(i) This is a combined synopsis/solicitation for commercial items prepared in accordance with the format in the Federal Acquisition Regulation (FAR), subpart 12.6, as supplemented with additional information included in this notice. This announcement constitutes the only solicitation; this is a Request for Quotation (RFQ) and a written solicitation will not be issued.

(ii) The solicitation number is N00030SUE0045

(iii) The solicitation document and incorporated provisions and clauses are those in effect through Federal Acquisition Circular 2005-88 and Defense Change Notice 20160630. Service Contract Act (SCA) WD 05-2351 applies.

(iv) This solicitation is a small business set-aside. The applicable North American Industry Classification System (NAICS) code 561621 –Security System Services (except Locksmith). The Small Business Size Standard for this NAICS code is $20.5 Million.

(v) Naval Criminal Investigative Service (NCIS) has a requirement for a new Intrusion Detection System (IDS) and Installation of (IDS) at Naval Criminal Investigative Services located at Naval Weapons Station (NWS), Bldg C46, Earle, New Jersey.

The New Intrusion Detection Systems must be comparable to the LENEL system. New Systems must be tied to the existing

CLIN	DESCRIPTION	QUANITY
0001	**INTRUSION DETECTION SYSTEM (IDS)**	1
	Lenel Server and Software License	1
	Lenel Intelligent Dual Reader Controller	1
	Lenel Dual Reader Interface Module	1
	Lenel Input/Output Control Module	1
	Lenel HID Card Reader	11
	Lenel Command Keypad	3
	12VDC 7AH Battery	3
	Wireless Doorbell	1
	Door Release Button	1
	High Security Door Sensor	10
	12VDC Electric Strike	11
	Ceiling-mounted 360 Degree Motion Sensor	20
	Hold-Up Switch	3
	Wireless Receiver/Transmitter	1
	Two-tone Siren	3
	Wall-mounted Tamper Resistant Camera with Pan/Tilt/Zoom	1
	12” Monitors	3

	Miscellaneous Wire and Cable and Hardware	
0002	**INSTALLATION AND TESTING OF IDS**	1
	Install and wire CLIN 0001 components. Program and test installed system. Installed system must be tied to the existing NWS LENEL system	
0003	**INSTALLATION DRAWING**	1
	Digital and Hard Copy of completed drawing of final equipment locations and wiring details	

See Attached Statement of Work for project specifications

(vi) Description of Requirements (requirement listed in this paragraph are for Item 0001 through 0003

Statement of Work (SOW
For Naval Criminal Investigative Service
Intrusion Detection System and Installation

SECTION 28 20 00.00 20
ELECTRONIC SECURITY SYSTEMS (ESS), COMMERCIAL –

PART 1 GENERAL

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

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

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

INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS (IEEE)
IEEE 100 (2000; Archived) The Authoritative Dictionary of IEEE Standards Terms

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

NATIONAL FIRE PROTECTION ASSOCIATION (NFPA)

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

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

U.S. DEFENSE INTELLIGENCE AGENCY (DIA)
DIA DCID 6/9 (2002) Director of Central Intelligence Directive No. 6/9

UNDERWRITERS LABORATORIES (UL)
UL 1037 (1999; Reprint Dec 2009) Safety Antitheft Alarms and Devices
UL 1076 (1995; Reprint Sep 2010) Proprietary Burglar Alarm Units and Systems
UL 1610 (1998; Reprint Sep 2010) Standard for Central-Station Burglar-Alarm Units
UL 294 (2013) Access Control System Units
UL 639 (2007; Reprint May 2012) Standard for Intrusion Detection Units
UL 681 (2014) Installation and Classification of Burglar and Holdup Alarm Systems
UL 796 (2010; Reprint Sep 2013) Standard for Printed-Wiring Boards

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

1.3 DEFINITIONS
Unless otherwise specified or indicated, electrical and electronics terms used in these specifications, and on the drawings, shall be as defined in IEEE 100.
a. Active mode: That in which some type of signal is continuously sent across the link, resulting in simple link breaks being readily detected.
b. Fail-safe: The capability to monitor system functions and report an alarm when a failure is detected in a critical system function.
c. Installer: Either the Contractor or a subcontractor with whom the Contractor has a firm contractual agreement.
d. Intruder: An animate object at least 48 inches in height, 75 pounds in weight and 4 cubic feet in volume, moving through the protected zones or portals at a velocity of 0.1 to 10 feet per second.
e. Sensor zone: A geographic position for which an intrusion must be identified and displayed and may be the combination of multiple detection devices.
f. Element: As used in this section means a constituent part of a complex signal such as an ac or dc voltage or current, ac phase, or frequency duration.

