hours

(5) Every 2 hours

(6) Each hour

(7) 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 must be a global function and operate completely independent of the ACS software, except configuring the passback rules. Additionally, the operator is to have the ability to manually forgive an individual user or all users by command from the ACS.

][2.4.2.11 Two Person Rule

Any access control reader on the system is to have the ability via software programming to require two valid cards for access. Any access control reader on the system that includes a keypad is to also have the ability to require a valid PIN number associated with each of the two valid cards.

]2.4.2.12 User List or Who's In (Muster Reports)

Provide the capability to generate dynamic lists of users in certain access-controlled areas, based either upon selected users or selected areas. The lists must have the option of automatically refreshing after a user-selected interval of time.

2.4.2.13 Crisis Mode

Provide support for a "crisis mode", in which user-selected alarm point activations cause changes to user access privileges. The changes to user access privileges must be configurable to restrict normal access to no access or limited access.

2.4.2.14 Door Groups

Allow up to [256] [_____] door groups to be configured. Doors belonging to the same group are capable of being locked, unlocked, disabled, and enabled on command from the ACS.

2.4.2.15 Door Interlocking

Allow a group of doors to be software configured so that if any door in the group is unsecure, all other doors are automatically disabled. This feature is also known as a "mantrap" configuration. The interlocking features must not require the ACS to be on-line for proper operation.

2.4.2.16 PIN Required

Provide support for the required use of a keypad code, in addition to a valid credential during user-selected schedules.

2.4.2.17 Remote Door Control

Provide the ESS operator the capability of manually controlling any access point by issuing a simple command from the ACS. Provide the operator the ability to lock, unlock, enable, and disable any door or Door Group in this manner. This activity is to cause an entry to be logged displaying the door name, number and time that it was performed.

2.4.2.18 Key Control

When interfaced with an approved key-control system, the system is to allow users to deny access to certain doors for any users who have keys in their possession.

[2.4.2.19 Guard Tour

Provide support for user-defined guard tours configurable in a set pattern of tour points or following a mode in which all tour points can be visited in any order within an allotted time. Allow for a tour to be started by ACS command, by use of a selected card at a selected reader, or by use of a selected keypad code at a selected keypad. Detect guard late-to-point, point missed, and point out-of-sequence events. Generate a report at tour completion.

]2.4.2.20 Reader Disable

****
NOTE: If it is a project requirement, provide camera coverage of the card readers.
****

Provide support for disabling readers in reaction to a user-selected number of invalid access attempts. [Locate a camera to view the card reader and interface to record the events of invalid access attempts.]

2.4.2.21 Disable Event Messages

Allow users to disable user-selected event messages (Door Forced Open, Door Open Too Long, Door Closed, Request to Exit) for user-selected doors. Allow users to disable certain messages (Door Forced Open, Door Open Too Long) according to a user-selected schedule.

2.4.2.22 Input and Output Groups

Allow for up to [256] [_____] user-defined (input and output) groups to be defined. Each Input device is to be able to be linked to these groups for arming, disarming, shunting and unshunted as well as output control.

2.4.2.23 Delays

Each alarm device must allow a delay to be specified which is either an entry type or a dwell type. An entry-type delay is to prevent the input from issuing an alarm event until the delay elapses. If unarmed during the delay period, the alarm is to be ignored. A dwell-type delay requires the input to remain in the alarm state for the full delay duration before issuing an alarm.

[2.4.2.24 Remote Input Control

****
NOTE: Remote access is not allowed for certain security locations such as SCIF and SAPF areas.
****

[Provide the operator the capability of manually controlling any alarm, input point, alarm partition or group by issuing a simple command from the SCC on the ACS allowing the ability to shunt, unshunt, disable and restore any input in this manner. This activity must cause an entry to be logged displaying the input name and time that it was performed. The arm and disarm, shunt and unshunt any alarm partition or group from the SCC must not be permissible in ICS 705-1 applications.] [The operator cannot have the capability to shunt or disable a tamper alarm.]

]2.4.2.25 Output Configuration

Allow each output relay to be software configurable as:

(1) Follows

(2) Latch

(3) Timeout

(4) Scheduled

(5) Timeout Re-triggerable

(6) Limit

(7) Counter

Allow for a time schedule to automatically control the activation and de-activation of the Scheduled type with all other types configured to activate based on input and output group conditions. Additionally, a time schedule must be specified to configure when the output is to actively monitor the input and output groups.

2.4.2.26 Remote Output Control

Provide the operator the capability of manually controlling any output point by issuing a simple command from the SCC. Based upon the output type, provide the ESS operator the ability to ENABLE, DISABLE, turn ON and turn OFF any output in this manner. A FOLLOWS type output must not be capable of being turned OFF or ON. Log an entry when this activity is performed displaying the output name and time performed. Manual control of outputs are not permissible in ICS 705-1 applications.

2.4.2.27 Remote Reset Command

Provide the capability for any ACU to reset manually or by command issued from the ACS with the option of simulating the ACU reset settings or forcing a reset type as specified by the user. The remote reset command is not to cause the ACU to degrade its level of protection to any access points defined.

2.4.2.28 Time Zone

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.

2.4.2.29 User-Selected LED Behavior

Allow the user to select different behaviors for the LEDs of each access-controlled reader.

2.4.2.30 Traced Cards

Provide the capability of selecting any number of cardholders for the purpose of limiting reports to only traced users displaying all traced cardholder events in a user-selected alternate color.

[2.4.2.31 Badge Print Tracking

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.

]2.4.3 Error and Throughput Rates

Rates must be portal to portal performance averages obtained when processing individuals one at a time. Features are not to reduce capability to meet throughput requirements when serial verification techniques or multiple attempts are required to satisfy error performance 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 must both be less than [0.1] [_____] percent. At the error rates, subsystem access throughput rate must be minimum of [12] [_____] individuals per minute through one card reader and keypad access control device.

2.4.4 Access Control System Central Processing

a. Provide serial management and control of system processing. Provide a microprocessor control device able to monitor and control units and up to [32] [_____] card reader and keypad access control devices. Central processor must interrogate and receive responses from each ACU within 100 milliseconds. Failure to respond to an interrogation is to cause an alarm.

b. Provide the central processor with a [Ethernet] [USB] [_____] 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] [_____] cardholders with by-name alphanumeric printout, and for automated [subsystem] [IDS] monitoring, management, and control functions.

c. Provide enrollment equipment as required in paragraph ENROLLMENT CENTER EQUIPMENT.

d. Provide system configuration controls and electronic diagnostic aids

for subsystem setup and troubleshooting with the central processor. Components are not to be accessible to operations personnel and must be tamper alarmed.

2.4.5 Access Control Unit(ACU)

Provide micro-processor based ACU with all access and input and output decisions to be made by the individual ACU(s). Provide modular solution which will allow for present security requirements and the capability to expand. Configure all field ACU panels to intercommunicate via [RS-422/485] or [RS-232 hardwired] or [TCP/IP]. Equip all field ACU(s) with a tamper contact.

Designate one ACU as "Primary", responsible for all ACS-to-ACU communications. All other ACU(s) up to a maximum of [16] [32] [64] [256] [_____] are to be designated as "Secondary" and communicate with the "Primary" via an [RS-422/485 hardwire], [TCP/IP network] or [fiber-optic configuration]. Provide ACU capable of, but not limited to, the following:

a. Built-in surge suppression circuitry on plug-in modular circuit boards with surge suppression, configured as an integral component of the system and self-sacrificing in the event of extreme surges or spikes.

b. 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.

c. Each port configured by ACS to support any one of the following peripheral devices:

(1) Card reader

(2) Alarm Monitoring Module

(3) Output Relay Module

(4) Elevator Reader

(5) Elevator Output Module

Any device combination can be supported on each ACU, up to a total of [2] [4] [8] [16] [_____] devices per ACU.

d. Capability of supporting multiple card reader technologies simultaneously, including:

(1) Keypad

(2) Card and Keypad

(3) [CAC] [PIV] compatible

(4) Biometrics

This capability must be an integral part of the ACU and will not require special external equipment. See NIST SP 800-116.

e. Built-in battery back-up of programmed information sustainable for a period of at least 90 days.

f. Powered by a [12] [24] [____] VDC power source rated at a minimum of [2] [_____] amperes with 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 [8] [_____] hours continuous service.

g. Electric strikes, other locking devices and ancillary peripherals on a separate power supply with battery back-up for continued operation in the event of power failure as specified in paragraph BACKUP POWER.

h. A minimum of a [10,300] [_____] event log buffer per ACU to record and hold access and alarm activity information until the ACS is connected and receives the information. Provide a software-configurable warning log buffer filling notification for ACU(s) configured with network switch capabilities.

2.4.6 Access Control Devices

****
NOTE: The Common Access Credential (CAC) cards are only supplied by the Government and must meet the requirements in UFC 4-021-02. Provide a card reader with an integrated keypad for portals where the added security of credential plus code access is required.
****

****
NOTE: This paragraph may be removed by the designer if encryption is not required by the project.
****

UL 294. The card, card reader, and panels must meet encryption requirements that are specified in paragraph DATA ENCRYPTION. Devices are to 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.

2.4.6.1 Card Readers

Provide [surface], [semi flush], [pedestal], or [weatherproof mountable] card readers as indicated for each individual location. Provide contactless [contactless w/keypad] [contact/contactless w/keypad] [contact/contactless w/keypad and fingerprint] type card readers capable of reading [Keypad] [[CAC] [PIV] and Keypad] [[CAC] [PIV] cards] [Biometric] type of access control cards.

Keypads must contain an alphanumeric and special symbols keyboard with symbols [arranged in ascending ASCII code ordinal sequence] [scramble type]. Provide keypad [as a stand-alone device] [or] [integrated into the card reader].

2.4.6.1.1 Contact Card Readers

Provide contact card readers that can read credential [PIV] [CAC] cards whose characteristics of size and technology meet those defined by ANSI ISO/IEC 7816 and meet NDAA Compliance and NIST FIPS 201-2 Approval Letter for ACS Products.

Provide readers with "flash" download capability to accommodate card format changes and the capability of reading the card data and transmitting the data, or a portion thereof, to the ESS control panel.

2.4.6.1.2 Contactless Card Readers

Provide contactless card readers that can read credential [PIV] [CAC] cards whose characteristics of size and technology meet those defined by ANSI ISO/IEC 7816 in close proximity to the card reader and meet NDAA Compliance and NIST FIPS 201-2 Approval Letter for ACS Products.

Provide readers with "flash" download capability to accommodate card format changes and the capability of reading the card data and transmitting the data, or a portion thereof, to the ESS control panel.

2.4.6.1.3 Card Readers With Integral Keypad and Biometric Reader

Equip contact and contactless card readers with integral keypads and biometric readers as specified in paragraph KEYPADS and as in FINGERPRINT ANALYSIS SCANNER.

2.4.6.1.4 Card Readers with Integral Keypad

Equip contact and contactless card readers with integral keypads as specified in paragraph KEYPADS.

2.4.6.1.5 Card Reader Display

Provide card readers with an LED or other visual indicator display which indicate power ON and OFF and whether user passage requests have been accepted or rejected.

2.4.6.1.6 Card Reader Response Time

The card reader is to respond to passage requests by generating a signal to the local processor.

2.4.6.1.7 Card Reader Power

Power the card reader from the source as shown on the drawings. The card reader must not dissipate more than 5 Watts.

2.4.6.1.8 Card Reader Mounting Method

Provide card readers suitable for [surface], [semi-flush], [pedestal], or [weatherproof] mounting as required.

2.4.6.2 Keypads

****

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

****

Entry control keypads are to use unique alphanumeric and other symbol combinations as an identifier. Keypads must contain an integral alphanumeric and special symbols keyboard with symbols arranged in [ascending ASCII code ordinal sequence] [random scrambled order]. Communications protocol is to be compatible with the local processor.

2.4.6.2.1 Keypad Display

Keypads are to include an LED or other type of visual indicator display and provide [visual] [visual and audible] status indications indicating power ON and OFF and whether user passage requests have been accepted or rejected.

The maximum horizontal and vertical viewing angles are to be limited by the keypad display or enclosure. The maximum horizontal viewing angle must be no more than plus and minus 5 degrees off a vertical plane perpendicular to the plane of the face of the keypad display. The maximum vertical viewing angle must be no more than plus and minus 15 degrees off a horizontal plane perpendicular to the plane of the face of the keypad display.

2.4.6.2.2 Keypad Response Time

The keypad is to respond to passage requests by generating a signal to the local processor.

2.4.6.2.3 Keypad Power

Power the keypad from the source as shown on the drawings. The keypad must not dissipate more than 5 Watts.

2.4.6.2.4 Keypad Mounting Method

Provide keypads suitable for [surface], [semi-flush], [pedestal], or [weatherproof] mounting as required.

2.4.6.2.5 Keypad Duress Codes

Provide a means for users to indicate a duress situation by entering a special code into the keypad.

2.4.6.3 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. CAC cards will be provided by the Government.

****

Provide cards with the capability of modification and lamination during enrollment process without readability reduction for use as a picture and identification badge. Cards must 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 a non-duplicated unique facility access control subsystem identification code common to access control cards within the card binary data.

[Configure cards for use as a photo identification card suitable for lamination.]

PIV cards must be be listed on the "FIPS 201 Approved Products List - PIV Card" found on the www.idmanagement.gov website.

2.4.6.3.1 Credential Card Modification

Provide entry control cards that can be modified by lamination or direct print process during the enrollment process for use as a picture and identification badge as needed for the site without readability reduction. Credential cards must allow adding at least one slot or hole for a clip affixing the credential card to the type of badge holder used at the site.

2.4.6.3.2 Card Size and Dimensional Stability

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

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

2.4.6.3.3 Card Materials and Physical Characteristics

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

2.4.6.3.4 Card Construction

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

Provide credential cards of core and laminate or monolithic construction. Hot stamp into material or direct print onto lettering, logos and other markings. [Incorporate [holographic images] [phosphorous ink] as a security enhancement.] [Provide a means to allow onsite assembly and credential cards lamination by Government.]

2.4.6.3.5 Card Durability and Maintainability

The credential cards must yield a useful lifetime of at least 5 years. The credential card must be able to be cleaned by wiping the credential card with a sponge or cloth wet with a soap and water solution.

2.4.6.3.6 Warranty

Include a minimum 3-year warranty.

[2.4.6.4 Personal Identity Verification Equipment

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

2.4.6.4.1 Hand Geometry

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

a. Hand geometry devices are to use unique human hand measurements to identify authorized, enrolled personnel. The device is to incorporate positive measures to establish that the hand being measured by the device belongs to a living human being. Provide alignment system which allows the user's hand to remain in full view of the user at all times.

b. During the scan process the hand geometry device is to make 3 dimensional measurements of the size and shape of the user's hand. The hand geometry device is to automatically initiate the scan process once the user's hand is properly positioned by the alignment system. Either left or right hands are to be able to be used for enrollment and verification. User hand geometry template must not require more than 50 eight-bit bytes of storage media space.

c. Hand geometry devices must include an LED or other type of visual indicator display and provide [visual] [visual and audible] status indications and user prompts. The display is to indicate power ON and OFF and whether user passage requests have been accepted or rejected.

2.4.6.4.1.1 Template Update and Acceptance Tolerances

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

2.4.6.4.1.2 Average Verification Time

The hand geometry device is to respond to passage requests by generating signals to the local processor. The verification time must be 1.5 seconds or less from the moment the hand geometry device initiates the scan

process until the hand geometry device generates a response signal.

2.4.6.4.1.3 Modes

a. Provide an enrollment mode, recognition mode, and code or credential verification mode that is selectable by the system manager or operator from the SCC.

b. The enrollment mode is to create a hand template for new personnel and enter the template into the entry control database file created for that person. Template information must be compatible with the system application software.

c. The hand geometry device allows passage when the hand scan data from the verification attempt matches a hand geometry template stored in the database files when operating in recognition mode.

d. The hand geometry device allows passage when the hand scan data from the verification attempt matches the hand geometry template associated with the identification code entered into a keypad or matches the hand geometry template associated with credential card data read by a card reader when operating in code or credential verification mode.