1.4 SYSTEM DESCRIPTION
Provide new Electronic Security Systems (ESS), including associated equipment and appurtenances. The design of the ESS shall include devices and equipment used to detect intrusion, control access to restricted areas, detect and deny unauthorized entries within specific areas, generate reports, produce Photo Identification badges, provide surveillance and annunciate alarms. The ESS shall be designed to provide operational flexibility and reliable performance. The ESS shall be modular, allowing for future incremental expansion or modification of inputs, outputs, and remote control stations. Integrated system capabilities shall include but not be limited to Intrusion Detection,
Automated Access Control, Intercommunications, and Photo Badge Identification. Each system shall be complete and ready for operation and provide for a fully integrated central station solution. The new

equipment shall be LENEL compatible with and operate accurately and reliably with the existing base system. Include materials not normally furnished by the manufacturer with the ESS equipment as specified in Section 26 20 00 INTERIOR DISTRIBUTION SYSTEM.

1.4.1 Design Requirements

1.4.1.1 Backup Battery Capacity Calculations
Submit calculations showing that backup battery capacity exceeds sensor operation, communications supervision, and alarm annunciation power requirements.

1.5 SUBMITTALS
Government approval is required for submittals with a "G" designation; submittals not having a "G" designation are for Contractor Quality Control approval. When used, the "A/E" designation following the "G" designation identifies that the submittal shall be reviewed by the Architect/Engineer.
Submittals with an "S" are for inclusion in the Sustainability Notebook, in conformance to Section 01 33 29.00 25 SUSTAINABILITY REQUIREMENTS.
Submit the following in accordance with Section 01 33 00 SUBMITTAL PROCEDURES:

The Electrical Engineer will review and Naval Criminal Investigative Service will approve submittals requiring special review in this section.

Include wiring diagrams and installation details of equipment indicating proposed location, layout and arrangement, control panels, accessories, piping, ductwork, and other items that must be shown to ensure a coordinated installation. Wiring diagrams shall identify circuit terminals and indicate the internal wiring for each item of equipment and the interconnection between each item of equipment. Drawings shall indicate adequate clearance for operation, maintenance, and replacement of operating equipment devices. Submittals shall include the nameplate data, size, and capacity. Submittals shall also include applicable federal, military, industry, and technical society publication references.
SD-02 Shop Drawings
ESS components; G A/E
Overall system schematic; G A/E
SD-03 Product Data
Interior point sensors; G A/E
Interior volumetric sensors; G A/E
Card reader; G A/E
Keypad; G A/E
Communications cable; G A/E
Communications interface devices; G A/E
Batteries; G A/E
SD-05 Design Data
Backup battery capacity calculations; G A/E
SD-06 Test Reports
ESS operational test plan; G A/E
SD-07 Certificates
ESS operational test plan; G A/E
Installer's qualifications; G A/E
Instructor's qualifications; G A/E
SD-10 Operation and Maintenance Data
ESS components, Data Package 5; G
ESS software, Data Package 1; G

Submit in accordance with Section 01 78 24.00 25 FACILITY ELECTRONIC OPERATION AND MAINTENANCE SUPPORT INFORMATION (eOMSI) and Section 26 00 00.00 20 BASIC ELECTRICAL MATERIALS AND METHODS.
SD-11 Closeout Submittals
As-Built drawings for ESS; G

1.6 QUALITY ASSURANCE

1.6.1 Drawings

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

1.6.1.2 Overall System Schematic
Indicate the relationship of integrated components on one diagram and show power source, system controls, impedance matches; plus number, size, identification, and maximum lengths of interconnecting wires. Drawings shall be not less than 11 by 17 inches.

1.6.2 Evidence of Experience and Qualifications

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

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

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

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

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

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

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

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

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

1.6.6.2 Material and Equipment Manufacturing Date
Products manufactured more than 3 years prior to date of delivery to site shall not be used, unless specified otherwise.

PART 2 PRODUCTS

2.1 ESS SUBSYSTEMS
Provide a complete integrated ESS consisting of the following major subsystems:
a. Intrusion Detection System
b. Automated Access Control System
c. Communications
d. Alarm reporting and display
e. Power

2.2 INTEGRATED SYSTEM FUNCTIONAL REQUIREMENTS
Ensure that ESS is fully integrated with physical security and other elements of the overall facility security system. Provide specific subsystem consisting of the following:
a. Intrusion Detection subsystem: Sensors, premise control units (PCU) and software modules to detect and report intrusion attempts and provide means to indicate a duress condition.

b. Automated Access Control subsystem: Electronic devices, access control units (ACU), sensors and software modules to detect intrusion attempts monitor and control personnel movement through normal access routes in and out of the facility and between protected areas within the facility.
c. Communications subsystem: Elements required to ensure that pertinent data is transferred from point of origin to point where appropriate actions can be taken.
d. Alarm reporting and display subsystem: Software, hardware and devices to control, process, integrate, and annunciate ESS data.
e. Power subsystem: Components required to ensure continuous operation of the entire ESS.

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

2.3 INTEGRATED SYSTEM PERFORMANCE REQUIREMENTS
The installed and operating ESS shall be integrated into the overall facility to detect intrusion and Control Access and shall perform as an entity, as specified below.