2.4.6.4.1.4 Reports

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

2.4.6.4.1.5 Electrical

The hand geometry device must not dissipate more than 45 Watts from the source indicated.

2.4.6.4.1.6 Mounting Method

Provide hand geometry devices suitable for [surface], [flush], or [pedestal] mounting as required.

2.4.6.4.1.7 Communications Protocol

The communications protocol between the hand geometry device and the local processor must be compatible.

2.4.6.4.2 Fingerprint Analysis Scanner

****

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

****

a. Fingerprint analysis scanners are to use a unique human fingerprint pattern to identify authorized, enrolled personnel. The device is to incorporate positive measures to establish that the fingers being measured by the device belong to a living human being. Provide alignment system which allows the user's fingers to always remain in full view of the user.

b. The fingerprint analysis scanner is to perform an optical or other type of scan of the user's fingers during the scan process. The fingerprint analysis scanner is to automatically initiate the scan process provided the user's fingers are properly positioned. Each user fingerprint template must not require more than 1250 eight-bit bytes of storage media space.

c. Include an LED or other type of visual indicator display and provide [visual] [visual and audible] status indications and user prompts. The display is to indicate power ON and OFF, and whether user passage requests have been accepted or rejected.

2.4.6.4.2.1 Template Update and Acceptance Tolerances

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

2.4.6.4.2.2 Average Verification Time

The fingerprint analysis scanner is to respond to passage requests by generating signals to the local processor. The verification time must be 2.0 seconds or less from the moment the fingerprint analysis scanner initiates the scan process until the fingerprint analysis scanner generates a response signal.

2.4.6.4.2.3 Modes

a. Provide an enrollment mode, recognition mode, and code or credential verification mode that is selectable by the system manager or operator from the SCC.

b. The enrollment mode is to create a fingerprint template for new personnel and enter the template into the system database file created for that person. Template information must be compatible with the system application software.

c. The fingerprint analysis scanner is to allow passage when the fingerprint data from the verification attempt matches a fingerprint template stored in the database files when operating in recognition mode.

d. The fingerprint analysis scanner allows passage when the fingerprint data from the verification attempt matches the fingerprint template associated with the identification code entered into a keypad or matches the fingerprint template associated with credential card data read by a card reader when operating in code or credential verification mode.

2.4.6.4.2.4 Reports

The fingerprint analysis scanner is to store template transactions involving fingerprint scans. The template match scores are to be stored

in the matching personnel data file in a file format compatible with the system application software, and to be used for report generation.

2.4.6.4.2.5 Electrical

The fingerprint analysis scanner must not dissipate more than 45 Watts from the source indicated.

2.4.6.4.2.6 Mounting Method

Provide fingerprint analysis scanners suitable for [surface], [flush], or [pedestal] mounting.

2.4.6.4.2.7 Communications Protocol

The communications protocol between the fingerprint analysis scanner and its associated local processor must be compatible.

2.4.6.4.3 Iris Scan Device

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

The iris scan identification device is to use the unique patterns found in the iris of the human eye to identify authorized, enrolled personnel. The device is to use ambient light to capture an image of the iris of a person presenting themselves for identification. The resulting video image is to be compared against a stored template that was captured during the enrollment process. The device authenticates the presenting individual as identified when the presented image is sufficiently similar to the stored image template. Provide the ability to adjust the threshold of similarity.

Users who wear contact lenses or eyeglasses are not to adversely affect the efficiency and accuracy of the device. Facial contact with the device is not to be required for identification. Provide a manual push-button to initiate the scan process when the user has aligned their eye in front of the device. Provide adjustments to accommodate differences in user height.

2.4.6.4.3.1 Display Type

Include an LED or other type of visual indicator display and provide [visual] [visual and audible] status indications and user prompts. The display is to indicate power ON and OFF and whether user passage requests have been accepted or rejected.

2.4.6.4.3.2 Template Update and Acceptance Tolerances

Iris scanners are not to automatically update a user's template. Significant changes in an individual's eye requires re-enrollment. Provide an adjustable acceptance tolerance or template match criteria under system manager or operator control. The iris scanner is to determine when multiple attempts are needed to verify the iris being scanned, and automatically prompt the enrollee for additional attempts up to a maximum of three. Three failed attempts generates an entry control alarm.

2.4.6.4.3.3 Average Verification Time

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

2.4.6.4.3.4 Modes

a. Provide an enrollment mode, recognition mode, and code or credential verification mode that is selectable by the system manager or operator from the Security Command Center.

b. The enrollment mode is to create an iris template for new personnel and enter the template into the system database file created for that person. Template information must be compatible with the system application software.

c. The iris scanner is to allow passage when the iris scan data from the verification attempt matches the iris scan template stored in the database files when operating in recognition mode.

d. The iris scanner allows passage when the iris scan data from the verification attempt matches the iris scan template associated with the identification code entered into a keypad or matches the iris scan template associated with credential card data read by a card reader when operating in code or credential verification mode.

2.4.6.4.3.5 Reports

The iris scanner is to store template transactions involving iris scans. The template match scores are to be stored in the matching personnel data file in a file format compatible with the system application software and be used for report generation.

2.4.6.4.3.6 Electrical

The eye scanner must not dissipate more than 45 Watts from the voltage source indicated.

2.4.6.4.3.7 Mounting Method

Provide eye scanners suitable for [surface], [flush], or [pedestal] mounting.

2.4.6.4.4 Facial Scanner

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

a. Facial recognition scanners are to use a unique human facial patterns to identify authorized, enrolled personnel. The device is to incorporate positive measures to establish that the face being measured by the device belong to a living human being. Provide alignment system which allows the user's face to always remain in full view of the user.

b. The facial recognition scanner is to perform an optical or other type of scan of the user's face during the scan process. The facial recognition scanner is to automatically initiate the scan process provided the user's face is properly positioned.

c. Include an LED or other type of visual indicator display and provide [visual] [visual and audible] status indications and user prompts. The display is to indicate power ON and OFF, and whether user passage requests have been accepted or rejected.

2.4.6.4.4.1 Template Update and Acceptance Tolerances

Facial recognition scanners are not to automatically update an user's profile. Significant changes in an individual's face require re-enrollment. Provide an adjustable acceptance tolerance or template match criteria under system manager or operator control. The facial recognition scanner is to determine when multiple attempts are needed for data verification, and automatically prompt the enrollee for additional attempts up to a maximum of 3. Three failed attempts are to generate an entry control alarm.

2.4.6.4.4.2 Average Verification Time

The facial recognition scanner is to respond to passage requests by generating signals to the local processor. The verification time must be 2.0 seconds or less from the moment the facial recognition scanner initiates the scan process until the facial recognition scanner generates a response signal.

2.4.6.4.4.3 Modes

a. Provide an enrollment mode, recognition mode, and code or credential verification mode that is selectable by the system manager or operator from the SCC.

b. The enrollment mode is to create a facial template for new personnel and enter the template into the system database file created for that person. Template information must be compatible with the system application software.

c. The facial recognition scanner is to allow passage when the facial data from the verification attempt matches a facial template stored in the database files when operating in recognition mode.

d. The facial recognition scanner allows passage when the facial data from the verification attempt matches the facial template associated with the identification code entered into a keypad or matches the facial template associated with credential card data read by a card reader when operating in code or credential verification mode.

2.4.6.4.4.4 Reports

The facial recognition scanner is to store template transactions involving facial scans. The template match scores are to be stored in the matching personnel data file in a file format compatible with the system application software, and to be used for report generation.

2.4.6.4.4.5 Electrical

The facial recognition scanner must not dissipate more than 45 Watts from the source indicated.

2.4.6.4.4.6 Mounting Method

Provide facial recognition scanners suitable for [surface], [flush], or [pedestal] mounting.

2.4.6.4.4.7 Communications Protocol

The communications protocol between the facial recognition scanner and its associated local processor must be compatible.

2.4.6.4.5 Palm Scanner

****

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

****

a. Palm scanners are to use a unique human hand pattern to identify authorized, enrolled personnel. The device is to incorporate positive measures to establish that the palm being scanned by the device belongs to a living human being. Provide alignment system which allows the user's hand to always remain in full view of the user.

b. The palm scanner is to perform an optical or other type of scan of the user's hand during the scan process. The palm scanner is to automatically initiate the scan process provided the user's hand is properly positioned. Each user's hand template must not require more than 1250 eight-bit bytes of storage media space.

c. Include an LED or other type of visual indicator display and provide [visual] [visual and audible] status indications and user prompts. The display is to indicate power ON and OFF, and whether user passage requests have been accepted or rejected.

2.4.6.4.5.1 Template Update and Acceptance Tolerances

Palm scanners are not to automatically update a user's profile. Significant changes in an individual's hand requires re-enrollment. Provide an adjustable acceptance tolerance or template match criteria under system manager or operator control. The palm scanner is to determine when multiple attempts are needed for data verification, and automatically prompt the enrollee for additional attempts up to a maximum of 3. Three failed attempts are to generate an entry control alarm.

2.4.6.4.5.2 Average Verification Time

The palm scanner is to respond to passage requests by generating signals to the local processor. The verification time must be 2.0 seconds or less from the moment the palm scanner initiates the scan process until the palm scanner generates a response signal.

2.4.6.4.5.3 Modes

a. Provide an enrollment mode, recognition mode, and code or credential

verification mode that is selectable by the system manager or operator from the SCC.

b. The enrollment mode is to create a hand template for new personnel and enter the template into the system database file created for that person. Template information must be compatible with the system application software.

c. The palm scanner is to allow passage when the hand data from the verification attempt matches a hand template stored in the database files when operating in recognition mode.

d. The palm scanner allows passage when the hand data from the verification attempt matches the hand template associated with the identification code entered into a keypad or matches the hand template associated with credential card data read by a card reader when operating in code or credential verification mode.

2.4.6.4.5.4 Reports

The palm scanner is to store template transactions involving hand scans. The template match scores are to be stored in the matching personnel data file in a file format compatible with the system application software, and to be used for report generation.

2.4.6.4.5.5 Electrical

The palm scanner must not dissipate more than 45 Watts from the source indicated.

2.4.6.4.5.6 Mounting Method

Provide palm scanners suitable for [surface], [flush], or [pedestal] mounting.

2.4.6.4.5.7 Communications Protocol

The communications protocol between the palm scanner and its associated local processor must be compatible.

]2.4.6.5 Portal Control Devices

****

NOTE: Portal Control Devices must be designed in accordance with NFPA 101, Means of Egress.

If ESS is to be integrated with the Fire Alarm System provide appropriate signage in accordancewith NFPA 101.

The designer must meet the requirements in Section 08 71 00 DOOR HARDWARE.

****

Portal control devices must meet the requirements in Section 08 71 00 DOOR HARDWARE.

2.4.6.5.1 Push-Button Switches

a. Provide momentary contact, back lit push buttons and stainless-steel switch enclosures for each push button. Provide switch enclosures suitable for [flush] [surface] mounting as required and push buttons suitable for flush mount in the switch enclosures. The push button switches are to meet the requirements of NEMA 250 for the area in which they are to be installed.

b. Where multiple pushbuttons are housed within a single switch enclosure stack vertically with each push button switch labeled with 7 mm 1/4 inch high text and symbols. The push button switches are to be connected to the local processor associated with the portal to which they are applied and operate the appropriate electric strike, electric bolt or other facility release device.

c. The continuous current of the IDS circuit is to be no more than 50 percent of the continuous current rating of the device supplied. Provide push button switches with double-break silver contacts that will make 720 VA at 60 amperes and break 720 VA at 10 amperes.

2.4.6.5.2 Panic Bar

Include panic bar emergency exit hardware on emergency exit doors as indicated. Provide an alarm shunt signal from the panic bar emergency exit hardware to the appropriate local processor. Provide panic bar compatible with [mortise-] [rim-] mount door hardware and operate by retracting the bolt.

2.4.6.5.2.1 Emergency Egress With Alarm

[Include a conspicuous warning sign with 25 mm 1 inch high, red lettering notifying personnel that an alarm will be annunciated if the panic bar is operated.

] Panic bar hardware operation is to generate an intrusion alarm [and local alarm annunciation]. The panic bar must depend upon a mechanical connection only and not depend upon electric power for operation, except for local alarm annunciation and alarm communications.

2.4.6.5.2.2 Normal Egress

Panic bar hardware operation is not to generate an intrusion alarm. The panic bar must depend upon a mechanical connection only when exiting. Provide the exterior, non-secure side of the door with an electrified thumb latch or lever to provide access after the credential I.D. authentication by the ESS.

Signal Switches: Strikes/bolts are to include signal switches indicating to the system when the bolt is not engaged, or the strike mechanism is unlocked. The signal switches are to report a forced entry to the system.

2.4.6.5.2.3 Delay Egress With Alarm

Include a conspicuous warning sign with 25 mm 1 inch high, red lettering notifying personnel that an alarm will be annunciated if the panic bar is operated.

Delay operation [15] [_____] seconds after initiation for portal control

devices.

2.4.6.5.3 Electric Door Strikes and Bolts

****
NOTE: The designer will specify whether the electric strike or lock will fail open, fail secure, or other configuration (such as fail security for entry into higher security area, while failing open for egress from the area). The designer must coordinate this with requirements of the site safety and fire personnel. The designer will determine if signal switches are required for the site.
****

Configure electric door strikes and bolts to [release automatically] [remain secure] in case of power failure using DC power to energize the solenoids. Incorporate end-of-line resistors to facilitate line supervision by the system. Install metal-oxide varistors (MOVs) to protect the controller from reverse current surges if not incorporated into the electric strike or local controller. Electric strikes must have a minimum forcing strength of 101 kN 2300 pounds.

2.4.6.5.3.1 Solenoid

The actuating solenoid for the strikes and bolts furnished must not dissipate more than 12 Watts and operate on [12] [24] VDC. The inrush current must not exceed 1 ampere and the holding current must not be greater than 500 milli-amperes. The actuating solenoid must move from the fully secure to fully open positions in not more than 500 milliseconds.

2.4.6.5.3.2 Signal Switches

Strikes and bolts are to include signal switches indicating to the system when [the bolt is not engaged] [the strike mechanism is unlocked]. The signal switches are to report a forced entry to the system.

2.4.6.5.3.3 Tamper Resistance

The electric strike and bolt mechanism is to be encased in hardened guard barriers to deter forced entry.

2.4.6.5.3.4 Size and Weight

Electric strikes and bolts are to be compatible with standard door frame preparations.

2.4.6.5.3.5 Mounting Method

Provide electric strikes and bolts suitable for use with single and double door installations, with [mortise-] [rim-] type hardware as indicated, and compatible with right- or left-hand mounting.

2.4.6.5.3.6 Astragals

See Section 08 71 00 DOOR HARDWARE for Astragal lock guards.

2.4.6.5.4 Electrified Mortise Lock

****

NOTE: The electrified mortise locks provide an excellent solution for stairwell doors that require positive latching when unlocked. The doors should be built with a raceway within the door for the power and signal wire. A wire transfer hinge or other device is required to get the wire from the door to the door frame for connection with the access control system.

****

Configure electrified mortise locks to [release automatically] [remain secure] in case of power failure using DC power to energize the solenoids. Provide solenoids rated for continuous duty. Incorporate end-of-line resistors to facilitate line supervision by the system. Install metal-oxide varistors (MOVs) to protect the controller from reverse current surges if not incorporated into the electric strike or local controller.

2.4.6.5.4.1 Solenoid

The actuating solenoid for the mortise locks furnished must not dissipate more than 12 Watts and operate on [12] [24] VDC. The inrush current must not exceed 1 ampere and the holding current must not be greater than 500 milli-amperes. The actuating solenoid must move from the fully secure to fully open positions in not more than 500 milliseconds.

2.4.6.5.4.2 Signal Switches

The mortise locks are to include signal switches indicating to the system when the locks are not engaged. The signal switches are to report a forced entry to the system.

2.4.6.5.4.3 Power Transfer

Provide an electric power transfer with each mortise lock to get power and monitoring signals from the lockset to the door frame.

2.4.6.5.4.4 Size and Weight

Electrified mortise locks are to be compatible with standard door preparations.

2.4.6.5.4.5 Mounting Method

Provide electrified mortise locks suitable for use with single and double door installations. The lock would be in the active leaf and the fixed leaf would be monitored in double door installations.

2.4.6.5.5 Electromagnetic Lock

Electromagnetic locks are to contain no moving parts and depend solely upon electromagnetism to secure a portal by generating at least 5.3 kN 1200 pounds of holding force. Interface the lock with the local processors without external, internal, or functional local processor alteration. Incorporate an end-of-line resistor to facilitate line supervision by the system. Install MOVs to protect the controller from

reverse current surges if not incorporated into the electromagnetic lock or local controller. Provide in accordance with ANSI/BHMA A156.23.

2.4.6.5.5.1 Armature

The electromagnetic lock is to contain internal circuitry to eliminate residual magnetism and inductive kickback. The actuating armature must operate on [12] [24] VDC and not dissipate more than 12 Watts. The holding current must be not greater than 500 milli-amperes. The actuating armature must take not more than 300 milli-seconds to change the status of the lock from fully secure to fully open or fully open to fully secure.

2.4.6.5.5.2 Tamper Resistance

The electromagnetic lock mechanism is to be encased in hardened guard barriers to deter forced entry.

2.4.6.5.5.3 Mounting Method

Provide electromagnetic lock suitable for use with single and double door installations with [mortise-] [rim-] type hardware as indicated, and compatible with right- or left-hand mounting.

2.4.6.5.6 Entry Booth

****

NOTE: The designer will choose either keypads or card readers as needed. The outside dimensions of the entry booth will not exceed the site limitations required for the proper installation and functionality of the booth.

If a project requirement, the entry booth must have the capability to be used for egress.

****

a. Entry booths are to be constructed as an integral part of the physical structure of the boundary for the area or facility to which entry is being controlled. The entry booth is to automatically lock the high security side door's [electric strike and bolt] [electrified mortise lock] [electromagnetic lock] or other facility interface release device and automatically open the low security side door's electric strike or other facility interface release device in case of power failure.

b. Connect entry booths to the SCC and include a local processor. The entry booth local processor subsystem is to support paired card readers on a single entry booth for anti-pass back functions.

[c. Provide the entry booth with egress capabilities.

]2.4.6.5.6.1 Local Alarm Annunciation

Provide local alarm annunciation for all system equipment located within the entry booth itself and its associated portals or zones and terminal devices and a means to enable and disable this feature from the SCC under operator control.

2.4.6.5.6.2 Terminal and Facility Interface Device Support

The entry booth local processor subsystem is to support the full range of system terminal and facility interface devices as specified.

2.4.6.5.6.3 Response Times

The entry booth local processor subsystem must respond to a SCC interrogation within 100 milliseconds. The entry booth local processor is to respond to valid passage requests from its associated terminal devices by generating a signal to the appropriate [electric strike and bolt] [electrified mortise lock] [electromagnetic lock] within 100 milliseconds after verification.

2.4.6.5.6.4 Autonomous Local Control

In the event of a communication loss, the entry booth local processor subsystem must automatically convert to autonomous local control and monitoring of its associated card readers, keypads, [electric strike and bolt] [electrified mortise lock] [electromagnetic lock] and automatically revert to central control upon communication restoration. Transactions occurring during the communications outage are to be recorded and retained in local memory and reported to the central database files upon communication restoration within 10 seconds.

2.4.6.5.6.5 Entry Booth Local Processor Subsystem Capacities

As a minimum, the entry booth local processor subsystem is to have sufficient capacity to control and monitor a combination of 6:

a. Card readers

b. Keypads

[c. Electric strikes and bolts

][d. Electrified mortise lock

][e. Electromagnetic lock

] All entry control identification decisions and controls are to be performed by the local processor subsystem. The entry booth local processor subsystem must provide a local transaction history file with capacity to store at least 1000 entry control transactions without losing any data.

2.4.6.5.6.6 Diagnostics

Provide built-in diagnostics implemented in software, firmware, or hardware. The booth is to automatically execute a series of built-in tests and report equipment malfunctions, configuration errors, and inaccuracies to the SCC each time the entry booth local processor subsystem is started up or re-booted. The system must annunciate a fail-safe alarm if the local processor fails the built-in diagnostics. Provide diagnostic aids within the entry booth local processor subsystem to aid in system set-up, maintenance, and troubleshooting.

2.4.6.5.6.7 Memory Type and Size

Data entered is to be stored for a minimum of 1 year in the absence of power from external source to the entry booth.

2.4.6.5.6.8 Tamper Protection

The local processor subsystem is to monitor all service entry panels for tamper. Tamper lines must not be accessible except through tamper protected entry panels. Provide entry panels with key locks. Provide the capability to take the booth off-line for service.

2.4.6.5.6.9 Entry Booth Configuration

Provide a closed-in structures suitable for occupancy by 1 person with a personnel passage area, equipment storage, a low security entry or exit door and a high security entry or exit door. Configure with paired [card readers] [keypads], 1 each, on the high security entry or exit door and low security entry or exit door; a key release switch outside the low security door; a glass break type emergency release switch. Both doors to the entry booth are to be normally secured.

2.4.6.5.6.10 Entry Booth Operation

a. Configure to allow passage requests to be initiated from only 1 door at a time. During emergency situations both doors must have the capability to able to be opened at the same time. The person is to be allowed entry to the booth by presenting valid credential card to the card reader or keypad identification code data to the keypad device. An unsuccessful attempt to enter the booth are to generate an entry denial alarm.

b. Incorporate a personal identity verification device as specified and grant the person egress from the booth after successful personal identity verification. The entry booth is to confine the person and generate an entry control alarm if the person fails the personal identity verification test. The local processor is to grant the person's passage request if all provided data is valid.

c. The person is to be confined if a tamper alarm is generated by any of the equipment associated with the subject entry booth while a person is inside. Operating the glass break type emergency release switch is to command the entry door [electric strike and bolt] [electrified mortise lock] [electromagnetic lock] release to the fully open position or with a delay after the egress door has been confirmed secured. The person may exit through the door used for entry once inside the entry booth and prior to personal identity verification test initiation.

2.4.6.5.6.11 Display Type

Include an LED or other type of visual indicator display and provide visual status indications and person prompts. The display is to indicate power on/off, and whether enrollee passage requests have been accepted or rejected. Provide 3 status lights outside each door indicating entry booth status by marking:

a. Green light indicates READY

b. Amber light indicates BUSY

c. Red light indicates INOPERATIVE

2.4.6.5.6.12 Lighting

Provide lights recessed above an acrylic light diffuser in the ceiling of the entry booth. Provide a separate light source within the overhead lighting fixture assembly to provide emergency lighting in case of a power failure.

2.4.6.5.6.13 Heating and Ventilation Equipment

Include built-in heating and cooling equipment to sustain the specific operating temperature range for the electronic equipment installed.

2.4.6.5.6.14 Entry Booth Wall and Frame Construction

Provide a rigid structure with the strength of the walls greater than or equal to 12-gauge steel with 25 mm 1 inch standing seams. All glass is to be at least 8 mm 5/16 inch laminated, annealed glass and meeting UL 972 certification requirements. The entry booth must meet flame spread rating 25 or less, fuel contribution of 50 or less, smoke development of 50 or less, in accordance with test method ASTM E84.

Provide entry booths constructed to minimize the heating effects of solar radiation, by using the manufacturer's standard clear, tinted, or bronzed glass with over-hanging roofs or other structural means to shade the windows.

2.4.6.5.6.15 Entry Booth Doors

Doors must be at least 889 mm wide, by 2.0 m high 35 inches wide, by 79 inches high with glass panels at least 788 mm wide, by 1.9 m high 31 inches wide, by 74 inches high. Provide door hinges and closers with adjustments for vertical, horizontal, and torque. Provide an inside push bar, and an outside mechanical pull handle. Aluminum parts are to be anodized finish.

2.4.6.5.6.16 Entry Booth Floor Construction

Provide entry booth with a rigid floor covered by a rubber mat or indoor or outdoor carpeting. The rubber mat or carpet must be at least 1.6 mm 1/16 inch thick and provide a continuous floor covering without seams.

2.4.6.5.6.17 Electrical Requirements

****

NOTE: The designer will specify whether the electric strike or lock will fail open, fail secure, or other configuration (such as fail secure for entry into higher security area, while failing open for egress from the area). The designer must coordinate this with requirements of the site safety and fire personnel. Life safety will be designed in accordance with NFPA 101, Life Safety Code.

****

The entry booth, including associated terminal and facility interface and

other type of devices housed within the entry booth must not dissipate more than 1500 Watts. Provide booth with an integral battery back-up system. The battery back-up system must power the entry control devices and [electric strike and bolt] [electrified mortise lock] [electromagnetic lock] for at least 30 minutes. The doors to the booth are to be [secured] [opened], and the booth must go into an inoperative status if AC power is not restored to the booth within 30 minutes. Upon AC power restoration, the booth is to upload all entry transactions from the local processor subsystem to the SCC.

****

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

****

2.4.6.5.6.18 VSS Camera

Design and configure the VSS camera for continuous operation and transmit video information to the [SCC] [and] [local video recorder] as specified and designed.

2.4.6.5.6.19 Weight Check Monitor

Provide a weight check monitor which continuously monitors the weight of the booth plus any occupant. The weight check monitor is to consist of synchronized, matched, electronic load cells located at the base of the entry booth and be connected to the local processor subsystem. The weight check monitor must be accurate to within plus or minus 2.3 kg 5 pounds. Configure the entry booth to compensate for side loading to prevent damage to the load cells by the passage of equipment through the booth. Include individual weights for each user in the reference database files as part of the enrollment process. Provide a method to enter a custom, predefined tolerance on valid weights of authorized persons.

Automatically update each person's weight profile based upon the last three uses of entry control booths. Generate an entry control alarm for any passage attempt for which the person's weight does not agree with system reference database file data and confine the person. The weight check monitor is not to increase the portal door threshold height by more than 6 mm 1/4 inch.

2.4.6.5.6.20 Double Occupancy Sensor

Incorporate a sensor connected to the local processor subsystem which monitors the entire occupant area to detect attempts at double occupancy. A double occupancy sensor activation is to generate a system alarm and confine the enrollees.

2.4.6.5.6.21 Intercom

Provide three combination speaker and microphones to provide 2-way communications at each speaker and microphone location. The speakers must be at least 100 mm 4 inches in diameter. Locate two of the speakers and microphones at the high and low security entry or exit doors, behind louvered panels, to provide communications for people outside the booth. The third speaker and microphone are to be located inside the booth behind a perforated metal screen above the personal identity verification device to provide communications for people inside the booth. Connect each of

the speakers and microphones to the operator console at the SCC and to the voice prompt system as indicated.

2.4.6.5.6.22 Voice Prompts

Include a voice prompt system using human voice commands to speed up the entry control process and improve throughput rate. This audible prompt system is to respond to the next sequential activity requirement as each employee accesses the booth. All commands are to be stored in electrically programmable read only memory chips located in the local processor subsystem. The voice prompts are to only be directed to the speaker and microphone nearest the employee. Use the voice prompts only if the employee does not perform the next step in the entry booth entry control process within a 5 second time window. The SCC must be able to enable and disable of voice prompts and adjustment of the time window under operator control.

[2.4.6.5.7 Vehicle Gate Operator

Provide vehicle gate operators suitable for connection to, monitoring, and control by the system's local processors and include all additional equipment and wiring to be an operable system. Provide a hand crank for the manual vehicle gate operator and a solenoid actuated brake operation to prevent gate coasting.

Provide an auto reverse time delay of at least 1 second and not more than 3 seconds to minimize shock loads on vehicle gate operator drive components. Include a contactor type motor starter that is appropriate for the gate operator motor.

2.4.6.5.7.1 Input Power

Provide vehicle gate operator that operates from the voltage source as shown on the drawings. Include manual reset type thermal and electrical overload devices.

2.4.6.5.7.2 Audible Warning

Provide an audible warning system to signal personnel in the vicinity of the vehicle gate operator that an opening or closing is about to commence. The audible warning must sound at least 2 seconds and no more than 5 seconds before movement begins.

2.4.6.5.7.3 Maximum Run Timer

The vehicle gate operator must incorporate an internal maximum run timer which limits the motor run time. The maximum run time is to be operator adjustable for at least the maximum amount of time gate opening or closing takes during normal operation.

2.4.6.5.7.4 Adjustable Load Monitor for Obstruction Sensing

Provide operator adjustable load monitor that senses obstructions in the path of the gate and automatically reverses the vehicle gate operator drive motor. Do not allow the gate to open once the gate has reached the limit switch.

2.4.6.5.7.5 Operator Override Controls

Provide the vehicle gate operator with an interface to a three pushbutton control station located within an entry-controlled area. The three pushbutton switches are to be labeled and function as Open, Close, and Stop controls, and meet the requirements of paragraph PUSH-BUTTON SWITCHES.

2.4.6.5.7.6 Limit Switches

Provide adjustable limit switches to define the range of gate travel and provide a means to securely lock the switches in place after adjustment.

2.4.6.5.7.7 Type of Gate

Provide the vehicle gate operators to be compatible with cantilever, roller, v-track, overhead, slide, and swing gates.

2.4.6.5.7.8 Safety

Provide safety compatible with paragraph TYPE OF GATE for entrapment protection.

]2.4.6.6 Active Barrier Interface

Provide active barrier interface in accordance with Section 34 75 13.13 CRASH RATED ACTIVE VEHICLE BARRIERS AND CONTROLS suitable for connection to, monitoring, and control by the system's local processors and include all additional equipment and wiring to be an operable system.

2.4.7 Elevator Control

****

NOTE: The designer will determine if floor tracking is appropriate for the site, see item b below.

If the ESS design includes Medical Facilities the elevator control must interface with Infant Protection Alarm System (IPAS).

****

2.4.7.1 Control Elevator Operation with Entry Control Terminal Devices

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

2.4.7.2 Floor Tracking

Deploy the elevator control system in such a manner as to provide "floor tracking" reports where the system records the individual's floor selection when elevator control is in effect.

2.4.8 Access Control System Date and Time

Provide system date and time per paragraph DATE AND TIME GENERATOR.

2.5 VIDEO SURVEILLANCE SYSTEM (VSS)

****

NOTE: Scene illumination must be even across the field of view of the camera, with a maximum light to dark ratio of 8 to 1.

For visual assessment of alarms use a minimum of two monitors. 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 16 cameras or less, use one monitor.

****

Select system components that conform to the Open Network Video Interface Forum (ONVIF) specification. Provide compatible [UL 62368-1] [and] [UL 2802] listed VSS components to provide visual assessment of ESS alarms automatically upon alarm or upon SCC operator selection. Otherwise, the subsystem is to continuously display the coverage area. Display alphanumeric camera location ID on all monitors. Provide the number of alarm monitors as required. The scene from each camera must appear clear, crisp, and stable on the respective monitor during both daytime and nighttime operation. Provide component equipment that minimizes both preventive and corrective maintenance. Provide components from a single manufacturer or justify mixing manufacturer components and demonstrate compatibility in submittal information.

2.5.1 Cameras

2.5.1.1 VSS Camera

Provide Internet Protocol (IP) cameras of fixed, pan-tilt-zoom (PTZ), or panoramic type as indicated on the drawings.

a. Day-Night [Color] [B&W] fixed, PTZ or panoramic cameras are to be used in all outdoor environments. Standard fixed, PTZ, or panoramic cameras are to be used for all indoor applications except when backlighting issues are observed. Use Day-Night cameras or standard cameras with backlighting compensation for backlighting or high contrast applications.

b. Provide PTZ cameras with a direct drive motor assembly. Belt driven PTZ camera units are not acceptable. Equip PTZ cameras with a slip ring assembly having an optical interface and be rated for continuous duty. PTZ cameras must be fully integrated units. The pan-tilt mechanism must be an integral part of the camera. The PTZ control system from the [joystick] [and] [mouse] to the camera to the viewed image must operate in real-time with no impact to operational accuracy of pan tile zoom function.

c. Provide cameras that operate over a voltage range of [12 VDC] [24 VDC] [12] [24] VAC at [50] [60] Hz Power over Ethernet (PoE) IEEE 802.3.

d. All cameras must be constructed to provide rigid support for electrical and optical systems so that unintentional changes in alignment or microphonic effects do not occur during operation, movement, or lens adjustments.

e. Video Frame Rate: [30] [60] [120] frames per second (fps)

f. Cameras without on-board SD card recording may be used.

g. Cameras with on-board SD card recording must be addressed in the system programming regarding the use of SD card recording. Network outages must be addressed regarding the upload procedure for the SD card data. Audio recording (if used) must be addressed also, including proper signage per all applicable laws.

2.5.1.1.1 Sensitivity

Minimum Illumination: 0.7 lux 0.07 foot-candles at F1.4 color mode; 0.09 lux 0.009 foot-candles at F1.4 in the B&W mode.

2.5.1.1.2 Signal-To-Noise Ratio

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

2.5.1.1.3 Resolution

Provide a minimum of [2.1] [_____] megapixel resolution. The imager must have a minimum of 1080P picture in progressive scan format. Resolution is to be maintained over the specified input voltage and frequency range, and not vary from minimum specification over the specified operating temperature range.

2.5.1.1.4 Synchronization

Provide cameras that have internal and line lock.

2.5.1.1.5 Low Light Level

Provide Day-Night cameras that have a B-W mode that may be automatically engaged on low light level and permit the use of integrated or external infrared illuminator. Electronic removal of the color signal is not acceptable. The camera must have an infrared cut filter capable of being removed automatically upon low light threshold or manually.

2.5.1.2 Camera Lenses

****

NOTE: The designer will provide drawings of the lens field of view labeled with the correct lens focal length for each camera, or a table that references the camera location and the required lens focal length in order to support this paragraph.

****

Camera lenses are to be all glass with coated optics. Provide lens mount that is [C or CS mount], [compatible with the cameras selected] [integrated with the cameras]. Provide lens with the camera that have a maximum f-stop opening of f/1.2 or the maximum available for the focal length specified. The lens is to have an auto-iris mechanism unless otherwise specified. Lenses having auto iris, manual iris, or zoom and focus functions are to be supplied with connectors, wiring, receiver and driver units, and controls as needed to operate the lens functions. Provide lenses with sufficient circle of illumination to cover the image

sensor evenly. Lenses are not to be used on a camera with an image format larger than the lens is configured to cover. Provide lens with focal lengths as indicated or specified in the manufacturer's lens selection tables.

2.5.1.3 Camera Housing and Mounts

The camera and lens are to be enclosed in a tamper resistant housing installed on a camera support. Any ancillary housing mounting hardware needed to install the housing at the camera location is to be provided as part of the housing. The camera support must be capable of supporting the mounted equipment and withstanding wind and ice loads normally encountered at the site.

2.5.1.3.1 Environmentally Sealed Camera Housing

The housing is to provide an environment needed for camera operation and be condensation free; dust and watertight; keep the viewing window free of fog, snow, and ice, and be fully operational in 100 percent condensing humidity. Provide housing equipped with a sunshield. Both the housing and sunshield are to be white in color. Housing must be purged of atmospheric air and pressurized with dry nitrogen, equipped with a fill valve, overpressure valve, and include a humidity indicator visible from the exterior. Housing must not have a leak rate greater than 13.8 kPa 2 psi at sea level within a 90 day period. Housing must resist influx of rain or snow from vertical to wind driven horizontal directions.

Provide housing equipped with supplementary camera mounting blocks or supports needed to position the camera and lens to maintain the proper optical centerline. All electrical and signal connections required for camera and lens operation are to be supplied. Provide a mounting bracket as part of the housing which allows weight adjustment to center the weight of the assembly.

2.5.1.3.2 Indoor Camera Housing

Provide housing with a tamper resistant enclosure for indoor camera operation and with the proper mounting brackets for the specified camera and lens. The housing and appurtenances color are not to conflict with the building interior color scheme.

2.5.1.3.3 Interior Mount

Provide camera mount suitable for either wall or ceiling mounting and have an adjustable head for mounting the camera. The wall mount and head must be constructed of aluminum or steel with a corrosion-resistant finish. Provide adjustable head with 360 degrees of pan and plus or minus 90 degrees of tilt.

2.5.1.3.4 Low Profile Ceiling Mount

Provide tamperproof ceiling housing which is low profile and suitable for use in 610 by 610 mm 2- by 2-foot ceiling tiles. The housing must be equipped with a camera mounting bracket and allows a 360-degree viewing setup.

2.5.1.3.5 Interior Dome Housing

The dome housing is to be capable of being mounted by pendant, pole,

ceiling, surface, or corner as shown on the drawings. The lower dome is to be black opaque acrylic and have a light attenuation factor of not more than 1 f-stop. Provide housing with:

a. Integral pan-tilt complete with wiring

b. Wiring harnesses

c. Connectors

[d. Receiver-driver

][e. Pan-tilt control system

][f. Pre-position cards

][g. Heavy duty bearings

][h. Hardened steel gears

] i. Permanent lubrication

j. Motors that are thermally or impedance protected against overload damage.

k. Any other hardware and equipment as needed to provide a fully functional pan-tilt dome. Provide pan movement of 360 degrees and tilt movement of at least plus or minus 90 degrees. Pan speed must be at least 20 degrees per second and tilt speed be at least 10 degrees per second.

2.5.1.3.6 Exterior Dome Housing

Provide dome housing capable of being mounted by pendant, pole, ceiling, surface, or corner as shown on the drawings and constructed to be dust and watertight, and fully operational in 100 percent condensing humidity. Purge the housing of atmospheric air and pressurize with dry nitrogen. Provide a fill valve and overpressure valve with a pressure indicator visible from the exterior. The housing is to be equipped with supplementary camera mounting blocks or supports as needed to position the specified camera and lens to maintain the proper optical centerline.

Provide all electrical and signal connections required for camera and lens operation. The housing is to provide the environment needed for camera operation. The lower dome is to be black opaque acrylic with a light attenuation factor of not more than 1 f-stop. Provide housing with:

a. Integral pan-tilt complete with wiring

b. Wiring harnesses

c. Connectors

[d. Receiver-driver

][e. Pan-tilt control system

][f. Pre-position cards

][g. Heavy duty bearings

][h. Hardened steel gears

] i. Permanent lubrication

j. Motors that are thermally or impedance protected against overload damage.

k. Any other hardware and equipment as needed to provide a fully functional pan-tilt dome. Provide pan movement of 360 degrees and tilt movement of at least plus or minus 90 degrees. Pan speed must be at least 20 degrees per second and tilt speed be at least 10 degrees per second.

2.5.1.3.7 Exterior Wall Mount

Provide exterior camera wall mount that is [406.4] [609.6] [914.4] [_____] mm [16] [24] [36] [_____] inches long and has an adjustable head for mounting the camera. The wall mount and head must be constructed of aluminum, stainless steel, or steel with a corrosion-resistant finish. Provide adjustable head for at least plus and minus 90 degrees of pan, and at least plus and minus 45 degrees of tilt. If to be used in conjunction with a pan-tilt, provide bracket without the adjustable mounting head, and a bolt hole pattern to match the pan-tilt base. Wind speeds up to [27] [ ] m/s [60] [_____] mph must not change alignment of the camera nor affect the PTZ operation.

2.5.1.3.8 Pan-Tilt Mount

a. Provide pan-tilt mount capable of supporting the camera, lens, and housing specified that is weatherproof and sized to accommodate the camera, lens and housing weight plus maximum wind loading encountered at the installation site if the pan-tilt is to be mounted outdoors. Provide pan-tilt with:

(1) Heavy duty bearings

(2) Hardened steel gears

(3) Externally adjustable limit stops for pan and tilt

(4) Mechanical, dynamic, or friction brakes

(5) Permanent lubrication

(6) Motors that are thermally or impedance protected against overload damage.

b. Provide pan movement of 360 degrees pan rotation, a minimum tilt movement of plus and minus 90 degrees. Manual pan speed must be a minimum of [0 to 80 degrees per second] [_____], and a minimum tilt speed of [10 degrees per second] [_____]. A minimum automatic pan speed of [280 degree per second] [_____] and tilt speed of [160 degree per second] [_____].

c. The pan-tilt is to be supplied complete with wiring, wiring harnesses, connectors, receiver-driver, pan-tilt control system, pre-position cards, or any other hardware and equipment as needed to provide a

fully functional pan-tilt mount to fulfill the site design requirements.

2.5.1.3.9 Explosion Proof Housing

The explosion proof housing must meet the requirements in paragraph COMPONENT ENCLOSURE for hazardous locations, see paragraph HAZARDOUS LOCATIONS. Configure housing to provide a tamper resistant enclosure and supply with the proper mounting brackets for the specified camera and lens.

2.5.2 Thermal Imaging System

IP Thermal Cameras

a. Provide an integrated thermal imaging device in an environmental enclosure.

b. Provide a native digital image from the image sensor to the IP video stream.

c. Provide of an uncooled, sun-safe amorphous silicon micro bolometer, long-wavelength infrared (LWIR) camera capable of 640 x 480 and 384 x 288 resolution formats.

d. Provide a temporal Noise Equivalent Temperature Difference (NETD) below 50mK at f/1.0 capable of multiple display formats including white hot, black hot, and rainbow.

e. Allow for input voltage of [24 VAC], [24 VDC], [or] [a selectable power source of [120] [230] VAC].

f. Provide a built-in heater and defroster and sun shroud in accordance with paragraph COMPONENT ENCLOSURE.

g. Support two simultaneous, configurable video streams. MJPEG and H.264 compression formats that are available for primary and secondary streams with selectable Unicast and Multicast protocols. The streams are to be configurable in a variety of frame rates, bit rates, and group of pictures (GOP) structures.

h. Use a standard Web browser interface for remote administration and camera parameter configurations.

i. Provide a [100Base-TX] [_____] network port for live streaming to a standard Web browser.

j. Provide built-in video analytics.

2.5.3 Video Analytics (VA)

2.5.3.1 Software

Provide capability range from basic activity detection to the search through databases to pre-empt serious incidents. The VA is to provide graphic identified movement identification, user-selectable monitored areas, compensation for environmental movement, and other features specified when provided as a capability of the NVR. Provide the following features:

2.5.3.1.1 Basic Motion Detection

a. Adaptive Motion

b. Abandoned Object

c. Object Removal

d. Camera Sabotage

e. Directional Motion

f. Object Counting

g. Loitering Detection

h. Stopped Vehicle

2.5.3.1.2 Advanced VA

2.5.3.1.2.1 Intruder Identification

This refers to identifying unauthorized humans in specified areas within the field of view.

2.5.3.1.2.2 Environmental Compensation

Recognizing and ignoring wind-blown debris, animals, background traffic, and so on.

2.5.3.1.2.3 Counting

This refers to recognizing a quantity of a particular object moving or activity performed.

2.5.3.1.2.4 Directional Identification

This refers to the ability to ignore objects moving in one direction, while alarming for objects moving in unauthorized directions.

2.5.3.1.2.5 Item Recognition

This refers to activation when specific user-selected items are removed from, placed in, or passed through the field of view.

2.5.3.1.2.6 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.

2.5.3.1.2.7 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.

2.5.3.1.2.8 Object Left Behind

This refers to the ability to detect objects left behind or added within

the field of view in a scene.

2.5.3.2 Embedded VA

2.5.3.2.1 Intelligent Video Analysis

a. Provide camera capable of processing and analyzing video within the camera itself, with no extra hardware required.

b. The camera is to be capable of detecting and sending alarms for abnormal events.

c. The camera is to be configurable to analyze up to 10 different scenes for one or more of the following events:

(1) Line Crossing

(2) Loitering

(3) Idle Object

(4) Removed Object

(5) Conditional Change

(6) Trajectory Tracking

(7) Filters

d. The camera is to allow users to set up to 10 separate profiles and switch profiles based on a day, night, or holiday schedule.

e. The camera is to support scene tours that automatically reposition the camera to each scene for a specified duration.

f. The camera is to incorporate an Alarm Rule Engine, enabling abnormal events that VA detects to prompt the camera to take one or more actions:

(1) Trigger a relay connected to an alarm siren, strobe, or both.

(2) Trigger a visual alert to be displayed on the operator's screen.

(3) Go to a specified scene (preset position).

g. Camera must provide [100] [_____] horizontal and [80] [_____] vertical pixels per foot at desired distance for License Plate Recognition. Camera must also provide [24] [_____] frames per second for License Plate Recognition.

2.5.3.2.2 Motion Tracking with PTZ Cameras

a. The camera is to offer Intelligent Tracking to continuously track an object using pan, tilt, and zoom actions.

b. The camera is to provide automatic motion tracking using intelligent video analytics.

c. Provide camera with the ability to follow an object continually when

passing behind a privacy mask.

d. Provide camera with the ability to restart tracking if a target starts moving in the same area where the initial target stopped moving or if the camera detects an object moving along the last known trajectory.

e. The camera is to allow an operator to select an object to track in the live image view.

2.5.4 Color Computer Monitors

****
NOTE: Certain display unit types may not be acceptable for use by the Activity. Verify with the SSO/CTTA for your project for acceptable formats.
****

Except as specified, provide computer monitors that:

a. Are rated for continuous operation.

b. LED flat panel computer monitor with [HDMI] [and] [DP] [USB-C] [DVI] input.

c. Have a [16:9][16:10] aspect ratio nominally measures [685][1066][1397][1651][_____] mm [27][42][55][65][_____] inches for LED displays.

2.5.4.1 Mounting

a. Mount monitors with compatible wall mount or manufacturer provided desk top stand.

2.5.4.2 Video and Signal Input

****
NOTE: Certain display input types may not be acceptable for use by the Activity. Verify with the SSO/CTTA for your project for acceptable formats.
****

Monitors are to operate with video input requiring a one [HDMI] [DVI-D] [DP] [USB-C] switchable to either loop-through or internal 75-ohm terminating impedance.

Signal input connectors must be [HDMI] [DVI-D] [DP] [USB-C] type.

2.5.5 Ancillary Equipment

Equipment is to consist of the items specified below:

2.5.5.1 Video System Date and Time

Provide system date and time per paragraph DATE AND TIME GENERATOR and paragraph VIDEO RECORDING PERFORMANCE.

2.5.5.2 Camera Identifiers

Label video signal from each camera using alphanumeric identifiers.

Camera alphanumeric identifiers may originate from either the camera or the video recorder.

2.5.5.3 Video Recording

2.5.5.3.1 Analog to IP Video Converter

For new construction projects or new installation of new cameras on an existing site analog cameras are not allowed. For existing analog cameras that must remain in service, provide an analog (base band video) to IP converter to allow the camera images to be recorded in the IP based system.

2.5.5.3.2 IP Based Video Recording Device/System

a. Provide video recording device/system with an integral video management software (VMS). Dedicated VSS monitors and authorized computers networked to the video recording device/system are to be capable of viewing recorded and live video from the network. The video recording device/system is to be able to record and transmit video with minimum 24 fps at maximum camera resolution. The video recording device/system is to network with and utilize smaller, non-server computers at off-site camera locations as local recorders.

b. Provide video recording device/system with the capability to de-warp live and recorded images.

c. The storage memory capacity of the video recording device/system is to be sufficient to store a minimum of [7] [14] [30] [_____] days of video at [3] [6] [9] [15] [_____] fps, [2.1] [_____] megapixel resolution and be expandable for an increased capacity of [_____] [GB] [TB] and be capable of including Redundant Array of Independent Disc (RAID) arrays [0] [1] [5] [6] [10] [_____].

d. The video recording device/system must have the capacity to address and process up to [8] [16] [24] [32] [64] [128] [256] [512] [_____] dual-streaming cameras. The video recording device/system must record all cameras onto a hard drive and allow remote network viewing via [internet] [intranet] browser. Hard drive capability must be sized to store all cameras recording 24 hours a day 7 days a week at [3] [6] [9] [15] [_____] frames per second per camera for [1] [2] [4] [ ] weeks.

2.5.5.3.3 Video Recording Performance

The video recording performance is to be as follows:

a. The NVR [video server] is to use modular hard disk media, with a digital format capacity of [2TB] [_____] per module.

b. Provide a [1000Base-T] [_____] connection for record review and camera view and control that is compatible for a PC workstation equipped with latest [Microsoft Windows [_____] Professional operating system software], [Internet Browser Software].

c. PC workstation Viewing: Include direct access from the ESS PC workstations to each NVR [video server] via a internet web browser. All necessary descriptive bookmarks and shortcuts are to be prepared on each PC workstation to allow this direct access. All functions are to be accessible through HTML commands from a user's web browser

interface. Pictures are to be available for attachment via a user-provided SMTP-based e-mail transport system and included capability for 16 users and 3 user access levels (admin, control and user).

d. Include sampling at 720(H) by 480(V) and 320(H) by 240(V) (Pixel Memory) with [_____] frames per second and 3-D scan conversion to enable jitter-free stabilized pictures in a single frame. Modes include:

(1) Emergency

(2) Event

(3) Schedule

(4) Manual Recording

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

f. Provide system date and time per paragraph DATE AND TIME GENERATOR. System Date and time to be digitally displayed on the monitor and also clearly shown on digitally stored recordings. The following information is to be included as part of the date and time stamps:

(1) Year

(2) Month

(3) Day

(4) Hour

(5) Minute

(6) Second

(7) Alphanumeric camera location ID up to 8 characters. The NVR [video server] is to feature video loss detection on all channels.

g. Pre-event recording: Pre-event recording should match the configuration in software to record [0.50 second] [1 minute] [3 minutes] or [_____ minutes] pre-event.

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

i. Disk Partitioning: Provide within the NVR [video server]an automated disk management and a RTOS (real-time operating system) platform to

include a minimum of [4.8] [_____] TB of digital video storage on a single partition.

The video recording system is to provide a choice of Physical Partitioning as RAID [0] [1] [5] [6] [10] [_____] to provide a redundant array of independent discs to increase performance and redundancy. Raid levels should be coordinated with user requirements. Allow the operator to be able to partition the available recording areas in a Virtual Partition by Regular, Event, and Copy Partitions. Manually and scheduled recorded video information is to be assigned to a Regular Recording Partition, which may be overwritten. Event and Emergency Recording Data is to be assignable to an Event Partition, where image overwriting is be prohibited. Any copied data is to be able to be assigned to the Copy Partition, which may be overwritten or saved as required.

j. Playback: 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).

k. Multiplexer Functions: Include an integral, software based IP switching capability that automatically switches multiple camera images to enable sequential spot monitoring and simultaneous field recording. The unit must have full screen, [4] [7] [9] [10] [13] [16] multiscreen monitoring modes.

l. Outputs

(1) Provide via HDMI female connections [4] [9] [16] [_____] outputs for all video source connections to external monitoring systems including multiscreen and spot monitor video outputs.

(2) Provide virtual camera number programming capability to support [64] [128] [256] [512] [_____] camera channels on a single system.

m. All camera selection buttons are to have Tri-State Indication, corresponding to Recording, Viewing and Control functions in the NVR [video server] software. Furnish the following indicators:

(1) Alarm

(2) Alarm Suspend

(3) Operate

(4) HDD1, Hard drive identifier

(5) Timer and Error indicators

(6) Camera Selection

(7) Iris

(8) Preset

(9) Camera Automatic Mode

(10) Pan-Tilt

(11) Set

(12) Jog Dial

(13) Shuttle Dial

(14) Setup-Esc

(15) Record

(16) Search

(17) Play-Pause

(18) Pan-Tilt Slow

(19) Stop

(20) Pan-Tilt Go to Last

(21) Zoom-Focus

(22) A-B

(23) Repeat

(24) Shift

(25) Alarm Reset Buttons

n. Networking: All NVR [video server] recording, review, playback, camera control and setup are to be available via the internally mounted Network Interface. A [1000Base-T] [_____] connection for record review and camera view and control will be required on a personal computer equipped with Internet Browser Software and an Ethernet 1000Base-T connection. 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). Support a minimum of [8] [_____] simultaneous clients viewing and [2] [ ] simultaneous FTP sessions.

o. Power: The video recording equipment must have a power source of [120] [230] VAC at [50] [60] Hz.

2.5.5.3.4 Recording Audio With Video

Recording audio with video is acceptable provided all applicable laws are followed. Audio recording is not allowed under any circumstances in certain areas per the law, and if allowed often has strict signage requirements.

2.5.5.4 Camera Control

Provide access to camera functions and real time control for all cameras via the video management software for 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 are to

be accessible via front panel controls or the optional system controller controls to be accomplished by [joystick] [mouse]. These functions are to include:

(1) Direct access of preset position

(2) Zoom (near/far)

(3) Focus (near/far)

(4) Iris (open/close)

(5) Pan (left/right)

2.5.6 Camera Mounting Structures

****

NOTE: Show footing details on drawings. For a camera pole, installation must meet the requirements as specified in Section 33 71 01 OVERHEAD TRANSMISSION AND DISTRIBUTION. For self-supporting towers, footings must be designed in accordance with UFC 3-301-01.

****

Provide camera mounting structures designed specifically for VSS cameras. The structure is to accommodate appropriate wiring pathways for power and communication as well as proper grounding and surge protection. Design loads for the camera mounting structure must conform to TIA-222 and all applicable addendums of the TIA standard. Allowable pole deflection is determined from the point of the camera mount and must not exceed 0.5 percent of the pole height under adjusted maximum wind load conditions. Adjusted maximum wind load conditions for deflection calculations must be 48 km per hour 30 miles per hour (mph) or 35 percent of the basic wind speed as determined by TIA-222, whichever is greater. Confirm compliance to TIA standards by structure manufacturer data or by analysis. Provide additional measures as required to stabilize the camera if placed in an environment that is subject to induced vibrations such as heavy winds or excessive traffic.

2.5.7 Video Surveillance System (VSS) Schedule

Provide a spreadsheet describing each individual camera installation location including the following items:

a. Unique camera location identifier.

b. Make/model/type (PTZ, fixed, fixed IR, etc.)/part-number of camera.

c. Make/model/part-number of camera mount.

d. Intended camera field of view.

e. Any additional information pertinent to that unique location.

2.6 SECURITY COMMAND CENTER (SCC)

****

NOTE: The specific size and speed of the computers

is directly related to the size and complexity of the installation along with the ESS software. The following minimum requirements are developed for IDS, ACS, and VSS workstations, enrollment center equipment (badging station), administrative workstation, and an Enterprise server.

****

The SCC must integrate all subsystems and communications and provide operator control interface to the ESS system. The components are as follows:

a. ESS Software

b. Monitoring Display Software

c. Graphical Map Software

d. Printers

e. Controls and Display Integration

f. Enrollment Center Equipment

2.6.1 ESS Software

a. Provide commercial off-the-shelf ESS software that utilizes a single database for the subsystem integrations provided under a single operating environment. The system is to archive all events in a database stored either on a local hard drive or a networked database server. The software has to support configuration and simultaneous monitoring of all subsystems.

b. Allow the networked PC workstation configurations connected via a TCP/IP network. Administrative tasks including configuration, monitoring, schedules, report generation and graphic display are provided from any PC workstation on the network. All system programming data must be instantly accessible to every PC Workstation connected to the network. The system is to utilize a non-proprietary SQL-based, ODBC-compliant database, managed by Sybase Adaptive Server Anywhere, Microsoft SQL Server, or Oracle.

c. Utilize a preemptive multi-tasking operating system, such as the latest Microsoft Windows [_____] Professional environment, that is multitasking, with many processes running at the same time without interference with each other and with higher priority tasks taking precedence over lower priority tasks.

d. Provide capabilities to define visual exclusion areas.

[e. Provide de-warping software for panoramic cameras.

]2.6.1.1 Alarm Call up

Support responses to alarms entering the system with each alarm capable of initiating one or more of the following actions:

a. Sending alarm commands to a VSS system interface

b. Triggering event recording

c. Activating output devices

d. Playing PC audio files

e. Controlling doors

f. Display graphical maps associated with the alarm device

Provide mode of system operation that requires an operator to acknowledge any alarm. While alarm is still active, the alarm cannot be cleared.

2.6.1.2 Programming

Provide the capability of, but not limited to, the following programming and functionality:

2.6.1.2.1 Daylight Savings Time Adjustment

The ACU(s) and PCU(s) must not need to be connected to the ESS in order for the adjustment to occur.

2.6.1.2.2 Operator Privileges

Support an unlimited number of system operators, each with a unique login and password combination. Operators are to be assigned privileges based on the loops, commands, or programmed features that are available to each individual operator.

2.6.1.2.3 Alarm Priorities

Provide the ability for each alarm device to be user configured to belong to one of [10,000] [_____] priority levels which are assigned to an alarm based on alarm importance. These priorities are to define which alarm events to display on individually specified ESS workstations.

2.6.1.2.4 Reports

Include integrated reporting capabilities as well as the ability to run [Crystal Report] [_____] templates.

2.6.1.2.5 User Interface

The ESS programming is to be menu-driven, with "wizards" to assist with software configuration, and include 'Help' information.

2.6.1.2.6 Messages

Permit the use of user-selected colors for event messages.

2.6.1.2.7 Graphics

Provide the capability to display a floor-plan graphic for card activity and alarm events as part of the ESS integration.

2.6.1.2.8 Device Status

Provide the capability to display the dynamic status of a user-selected

list of devices, including doors, inputs, and outputs.

2.6.1.2.9 Diagnostics

Include diagnostic software tools that interface and query the hardware for information and to issue commands.

2.6.1.2.10 Mandatory Data Fields

Require any cardholder data field to be selected by the user as mandatory.

2.6.1.2.11 User Defined Data Fields

Provide [20] [_____] unassigned data fields for storing user-defined data that support user-defined labels, and are user-configurable as plain text fields or drop-down selection lists.

2.6.1.2.12 Archive Database

Include a connection to an archive database which stores purged events and deleted programming which can be accessed for reporting.

2.6.1.2.13 Programmable Database Backup

Include the capability of performing user-scheduled database backups without the use of third-party backup software.

2.6.1.2.14 Programmable Database Purging

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.

2.6.1.2.15 Database Importing

Include the capacity to import user data from an ODBC data source (Access, Excel, text).

2.6.1.2.16 Data Exporting

Include the capacity to export data from any table in the database to either a [text] [HTML] [Excel] [Access] file in any user-selected order.

2.6.1.2.17 Event Log Output

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.

2.6.1.2.18 Data Audit Trail

Record changes to programming, recording the date and time stamp of the change, the name of the operator making the change, and the nature of the change. This data audit is to be available in history for reporting.

2.6.1.2.19 Alarm Forwarding

Provide the capability to forward alarms to cellular telephones via dedicated applications or text message to be utilized by authorized system personnel when they are away from the SCC.

2.6.2 ESS Monitor Display Software

ESS Monitor display software is to provide for text and graphic map displays that include zone and device status integrated into the display. Different colors are to be used for the various components and real time data. Colors must be uniform on all displays. Follow the color coding as follows.

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.

2.6.3 Graphical Interactive Map Software

a. ESS graphical map software is to show the [graphic and] visual data of all subsystem devices. Use a [480] [533][762] [1066] [_____] mm [19] [21] [30] [42] [_____] inches, LED flat screen display with messages displayed in the English language. Provide graphical maps showing a layout of all the protected facilities. Highlight zones corresponding to those monitored by the ESS on the graphical maps. Display status of each zone using graphical icons as required within each designated zone.

b. Provide capability for graphical maps to 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. Allow for [3] [6] [_____] layers of maps to be defined for any given ESS device. To speed an incident location, 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.

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

d. The status of intrusion devices, access control readers, doors, auxiliary monitor points, and auxiliary outputs is to be able to be requested from any map by simply selecting the icon representing the device and its current state will be displayed. VSS camera control, digital video review, alarm panel transactions and intercom requests are to be available for inclusion on the map with the associated management module installed.

e. Allow for SCC operators 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 is to cause the appropriate command options list to appear for selection. Confirmation is provided by reflecting the change in status on the display after a command is selected.

f. 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.

g. Create maps using standard office tools allowing drawings to be imported in Jpeg, Bitmap, Windows metafile, PDF or DXF file formats to provide maximum flexibility.

2.6.4 Printers

****
NOTE: A shared printer can be used for reports and alarms. If a project requirement includes the badge printer a separate badge printer is required.
****

2.6.4.1 Report Printer

Provide a laser text printer to generate reports that is a [USB] [wired network (RJ45)] interface dry-type laser process printer. Provide a printer with the capability of holding a minimum of 500 pages. The unit must print a minimum of 30 pages per minute at 600 dpi resolution.

2.6.4.2 Alarm Printer

Provide an alarm printer interconnected to the SCC equipment with a minimum print rate of 30 characters per second to produce hard copy of system events. Printer must meet requirements per paragraph REPORT PRINTER.

[2.6.4.3 Badge Printer

Provide a dye-sublimation or resin thermal transfer type image printer for Badge Identification credentials that is capable of printing two sides, edge to edge, directly onto a white-unfinished 0.030 PVC, PVH or PVCH card at a rate of approximately 80 seconds per card. [Provide an encoder to be an integral part of the printer with encoding conforming to ABA Track II and ANSI specifications].

]2.6.5 Control and Display Integration

Integrate human engineer SCC controls so the entire SCC can be operated by a single or multiple operator(s). Integrate switching and monitoring components of the assessment subsystem with the SCC so that SCC operator(s) can effectively monitor, assess alarms, and control the ESS. [Method of system integration must be as a single console. Provide chassis, and modules required for console SCC configuration.]

2.6.6 Enrollment Center Equipment

****
NOTE: The designer will calculate if 25 percent is adequate for future use. If it is not, the designer will specify the correct percentage.

SCIF and SAPF enrollment equipment must be inside the SCIF or SAPF areas.
****

Provide enrollment stations to enroll personnel into, and disenroll personnel from, the system database. The enrollment equipment is to only be accessible to authorized entry control enrollment personnel.[Provide a quantity of credential cards equal to or greater than the number of personnel to be enrolled at the site plus an extra [25] [_____] percent for future use.] The enrollment equipment is to include subsystem configuration controls and electronic diagnostic aids for subsystem setup and troubleshooting with the SCC. Provide a [CAC] [PIV] [proximity] card reader at the enrollment station.[Also provide a [fingerprint reader] [palm scanner] [facial scanner] and [keypad] at the enrollment station.][Provide a printer for the enrollment station which meets the requirements of paragraph REPORT PRINTER.]

2.6.6.1 Enrollment Client Accessories

a. Provide a steel desk-type console and equipment racks. The console is to be in accordance with ECIA EIA/ECA 310-E and as indicated.

b. Rack mount all equipment in the console and equipment racks, except for printer. Color coordinate the console and equipment racks and cabinets, obtaining approved by the Contracting Officer.

[c. Provide a locking cabinet approximately 1.8 m 6 feet high, 900 mm 3 feet wide, and 600 mm 2 feet deep with three adjustable shelves, and two storage racks for storage of CDs, DVDs, printouts, printer paper, ink/toner, manuals, and other documentation.

]2.6.6.2 Enrollment Center I.D. Production

a. Equip the enrollment client with a high-resolution digital camera structurally mounted or provided with a reliable tripod. The camera model is to be as recommended by the manufacturer of the ESS. Provide commercial off-the-shelf components.

b. Design and provide a lighting system sufficient for quality, still-video capture.

c. Equip the enrollment client with a dye-sublimation [_____] printer capable of printing directly to the access control or I.D. credential. Provide printer toner kits and other printing supplies to complete the initial enrollment by 200 percent.

2.6.6.3 Enrollment Client Software

Provide database management functions for the system and allow an operator to change and modify the data entered in the system as needed. The enrollment station is not to have any alarm response or acknowledgment functions as a programmable system function. Multiple, password-protected access levels are to be provided at the enrollment station. Database management and modification functions are to require a higher operator access level than personnel enrollment functions. Provide a means for disabling the enrollment station when it is unattended to prevent unauthorized use.

Provide a method to enter personnel identifying information into the entry control database files through enrollment stations to include a credential unit in use at the installation. In the case of personnel identity verification subsystems, this data is to include biometric data. Allow entry of this data into the system database files using simple menu

selections and data fields. The data field names are to be customized to suit user and site needs. All personnel identity verification subsystems selected for use with the system are to fully support the enrollment function and be compatible with the entry control database files.

2.7 COMMUNICATIONS

a. Communications are to link together subsystems of the ESS and be in accordance with Section 27 10 00 BUILDING TELECOMMUNICATIONS CABLING SYSTEM. Interfaces between subsystems cannot be accomplished by use of an electro-mechanical relay assembly. Communications links must be supervised. Provide common communications interface devices throughout the ESS. Provide the sensor to control unit interface as a dry contact relay that is normally open (NO) or normally closed (NC), except as specified otherwise.

b. Use digital, asynchronous, or multiplexed data control unit for central alarm reporting and display processor interface. Group individual data bits into word format and transmit as coded messages. Implement interface with network switches which function as a communications controller, perform data acquisition and distribution, buffering message handling, error checking, and signal regeneration as required to maintain communications.

c. Provide totally automatic status changes communication, commands, field-initiated interrupts, and any other communications required for proper system operation. Do not require system communication operator initiation or response. System communication is to return to normal after any partial or total network interruption including power loss or transient upset. Automatically annunciate communication failures to the operator with communication link identification that has experienced a partial or total failure.

2.7.1 Link Supervision

2.7.1.1 Hardwire Direct Current Line Supervision

Provide only for the sensor to control unit links which are within the ESS protected area. Supervise circuits by monitoring changes in the current that flows through the detection circuit and a terminating resistor of at least 2.2 K ohms. Supervision circuitry is to 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 are to provide an alarm response in the annunciator in not more than one second because of the following changes in normal transmission line current:

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

b. Ten percent or more in normal line signal when it consists of direct current from 10 microamperes to 0.5 milliamperes.

c. 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.

d. 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.

2.7.1.2 Hardwire Alternating Current Supervision

Supervision is not to be capable of compromise by use of resistance, voltage, or current substitution techniques. Use this method on circuits which employ a tone modulated frequency-shift keying (FSK), interrogate-and-reply communications method. Supervisory circuit are to be immune to transmission line noise, crosstalk, and transients. Terminate detection circuit by complex impedance. Maintain line supervision by monitoring current amplitude and phase. Size complex impedance so that current leads or lags the driving voltage by 0.785 plus or minus 0.087 rad 45 plus or minus 5 degrees.

Alarm when rms current changes by more than 5 percent, or phase changes by more than 0.087 rad 5 degrees for supervision current of 0.5 to 30 milliamperes rms. Alarm when rms current changes by more than 10 percent, or phase changes by more than 0.139 rad 8 degrees for lines with supervision currents of 0.01 to 0.5 milliamperes. Identified line supervision alarm must be communicated within one second of the alarm.

2.7.1.3 Hardwire Digital Supervision

Local processors are to exchange digital data to indicate secure or alarm at least every 2 seconds. Alarm if data is missed for more than one second for passive supervisory circuits. Coding used for data cannot be decipherable by merely viewing data on an oscilloscope. Supervisory circuits are to asynchronously transmit bursts of digital data for transponder schemes. Data pattern is to be random in nature. Remote detectors are to receive data and encode a response based on a proprietary coding scheme.

Provide a unique encoding scheme; [an industry-wide or vendor standard is not acceptable.] Transmit encoded response back to supervisory circuit. Supervisory circuit is to compare the response to an anticipated response. Alarm on failure of the detector to return a data burst or return an incorrect response.

2.7.2 Hardwire

2.7.2.1 Electrical Conductor Lines

a. Use electrical conductor lines for hardwire that rely on current path except for electrical wires; neutral conductors of electrical distribution systems cannot be used as signal transmitters.

b. Conductors outside the protected area are to be [shielded cable] [buried] [[installed in Galvanized Rigid Steel Conduit (GRC, RMC)] [installed in Electrical Metallic Tubing (EMT)] in accordance with Section 26 20 00 INTERIOR DISTRIBUTION SYSTEM]. Supervision circuitry is not to 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.

c. Ambient current levels chosen for line supervision must be sufficient to detect tampering and be within the normal operating range of electrical components. Report line supervision and tamper alarms regardless of mode of operation.

d. Provide hardwire links in accordance with UL 1076 and Section 26 20 00 INTERIOR DISTRIBUTION SYSTEM for interior applications with additions and modifications specified. Conductors are to be copper. Conductors for links which also carry AC voltage, are to be No. 12 AWG minimum; single conductors for low-voltage DC links are to be No. [14] [16] AWG minimum. Conductors are to be color coded. Conceal wiring in finished areas of new construction and wherever practical in existing construction if not otherwise precluded by the Government.

e. 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 is to be distinctively color-coded. Each circuit color-coded wire is to remain uniform throughout circuit. Tamper switches meet requirements of paragraph TAMPER SWITCHES.

2.7.2.2 Communication Link

a. Provide a dedicated circuit communication link from sensor to control unit. Opening or closing a relay contact will indicate an alarm. Convert analog signals to digital values or a relay closure or opening within 76 m 250 feet of the sensing point. Communications from control unit to central alarm reporting and display processor are to operate in a continuous interrogation and response mode, using time-multiplexed digital communications techniques at a data rate of [5.12] [10.24] [_____] kilobaud.

b. Interrogation and response communications between the control unit and central processor is to be half-duplex and bidirectional on one dual twisted pair cable (one pair for interrogation and one for response), which may have one or more parallel branches. Individual control unit lines are to be at least 22 AWG wire. Connect control wires in parallel to the hardwire link. Communication system is to provide as many as [255] [_____] control unit connections.

c. The communication system must maintain specified performance over a link length of 2287 m 7500 feet when operating without line repeaters or other signal regenerating or amplifying devices. The communications system must maintain specified performance over a link length of 22,865 m 75,000 feet when operating with signal-regenerating line repeaters.

d. Control unit to central alarm reporting and display processor communications link is to also be capable of operating over a maximum of [two] [four] [_____] standard voice grade telephone leased or proprietary lines. Link is to be capable of operating half-duplex over a Type 3002 data transmission pair and be capable of modular expansion. Telephone lines will be provided by the Government. Coordinate and check out system operation. General characteristics and telephone line service are to be as follows:

e.

Connections	Two- or four-wire
Impedance at 1000 Hz	600 ohms
Transmitting level	0 to 12 dBm
Transmitting level adjustment	3 dB increments
Type	Data
Direction	Two-way alternate (half-duplex)
Maximum speed	[1.2] [5.12] [10.24] [_____] kilobaud
Maximum loss at 1000 Hz	33 dB

2.7.3 Radio Frequency Link

****

NOTE: Radio frequency links may not be allowed on some of Government facilities. Recommended usage for RF links is as backup to hardwire links or to a remote location lacking telephone lines. As soon as possible, but no later than schematic design, the designer must 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 DODI 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 local/regional contact responsible for frequency allocation.

****

a. Provide a full-duplex, supervised RF, polling system specifically used for alarm data communications with components manufactured by one manufacturer operating in the VHF, [134 to 154 MHz] [_____] band. System is to interface directly with ESS hardwire data link from control unit to central alarm reporting and display location and is to translate (reduce) the data rate for RF transmission, modulate and demodulate the data signal, and transmit and receive ESS data.

b. 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 is to be ignored by all units except the addressee. Unit with the correct address is to decode the interrogation signal and respond to the interrogation with the status of the reporting sensors. Re-interrogate when the addressee fails to respond. Alarm upon failure to respond a second time.

c. Remote units in the RF system are to be individually polled in turn. Polling response time and transmission data rate, data error rate, and equipment reliability is to ensure that overall, ESS alarm annunciation time reliability and Pd is not degraded.

d. Provide RF transmitters, receivers, or transceivers in sufficient quantities to meet specified requirements. RF link transmissions are to be on one or more of the frequencies within the specified band as required to meet specified requirements and neither interfere with other ESS components nor any facility electronic components. Provide transmitters which are in accordance with applicable requirements of 47 CFR 15.

e. Message types and content are to be identical to those transmitted by other portions of the ESS data communications subsystem. ESS alarms sent by RF link are not to fail and are to be transmitted by the RF link due to event occurrence during "off air" periods. RF link is to provide message transmission priority in the following order:

(1) Intrusion alarms

(2) Tamper alarms

(3) Access denial alarms

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

f. Provide [omnidirectional, coaxial, half-wave dipole] [_____] antennas for alarm transmitters and transceivers with a driving point impedance to match transmission output. Provide antennas and antenna mounts that are corrosion resistant and able to withstand wind velocities of [160] [_____] km per hour [100] [_____] mph and physical damage caused by vandalism. Antennas cannot be mounted directly to any facility fence or roofing system.

g. Provide antennas from the same manufacturer as the rest of the RF link. Provide coaxial cable in lengths as required. Cables are to use PL-type fittings or connectors, properly protected against moisture. Cables must match transmitter output impedance.

2.7.4 Data Encryption

****

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

when appropriate. The designer should choose which encryption is required. AES is the strongest but may not be available from all manufacturers, TDES next, and DES is the lowest level of data encryption. Data encryption must be in accordance with NIST FIPS 140-2.

****

Incorporate data encryption equipment on data transmission circuits as shown on the drawings. The algorithm used for encryption must be the [Advanced Encryption Standard (AES) algorithm described in NIST FIPS 197] of [TDES], ASC/X9 X9.52, as a minimum. Data encryption must be in accordance with NIST FIPS 140-2.

2.7.5 Network Switch

****

NOTE: Designer to determine the hierarchy of the network such as star, self-healing ring, etc. Layer 3 switches should be considered for use throughout the design to accommodate future network requirements. Verify the existing environmental conditions to make sure the switch temperature range is compliant. Determine if multimode fiber or single mode fiber is required for Outside Plant (OSP) and Inside Plant (ISP) to accommodate future network requirements.

Verify network switch with local activity telecommunications manager.

For Army projects reference UFC 3-580-01.

****

[For Department of Defense projects network switches must comply with DISA APL.]The small form-factor pluggable (SFP) is to provide full-duplex 1000/100/10-Mbps connectivity between switches over [multimode fiber (MMF)] [single mode (SM)] infrastructures. Provide mounting accessories for a typical [field distribution box] [cabinet] [rack]. Rack requirements as specified in paragraph EQUIPMENT RACK.

2.7.5.1 Inside Plant

Provide a network switch for ESS system with [8] [12] [24] [48] [64] [_____] SFP Ethernet ports. Allow dynamic port base security and rapid spanning tree protocol with VLAN assignments for specific users regardless of where the switch is connected. The switch will use AC input voltage nominal of [120] [230] VAC at [50] [60] Hz. The switch is to be less than 2 Rack Units (RU) and Layer 3 capable. The switch is to have the capability of commanding a self-healing ring configuration. 1000Base-LX SFP Fast Ethernet Interface Converter is to be a hot swappable device that plugs into a Gigabit fiber SFP uplink port on the switch. The switch is to be a fully managed power over Ethernet (PoE) to all ports. Provide switch capable of using a Layer 3 (routed) port to connect to a LAN gateway port for Internet and web base access. The Mean Time Between Failure (MTBF) must be greater than 210,000 hours.

2.7.5.2 Outside Plant

Provide hardened managed Ethernet switch with a minimum of [6] [8] [12] 10/100/1000 switched RJ-45 ports and two 1000 Mb fiber ports designed for unconditioned outdoor applications. The switch is to be sealed, conduction cooled, use a rugged case with no fans and no air vent openings. The ambient operating temperature range is -40 to 75 degree C 40 to 170 degree F. The software includes SNMP, QoS, Telnet, Security, STP, VLAN, BootP / DHCP.

2.7.6 Video and ESS Transmission

****
NOTE: Include industry standard for each cable type on cable data sheets at the end of section.
****

Transmission is to be by optical fiber dedicated to the associated circuit. Video and ESS transmission cables must conform to the industry standards in [Section 27 10 00 BUILDING TELECOMMUNICATIONS CABLING SYSTEM] [Section 33 82 00 TELECOMMUNICATIONS OUTSIDE PLANT (OSP)].

Install interior cable in [Rigid Metal Conduit (RMC)] [Electrical Metallic Tubing (EMT)] conduit unless indicated otherwise. Provide conduit and fittings in accordance with Section 26 20 00 INTERIOR DISTRIBUTION. Use only compression fittings for EMT conduit. No set screw fittings allowed. Cable is to be rated for the installation method intended. Install exterior cable underground installed in [Schedule 40] [Schedule 80] Polyvinyl chloride (PVC) conduits.

2.7.7 Wire and Cable

****
NOTE: Designer to provide wire and cable data sheets for each wire and cable type. Refer to IC Tech Spec for IDC-ICS 705 and UFC 4-010-05 SCIF for for cables associated with SCIF environments.
****

Provide all wire and cable (including copper power cable, UTP data cable, optical fiber cable, and coaxial cable) not indicated as Government-furnished equipment. Wiring must meet NFPA 70 standards and as indicated in the Wire and Cable Data Sheets Attachment at the end of this section. Provide optical fiber test data and UTP test data for field connectorized cable, including any existing optical fiber cable and/or existing UTP which will be used to transmit data for any ESS items provided in the project..

2.7.8 Digital Data Interconnection Wiring

Interconnecting cables carrying digital data between equipment located at the SCC or at a secondary control and monitoring site is to be optical fiber cable. Interconnecting cables conform to the industry standards in [Section 27 10 00 BUILDING TELECOMMUNICATIONS CABLING SYSTEM] [Section 33 82 00 TELECOMMUNICATIONS OUTSIDE PLANT (OSP)].

2.7.9 Aboveground Sensor Wiring

Sensor wiring is to be 20 AWG minimum, twisted and shielded, 2, 3, 4, or 6

pairs to match hardware. Provide multiconductor wire with a PVC outer jacket.

2.7.10 Direct Burial Sensor Wiring

Sensor wiring is to be 20 AWG minimum, twisted and shielded, 2, 3, 4, or 6 pairs to match hardware.

2.7.11 Local Area Network (LAN) Cabling

Category 6 cabling must be in accordance with TIA-568.2. Provide permanent link testing and a test report for all Category 6 cabling.

2.7.12 Cable Construction

Provide all cable components that will withstand the environment in which the cable is installed for a minimum of 20 years.

[2.8 SECURITY LIGHTING INTERFACE

Provide an interface for control of the security lighting system in accordance with [Section 26 56 00 EXTERIOR LIGHTING] and as shown on the drawings.[Provide motion activation of lights for enhanced VSS performance.]

][2.9 MEDICAL FACILITY SYSTEM

****
NOTE: If the ESS design includes Medical Facilities, the designer to include additional security features to meet the requirements in UFC 4-510-01 Medical Military Facilities.

If the ESS design includes Medical Facilities the elevator control must interface with IPAS.
****

2.9.1 Infant Protection Alarm System (IPAS) Performance Requirements

****
NOTE: The Hospital will have a method of notifying responders to Medical Emergencies such as Radio Page or other Wireless Personal Communications Device. Use the same system to notify the staff in the protected area and any on site security team designated by the facility users.
****

a. Fully integrate the IPAS with the ESS system. Infant abduction alarms (exit alarms and tag tamper alarms) from the IPAS are to be received and processed the same as all other alarms and concurrently routed in real time to all Operator Workstations. Send notifications via radio page or other wireless Personal Communications device to the security unit staff and paged to the nursing staff in the alarmed unit.

b. The IPAS is to detect and report alarms if an attempt is made to remove an infant tag from the secured nursing area (exit alarm) or of an unauthorized removal of a tag strap from an infant (tag tamper alarm).

c. Wireless readers are to adequately cover all areas of the secured nursing units.

2.9.2 Infant Protection Alarm System (IPAS) Major Components

Major components of the IPAS include:

a. Network Adapters

b. Infant Protection Workstations

c. RF Readers

d. Infant Tags

e. Tag Straps

f. External Relay Boxes

g. Door Position Switches

h. Dome Lights with Buzzer Device

i. Electromagnetic Locks & Power Supplies (part of Door Hardware)

j. Card Readers

(1) Remote Display Units (RDU)

(2) Infant Protection Software

2.9.3 Infant Protection Operator Workstations

a. Operation, management, and monitoring of the Infant Protection Alarm Systems are to be performed from Infant Protection Workstations located in the [Nurse Stations] [Labor and Delivery] [Mother Baby Units] for the patient care units served. Locate an additional monitoring workstation at the [Nurse Team Center] [_____] of the [Med Surge Unit] [_____]. Functions performed at these workstations include:

(1) Management of the subsystem for the protected unit

(2) Infant Tag inventory, activation and assignment, and deactivation

(3) Strap inventory and use

(4) Infant data, tag and strap assignment, and discharge

(5) Alarm event reporting and monitoring

(6) Activity and event reports

(7) Display of alarm receivers and status

(8) Video display of alarmed cameras

b. The infant protection operator workstations include:

(1) CPU

(2) Computer keyboard

(3) Mouse

(4) Two video monitors

(5) Printer

(6) Removable media storage unit that provides for offline storage and retrieval of event activity

2.9.4 Remote Display Unit

Locate a RDU and an associated card reader near the secure side of each designated [exit door] [and elevator] to allow authorized staff to quickly suspend an infant tag, so that an infant can be taken out of the secured nursing unit without generating an exit alarm. Allow authorized staff to reactivate the infant tag when the infant is returned to the secured nursing unit. The RDU is to be inoperative until activated by the associated card reader when the card reader senses an access control card from a staff member that is authorized to take the infant out of the secured nursing unit. The RDU is to remain active for a programmed short period of time to allow the transaction to occur and then the RDU is to automatically become inactive.

2.9.5 Operator Interface

The IPAS operator workstations are to enable the real-time display of any alarms on graphical floor plans. Provide graphical display with the ability to select the following views:

a. All tags in the system, or

b. A specific tag

The system operator interface is to enable tags to be easily added or deleted from the system, by either using a button press to identify the tag ID code, or by typing in the tag ID code.

2.9.6 Alarm Management

The IPAS is to support several different types of alarms for the tags, including:

2.9.6.1 Tamper Alarm

This indicates a strap attaching a baby tag has been tampered or disconnected. Display the tag's name, description, and location in the alarm line.

2.9.6.2 Near Exit Alarm

This indicates a tag has moved into the proximity of a monitored exit door or elevator. The tag name, description, and location is to be displayed within 0.5 seconds on the IPAS Operator Workstation, transmit the alarm to radio pagers carried by on-duty security and nursing staff, and transmit

the alarm to the system database and system Operator Workstations.

The IPAS is to activate the electrical locks on the doors to the protected area. The doors will automatically unlock either upon the staff clearing the alarm, a power outage to the electrical lock control, an independent activation of the smoke alarm system, or water flow in the sprinkler system. The staff is to have the ability to unlock the doors at any time from inside the unit. The alarm event is to also activate a dome light and buzzer at the door until the alarm is acknowledged. Activation of IPAS will prevent the elevator from opening or stopping on the event floor.

2.9.6.3 Battery Alarm

This indicates the battery of a tag is low and should be replaced. Display the tag name, description, and its location in the alarm line.

2.9.6.4 Failed Communications Alarm

This indicates the network is not working or the database server has been shut down. No tag location or alarm can be performed while this alarm is active.

2.9.6.5 Lost Alarm

This indicates the tag cannot be detected by any reader in the system. Display the tag name, description, and its last-known location in the alarm line.

2.9.7 IPAS Area Wireless Tag Readers

The IPAS area wireless tag readers are to be able to be mounted either in the ceiling or on the walls. Provide readers with 360-degree coverage and an effective read range as required by the IPAS. The system is to assign the tag to the reader with the highest signal strength if more than one area wireless reader detects the tag signal. Multiple area wireless readers are to be able to be installed in a single room to narrow the location down to areas as small as a 10 foot radius using signal strength levels. The area wireless readers are to operate at an unlicensed radio frequency and have all necessary regulatory approvals.

2.9.8 IPAS Door Wireless Reader

The IPAS door wireless readers are to be able to be mounted either in the ceiling or walls. The readers are to transmit within an adjustable range (distance from and width of exit door) of each exit door to limit ifant tags detection within a very short distance of the exit door. The readers are to support wireless fields synchronization if multiple door wireless readers are used to cover a large entry area. The transmission field generated by the door wireless reader is to include an encrypted ID code that can be decoded by tags that enter the field.

2.9.9 Infant Tags and Straps

2.9.9.1 Tag Characteristics

Technology	Very low power wireless transmission
Power Battery	Rechargeable lithium battery with 5-year life
Transmission Rates	As required
LED Indication	Low battery, transmission
Tag ID	Unique factory programmed
Water Resistance	Waterproof and completely sealed housing

2.9.9.2 Tag Features

a. Automatically activate when attached to a baby

b. Manufactured with latex free adjustable strap made from skin safe material that includes a soft pad to prevent skin irritation

c. Have a re-adjustable strap to suit ankle shrinkage

d. Be easy to clean

e. Be manufactured with disposable parts, ensuring re-use of tag up to 1000 times without compromising hygiene level

f. Be rechargeable by placing them in a desktop charger that is supplied with the system. Multiple tags can be recharging simultaneously

2.9.10 IPAS Dome Lights

Mount a dome light configured with indicator lamps and a tone device over exit doors from areas equipped with an IPAS. A red light is to illuminate and the tone sound when an exit alarm is activated. The light and tone are to remain on until the exit alarm is acknowledged.

[2.9.11 Radio Page Interface

a. Unit is to interface with the radio page system capability of Section 27 52 24 NURSE CALL SYSTEM. This interface must be a hardwired connection to an input port on the radio page encoder.

b. Route all alarms to the radio page system for transmission to alphanumeric pagers carried by the security staff.

c. Transmitted alphanumeric alarm information is to include the type, location, date, and time of the alarm event.

d. Infant protection alarm event is to be radio paged to the nursing staff in the patient care area where the alarm originated.

]]2.10 SURVEILLANCE AND DETECTION EQUIPMENT

****
NOTE: For Army projects, contact the Electronic Security System Mandatory Center of Expertise (ESS MCX) for assistance in determining requirements for these devices. The ESS MCX e-mail address is AskESSMCX@usace.army.mil
****

2.10.1 Article Surveillance and X-Ray

Provide X-ray package search system suitable for [automated] [manual] detection and material density identification. The article surveillance is to function as a sensor or detector subsystem and connect to the local processors and alarm monitoring.

The article surveillance and X-ray device are to provide adjustable contrast and a surface area threshold setting. Incorporate a long-term image storage system to document subsystem operations. The article surveillance and X-ray device must have a minimum throughput rate of 600 packages per hour and be rated for continuous operation. The article surveillance and X-ray device must meet the requirements of 21 CFR 1020, Section 1020.40.

2.10.1.1 Size and Weight

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

2.10.1.2 Local Audible Alarms

Provide local audible alarm annunciation and automatic threat alert based upon an adjustable contrast and a surface area threshold setting. Immediately communicate to and annunciate alarms generated by the article surveillance and X-ray device at the SCC.

2.10.1.3 Maximum Package Size

Allow inspection of packages and other articles up to 380 mm tall, by 610 mm wide and 1.5 m long 15 inches tall, by 24 inches wide, and 60 inches long.

2.10.1.4 X-Ray Tube

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

2.10.1.5 Electrical

The article surveillance and X-ray device is to operate from the power source as indicated.

2.10.1.6 Safety

Include dual lead-lined curtains at the entrance and exit to the conveyer system package scanning region. The radiation exposure to operator for each package inspection must be no more than 0.2 milli-roentgens. The

article surveillance and X-ray device is not to adversely affect magnetic storage media as it is passed through the device.

2.10.1.7 Display

Use a standard 525 line [LCD] [LED] monitor to present X-ray data to the article surveillance and X-ray device operator. Configure the article surveillance and X-ray device to provide at least 64 gray scale shades or at least 64 distinct colors. The article surveillance and X-ray device is to provide:

a. Image enhancement

b. Zoom

c. Pan

d. Split screen

e. Freeze-frame capabilities

2.10.1.8 Conveyor

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

2.10.1.9 Material Identification and Resolution

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

2.10.2 Metal Detector

a. The metal detector is to function as a sensor or detector subsystem and connect to the local processors and alarm monitoring. The metal detector is to be rated for continuous operation. The metal detector is to use an active pulsed or continuous wave induction detection field.
b. The metal detector is to create a field detection pattern with no holes or gaps from top to bottom and across the passage area and provide 100 percent Faraday shielding of the sensor coil. The metal detector is to incorporate measures to minimize false alarms from external sources. Provide a synchronization module to allow simultaneous multiple metal detection subsystem operation, with no sensitivity or function degradation, when separated by 1.5 m 5 feet or more.

c. The metal detector is not to adversely affect magnetic storage media.

d. When incorporated into an entry booth, the metal detector is to be physically compatible with the entry booth configuration and connected to the entry booth local processor subsystem.

2.10.2.1 Size and Weight

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

2.10.2.2 Local Alarms

Provide metal detector with local audible and visual alarm annunciation that are also immediately communicated to and annunciated at the SCC.

2.10.2.3 Material Identification and Sensitivity

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

2.10.2.4 Traffic Counter

****
NOTE: If traffic counters are not required, eliminate this paragraph.
****

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

2.10.2.5 Electrical

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

2.11 BACKUP POWER

a. Intrusion alarms are not to be generated because of power switching; however, Provide a power switching indication and on-line source at the alarm monitor.

b. The system is to automatically switch back to the primary source upon primary power restoration. Detect and report failure of an on-line battery as a fault condition. Power products must be in accordance with Section 26 20 00 INTERIOR DISTRIBUTION SYSTEM.

c. Provide backup power to the primary power by [backup batteries in each element or subsystem] [uninterruptible power supply (UPS)].

[2.11.1 Uninterruptible Power Supply (UPS)

Backup power required for uninterrupted ESS operation [until a diesel engine generator set can assume the full load] is to be provided by a UPS.

The UPS is to consist of a rectifier, battery and support racks, a static inverter, static switch transfer, and a manual bypass switch. Provide UPS with a continuous output to supply the maximum load requirements of the ESS. Size the battery to sustain the UPS at full rated load [for [8] [24] [_____] hours] [for 15 minutes] [until diesel engine generator set can assume the load] [_____]. [The UPS is to be in accordance with Section 26 33 53 STATIC UNINTERRUPTIBLE POWER SUPPLY (UPS).]

][2.11.2 Batteries

Provide backup by dedicated batteries in remotely located system elements including individual sensors or control units. Batteries are to be an integral part of dispersed system elements when radio frequency (RF) operation is required. Batteries are to be capable of operation in any position and be protected against venting caustic chemicals or fumes within an equipment cabinet. Provide batteries capable of continuous operation for up to [8] [24] [_____] hours without recharge or replacement.

]2.12 SURGE SUPPRESSION DEVICES

Comply with requirements in Section 33 82 00 TELECOMMUNICATION OUTSIDE PLANT (OSP).

2.12.1 Powerline Surge Protection

Power Line Surge Protection Equipment connected to alternating current circuits must be protected from power line surges. Equipment protection must withstand surge test waveforms described in IEEE C62.41.1 and IEEE C62.41.2. Fuses must not be used for surge protection.

2.12.2 Powerline Sensor Device Wiring and Communication Circuit Surge Protection

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

a. A 10-microsecond rise time by 1000 microsecond pulse width waveform with a peak voltage of 1500 Volts and a peak current of 60 Amperes.

b. An 8-microsecond rise time by 20-microsecond pulse width waveform with a peak voltage of 1000 Volts and a peak current of 500 Amperes.

2.13 COMPONENT ENCLOSURE

****

NOTE: Designer will show on the drawings which specific enclosure is needed. Show metallic enclosures for both standard installations and high

security areas.
****

Alarm enclosures with a tamper switch(es). Refer to paragraph TAMPER SWITCHES. Enclosures is to be formed and assembled to be sturdy and rigid. These include:

a. Consoles

b. Annunciator housings

c. Power supply enclosures

d. Sensor control and terminal cabinets

e. Control units

f. Wiring gutters

g. Other component housings

2.13.1 Interior Sensor

Provide sensors to be used in an interior environment with a housing that provides protection against dust, falling dirt, and dripping noncorrosive liquids. Refer to paragraph INTERIOR ENCLOSURES for enclosure ratings.

2.13.2 Exterior Sensor

Provide sensors to be used in an exterior environment with a housing that provides protection against windblown dust, rain and splashing water, and hose directed water. Sensors are not to be damaged by the ice formation on the enclosure. Refer to paragraph "Exposed-to-Weather Enclosures" and "Corrosion-Resistant Enclosures" for enclosure ratings.

2.13.3 Interior Enclosures

Enclosures to house equipment in an interior environment must be housed in a metallic enclosure and meet the requirements of NEMA 250 Type [12] [1] [_____].

2.13.4 Exposed-to-Weather Enclosures

Enclosures to house equipment in an outdoor environment must be housed in a metallic enclosure and meet the requirements of NEMA 250 Type [3R] [4] [4X] [_____].

2.13.5 Corrosion-Resistant Enclosures

Enclosures to house equipment in a corrosive environment must be housed in a metallic enclosure and meet the requirements of NEMA 250 Type 4X.

2.13.6 Hazardous Environment Equipment

All system electronics to be used in a hazardous environment must be housed in a metallic enclosure which meets the requirements of paragraph HAZARDOUS LOCATIONS.

2.13.7 Metal Thickness

Thicknesses of metal in cast and sheet metal enclosures of all types must be not less than those listed in Tables 8.1, 8.2, and 8.3 of UL 1610 for alarm components, and NEMA ICS 2 and NEMA ICS 6 for other enclosures. Sheet steel used in enclosure fabrication is to be at least 16 gauge; consoles are to be at least 18 gauge.

2.13.8 Doors and Covers

a. Doors and covers are to be flanged. Provide tight pin hinges or the ends of hinge pins are to be tack welded to prevent ready removal where doors are mounted on hinges with exposed pins.

b. Provide doors having a latch edge length of less than 600 mm 24 inches with a single lock. Provide the door with a three-point latching device with lock where latch edge of a hinged door is 600 mm 24 inches or more in length; or alternatively with two locks, one located near each end.

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

2.13.9 Ventilation

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

2.13.10 Mounting

Sheet metal enclosures are to be rated for wall mounting with top hole slotted, unless otherwise indicated. Mounting holes are to be in positions which remain accessible when major operating components are in place and door is open and be inaccessible when door is closed.

2.13.11 Labels

Junction Boxes utilized for ESS and ESS system connections must be labeled with "ESS".

2.13.12 Test Points

Provide readily visible and accessible with minimum disassembly of equipment to test points, controls, and other adjustments inside enclosures. Test points and other maintenance controls must be readily accessible to operator personnel.

2.14 EQUIPMENT RACK

****

NOTE: The designer will provide a drawing showing the amount of rack space needed for the rack mounted IDS, ACS,and VSS equipment, and placement of the equipment in the rack. Coordinate the IDS, ACS, and VSS equipment rack with actual equipment being

installed.
****

Provide standard 483 mm 19 inch electronic rack cabinets conforming to UL 50 for the ESS system at the SCC and remote control and monitoring sites as shown on the drawings. Equipment rack must be in accordance with Section 27 10 00 BUILDING TELECOMMUNICATIONS CABLING SYSTEM.

2.14.1 Labels

Provide a labeling system for cabling as required by TIA-606 and UL 969. Provide stenciled lettering for voice and data circuits using [thermal ink transfer process][laser printer] [_____].

2.15 LOCKS AND KEY LOCK

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

2.15.1 Lock

Provide locks on system enclosures for maintenance purposes that meet UL 437 and are [round-key type, with three dual, one mushroom, and three plain pin tumblers] [or] [conventional key type lock having a five-cylinder pin and five-point three position side bar combination]. Keys must be stamped "U.S. GOVT. DO NOT DUP.". Keys are only to be withdrawn when in the locked position. Key all maintenance locks alike and furnish only two keys for all of these locks.

2.15.2 Key-Lock Operated Switches

All key-lock-operated switches required to be installed on system components are to be UL 437, [with three dual, one mushroom, and three plain pin tumblers,] [or] [conventional key type lock having a five-cylinder pin and five-point three position side bar combination]. Keys must be stamped "U.S. GOVT. DO NOT DUP.". Key-lock-operated switches are to have two positions, with the key removable in either position. Key all key-lock-operated switches differently and furnish only two keys for each key-lock-operated-switch.

2.15.3 Construction Locks

Use a set of temporary locks during installation and construction. Do not include any of the temporary locks in the final set of locks installed and delivered to the Government.

2.16 FIELD FABRICATED NAMEPLATES

Nameplates must comply with 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 is to identify the function and, when applicable, the position.

Nameplates are to be melamine plastic, 3 mm 0.125 inch thick, white with [black] [_____] center core. Surface is to be matte finish. Corners are to be square. Accurately align lettering and engrave into the core. Minimum size of nameplates must be 25 by 65 mm 1 by 2.5 inches. Provide lettering a minimum of 6.35 mm 0.25 inch high normal block style. Nameplates are not required for devices smaller than 25 x 75 mm 1 x 3 inches.

2.16.1 Manufacturer's Nameplate

Each item of equipment is to 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.

2.17 FACTORY APPLIED FINISH

Electrical equipment is to have factory-applied painting systems which meets the requirements of the NEMA 250 corrosion-resistance test as a minimum.

PART 3 EXECUTION

3.1 INSTALLATION

Install the system in accordance with safety and technical standards NFPA 70, UL 681, UL 1037, and UL 1076. Configure components within the system with appropriate service points to pinpoint system trouble in less than 20 minutes.

****
NOTE: Electric metallic tubing (EMT) may be considered for use if it is used solely within the secure protected area.
****

Install all system components, including any equipment that is furnished by the Government, and appurtenances in accordance with the manufacturer's instructions, NFPA 70 and as shown on the drawings, and furnish all necessary connectors, terminators, interconnections, services, and adjustments required for a complete and operable system.

3.1.1 Existing Equipment

Connect to and utilize existing equipment, control signal transmission lines, and devices as shown on the drawings. Any equipment and signal lines that are usable in their original configuration without modification may be reused with Government approval.

Make written requests and obtain approval prior to disconnecting any signal lines and equipment that creates equipment outage. Such work can proceed only after receiving Government approval of these requests. If any device fails after work has commenced on that device, signal, or control line, diagnose the failure and perform any necessary corrections to the equipment. The Government is responsible for maintenance and repair of Government equipment. The Contractor will be held responsible for repair costs due to negligence or abuse of Government equipment on their part.

3.1.2 Software Installation

****
NOTE: Coordinate Software Installation with Government's cybersecurity requirements and interpretations.
****

Load software as specified and required for an operational system, including databases and specified programs. Provide original and backup copies on [optic discs] [_____] of all accepted software, including diagnostics, upon successful endurance test completion.

3.1.3 Enclosure Penetrations

Enclosures are to be penetrated from the bottom unless shown otherwise. Penetrations of interior enclosures having transitions of conduit from interior to exterior, and penetrations of exterior enclosures are to be sealed with rubber silicone sealant to preclude the entry of water. Terminate conduit risers in a hot-dipped galvanized metal cable terminator that is filled with a sealant as recommended by the cable manufacturer, and in a manner that does not damage the cable.

3.1.4 Cable and Wire Runs

****
NOTE: Design requirements must conform to NFPA 70, Section 26 20 00 INTERIOR DISTRIBUTION SYSTEM, and ICS 705-1.
****

Perform required cable and wire routings per NFPA 70 [and] [Section 26 20 00 INTERIOR DISTRIBUTION SYSTEM,] [ICS 705-1], and as specified. Terminate conduits including flexible metal and armored cable in the sensor or device enclosure. Fit ends of conduit with insulated bushings. Exposed conductors at ends of conduits external to sensors and devices are not acceptable.

3.1.5 Soldering

Soldered electrical connections must use composition Sn60, Type AR or S, for general purposes; use composition Sn62 or Sn63, Type AR or S, for special purposes. Flux must conform to ASTM B32 when Type S solder is used for soldering electrical connections.

3.1.6 Galvanizing

Ferrous metal is to be hot-dip galvanized in accordance with ASTM A123/A123M. Provide screws, bolts, nuts, and other fastenings and supports that are corrosion resistant.

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

3.1.7 Conduits

****

NOTE: Design requirements for interior conduits must conform to NFPA 70, Section 26 20 00 INTERIOR DISTRIBUTION SYSTEM, and ICS 705-1. Design requirements for exterior conduits must conform to NFPA 70, Section 33 71 02 UNDERGROUND ELECTRICAL DISTRIBUTION, and ICS 705-1.

****

Install interior conduits in accordance with NFPA 70, Section 26 20 00 INTERIOR DISTRIBUTION SYSTEM and ICS 705-1. Install exterior conduits in accordance with NFPA 70, Section 33 71 02 UNDERGROUND ELECTRICAL DISTRIBUTION and ICS 705-1.

3.1.8 Underground Cable Installation

Install underground conductors connecting protected structures and objects to the central alarm updating and display unit as direct burial or in conduit in accordance with Section 33 71 02 UNDERGROUND ELECTRICAL DISTRIBUTION. Coaxial cable cannot be spliced.

3.1.9 Exterior Fences

****

NOTE: Coordinate this requirement with requirements of Section 32 31 13 CHAIN LINK FENCES AND GATES; 32 31 13.53 HIGH-SECURITY FENCES (CHAIN LINK AND ORNAMENTAL) AND GATES.

****

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

3.1.10 Camera Housings, Mounts, and Poles

****

NOTE: Designer will specify correct Section numbers for concrete camera pole foundations, electrical work, and control signal cable.

****

a. Provide a foundation for each camera pole as specified and designed.

b. Provide a ground rod for each camera pole and connect the camera pole to the ground rod [as shown on the drawings] [in accordance with Section 33 71 01 OVERHEAD TRANSMISSION AND DISTRIBUTION.]

3.1.11 Field Applied Painting

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

3.1.12 Bonding, Grounding, and Shielding

Provide in accordance with TIA-607 and NFPA 70. Provide ground rods, bonding conductors, and grounding busbars in accordance with Section 26 20 00 INTERIOR DISTRIBUTION SYSTEM.

****

NOTE: General requirements for grounding, bonding and shielding are contained in MIL-STD-188-124B and MIL-HDBK-419A. Designer will ensure that proper grounding, bonding, and shielding is provided to all security equipment.

****

3.1.12.1 Grounding

Provide a ground system that consists of the earth electrode and lightning protection, surge protection, fault protection and signal reference subsystems.

3.1.12.1.1 Earth Electrode Subsystem

Provide an earth electrode subsystem that provides a path of low resistance to earth for lightning and power fault currents.

3.1.12.1.1.1 Ground Rod

Provide ground rods as needed. Ground rods must be [copper clad galvanized] [stainless steel], a minimum of [3.0] [_____] m [10] [_____] foot in length and not less than [19.1] [_____] mm [3/4] [_____] inch in diameter. Install ground rods vertically with the top at least [304.8] [_____] mm [12] [_____] inches below grade. The resistance to earth should not exceed 10 ohms for any ground rod location supporting an electronic sensor. Consider alternate methods for reducing the resistance to earth where 10 ohms cannot be obtained due to high soil resistivity, rock formations, etc.

3.1.12.1.1.2 Perimeter Fence

Ground perimeter animal control or security fences for personnel safety and to minimize the potential for equipment damage caused by lightning strikes. Ground sensored fences with ground rods at every sensor post supporting an electronic sensor. Ground fences with no electronic security equipment with ground rods at intervals of 198.12 meters 650 feet. Ground all fences on each side of all gates, at each corner, or change in fence direction, at points 45.72 meters 150 feet on each side of high tension wiring crossings, and at the closest approach to any building located within 15.24 meters 50 feet of the fence. For all fences, bond a #2 AWG copper wire to the fence post, bottom steel tension wire, and ground rod. Bonding will be in accordance with MIL-HDBK-419. Bond ground straps to posts and ground rods by exothermic welding or brazing. Bond hinged gates to gate posts. Ensure each bend in the copper cable is gradual and does not exceed a radius of 203.2 mm 8 inches. The angle of any bend will not be less than 90 degrees. The fence to earth ground will not exceed 10 ohms. Non-electronic, sensored fences may be grounded to 25 ohms.

3.1.12.1.1.3 Field Distribution Boxes (FDBs)

Ground each FDB with a grounding rod, which will be commonly bonded with power and sensor ground in the FDB on a common ground bus. Verify that all paint and or foreign substance that would preclude continuity of the signal path has been removed when securing a ground bus/strip. Attach the FDB ground wire to the grounding rod by exothermic welding.

3.1.12.1.1.4 Towers and Structures

****
NOTE: NFPA 70 and MIL-HDBK-419A provide design guidance on protection of structures and surge protection for equipment.
****

Provide security alarm monitoring facilities that contain major concentrations of security equipment such as consoles with a lightning protection system including air terminals, down conductors, surge arrestors and station grounds, all connected to a common counterpoise system.

3.1.12.2 Surge Protection Subsystem

3.1.12.2.1 Exterior Equipment

Provide lightning surge protection for exterior sensor equipment, Field Distribution Boxes, and camera equipment. Provide surge protection on input and output circuits of field equipment boxes to protect transponders and power supplies.

3.1.12.2.2 Interior Equipment

Ground interior sensor surge protection devices to an existing facility ground provided the ground is thoroughly checked for integrity. If a proper facility ground is not available, install a code compliant ground in accordance with the National Electric Code.

3.1.12.2.3 Fault Protection Subsystem

****
NOTE: The fault protection subsystem consists of a separate grounding conductor to provide protection to personnel and equipment from static charge buildup and electrical faults.
****

Install a fault protection subsystem that provides a conductive path between the earth electrode subsystem and all exposed metal parts of electrical enclosures. Provide fault protection for exterior and interior equipment by means of an equipment-grounding conductor routed from the equipment to the AC power distribution panel.

3.1.12.2.4 Signal Reference Subsystem

****
NOTE: This interior subsystem is that part of a ground system that is used to provide a ground reference plane for all signal paths. It is used

essentially to control noise.
****

Install a proper Signal Reference Subsystem for security systems in accordance with MIL-HDBK-419. Bond all security equipment cases or cabinets to the equipotential planes by the shortest and most direct route.

3.1.12.3 Bonding

****
NOTE: Bonding is essential in all circuits, both communications and power, as well as in lightning protection, where conductors must be joined. The engineer must specify bonding requirements per MIL-STD-188-124 and MIL-HDBK-419A.
****

Provide bonding by [welding] [brazing] [clamping] in accordance with MIL-STD-188-124 and MIL-HDBK-419.

3.1.12.4 Shielding

****
NOTE: Shielding prevents the security equipment or cabling from propagating interference and also protects it from similar effects by other electrical or electronic systems. It is the engineers' responsibility to specify the proper type of shielding to be used for security equipment and cabling, and to adhere to standards in MIL-HDBK-419A.
****

Provide [_____] shielding in accordance with the standards in MIL-HDBK-419.

3.1.13 Nameplate Mounting

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

3.2 ADJUSTMENT, ALIGNMENT, SYNCHRONIZATION, AND CLEANING

a. Clean each system component of dust, dirt, grease, or oil incurred during and after installation or accrued subsequent to installation from other project activities subsequent to installation.

b. Prepare for system activation by manufacturer's recommended procedures for adjustment, alignment, or synchronization.

c. Prepare each component in accordance with appropriate provisions of component installation, operations, and maintenance manuals.

d. Remove large vegetation that may sway in the wind and touch fencing.

e. Adjust sensors so that coverage is [overlapping and] maximized without mutual interference.

3.3 SYSTEM STARTUP

Do not apply power to the system until after:

a. Set up system equipment items and communications in accordance with manufacturer's instructions.

b. Conduct a system visual inspection to ensure that defective equipment items have not been installed and that there are no loose connections.

c. Test and verify system wiring as correctly connected.

d. Verify system grounding and transient protection systems as properly installed.

e. Verify the correct voltage, phasing, and frequency of the system power supplies.

Satisfaction of the requirements above does not relieve the contractor of responsibility for incorrect installations, defective equipment items, or collateral damage as result of Contractor work or equipment.

3.4 SUPPLEMENTAL CONTRACTOR QUALITY CONTROL

****

NOTE: The Contractor quality control requirements for all electronic security projects, as stated in 01 45 00 QUALITY CONTROL, must be included in contracts, regardless of increase in project cost. Normally this Contractor quality control requirement is applicable to projects in excess of $1,000,000.

****

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

The above requirements supplement the quality control requirements specified elsewhere in the contract.

3.5 ESS SYSTEM TESTING

All ESS Testing requirements are specified in Section 28 08 10 ELECTRONIC SECURITY SYSTEM ACCEPTANCE TESTING.

3.6 ESS TRAINING

Conduct training courses for [10] [_____] designated personnel in system maintenance and operation. Coordinate training with the Government. The training is to be oriented to the specific system being installed. Training content is to include training manuals and audio-visual materials. Deliver training manuals for each trainee with 2 additional copies delivered for archiving at the project site. The manuals are to

include an agenda, defined objectives for each lesson, and a detailed subject matter description for each lesson.

Furnish audio-visual equipment and other training materials and supplies. Deliver copies of the audio-visual materials to the Government either as a part of the printed training manuals or on the same media as that used during the training sessions when course portions are presented using audio-visual material.

3.6.1 ESS Training Outline

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

Submit a training plan for the training phases, including type of training to be provided, outline of training manuals, training course agendas, and a list of reference material, for Government approval.

3.6.2 Typical Training Day

A training day is defined as:

a. Eight hours of classroom instruction, with

(1) Two 15-minute breaks

(2) One hour lunch break

b. Conducted:

(1) Monday through Friday

(2) During the daytime shift in effect at a government-provided training facility

For guidance in planning the required instruction, assume that attendees will have a high school education or equivalent, and are familiar with ESS. Approval of the planned training schedule is to be obtained from the Government at least 30 days prior to the training.

3.6.3 ESS Administrator Training

a. ACS and IDS Administrator Training includes:

(1) [Two] [_____] eight-hour on-site training sessions

(2) Operating system procedures and configuration

(3) Operator functions

(4) Database functions and setup

(5) Card holder 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

(10) System backup and restore

b. VSS Administrator Training includes:

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

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

3.6.4 ESS Operator Training

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

a. ACS and IDS Operator Training includes:

(1) [Four] [_____] (one-day) [8] [_____] hour 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. VSS Operator Training includes:

(1) [Two] [_____] (one-day) [8] [_____] hour on-site training sessions

(2) System operating procedures

(3) System configuration

(4) Video call-up

(5) Camera and monitor control

(6) Graphics functionality

(7) Basic device terminology and troubleshooting

3.6.5 Maintenance Personnel Training

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

course. The training includes:

a. Physical layout of each piece of hardware.

b. Troubleshooting and diagnostics procedures of each piece of hardware.

c. Component repair and replacement procedures of each piece of hardware.

d. Maintenance procedures and schedules to include system testing after repair of each piece of hardware.

e. Calibration procedures of each piece of hardware. Upon course completion, the students are to be proficient in system maintenance.

f. Review of site-specific drawing package, device location, communication, topology, and flow.

3.6.6 Follow-up Training

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

b. Follow-up training is to begin one month after initial training.

c. Training is to include testing for system competence.

-- End of Section --