2.3.1 Detection Coverage
Provide and adjust sensors so that coverage is maximized without mutual interference. ESS coverage shall include the facility perimeter and critical spaces within the facility.

2.3.2 Detection Resolution (Sensitivity)
Sensitivity shall be capable of the following:
a. Locating intrusions within facility;
b. Locating intrusions at individually protected assets or at an individual portal;
c. Locating intrusions within volume or areas to within the coverage on a single volumetric sensor; and
d. Locating failures or tampering at individual sensors.

2.3.3 Detection Alarm and Reporting Capacity
The ESS shall have the capacity to collect, communicate, and display up to 256 sensor zone alarms. If the sensor zone is a combination of multiple alarm sources, the system shall maintain the capability to identify individual sensors in an alarm state. A single alarm shall be annunciated within one second average, 2 seconds maximum, after sensor transducer or other detection device activation.

2.3.4 Intrusion Detection System (IDS)
Provide a complete digital IDS with the performance criteria in accordance with specification Section 28 16 00.00 20 BASIC INTRUSION DETECTION SYSTEM (IDS).

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

2.4.1 Modularity
Provide components designed for modular increase or decrease of system capability by installation or removal of plug-in modules. Design system components to facilitate modular subassembly and part replacement.

2.4.2 Reliability

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

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

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

2.4.5 Environmental Conditions

2.4.5.1 Interior Conditions
Equipment installed in environmentally protected interior areas shall meet performance requirements specified for the following ambient conditions:
a. Temperature: 32 to 120 degrees F. Components installed in unheated security protected areas shall meet performance requirements for temperatures as low as zero degrees F;
b. Pressure: Sea level to 15,000 feet above sea level;
c. Relative humidity: 5 to 95 percent;
d. Fungus: Components shall be constructed of nonfungus nutrient materials or shall be treated to inhibit fungus growth; and
e. Acoustical noise: Components shall be suitable for use in high noise areas above 100 dB, such as boiler rooms, power plants, and foundries without adversely affecting their performance.

2.4.5.2 Exterior Conditions
Components mounted in locations exposed to weather shall be housed in corrosion-resistant enclosures with appropriate environmental protection.
Component performance shall not degrade because of improper housing design. Components in enclosures shall meet performance requirements when exposed to the following ambient conditions:
a. Temperature: Minus 25 to 140 degrees F;
b. Pressure: Sea level to 15,000 feet above sea level;
c. Solar radiation: Six hours of solar radiation at dry bulb temperature
of 120 degrees F including 4 hours of solar radiation at 104 watts per square foot;
d. Sand and dust: Wind driven for up to 6 miles per hour;
e. Rain: 2 inches per hour and 5 inches/hour cyclic with wind plus one period of 12 inches per hour;
f. Humidity: 5 to 95 percent;
g. Fungus: Warm, humid atmosphere conducive to the growth of heterotropic plants;
h. Salt fog: Salt atmosphere with 5 percent salinity;
i. Snow: Snow loading of 48 pounds per square foot (psf) per hour; blowing snow of 4.6 psf per hour;
j. Ice accretion: Up to 1/2 inch of radial ice;
k. Wind: Up to 50 mph with gusts to 66 mph, except that fence sensors shall detect intrusions up to 35 mph; and

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

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

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

2.4.8 Human Engineering
Aural considerations shall include location of annunciators, tone pitch, quality, and intensity. Number of different audible signals shall not exceed four. Component design shall provide for ease of accessibility for maintenance.

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

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

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

2.4.9.1 Mission Software
Mission software shall consist of software implemented to provide complete operation of the ESS. Software shall be LENEL compatible.

2.4.9.2 Support Software

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

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

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

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

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

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

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

2.4.11.4 Mounting
Unless otherwise indicated, sheet metal enclosures shall be designed for wall mounting with top hole slotted. Mounting holes shall be in positions which remain accessible when major operating components are in place and door is open, but shall be inaccessible when door is closed.
2.4.11.5 Labels
Labels shall be affixed to such boxes indicating they contain no connections. These labels shall not indicate that the box is part of the intrusion detection system.

2.4.11.6 Enclosure Locks

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

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

2.4.12.1 Interior Point Sensors
a. Door and window protection: Accomplish by one or more of the following:
(1) Balanced magnetic switches (BMS): Switches shall be surface mounted and shall have a minimum of three encapsulated reed switches. Switches shall activate when a disturbance in the balanced magnetic field occurs. Provide each BMS with an overcurrent protective device, rated to limit current to 80 percent of the switch capacity. BMS shall be rated for a minimum lifetime of one million operations. House the BMS components in nonferrous enclosure materials.
(2) Surface mount BMS: Switch mechanism shall be internally adjustable so the operating gap between faces of the switch housing and the magnet housing may be adjusted from 1/4 to 1/2 inch to accommodate installation variances. Surface mount BMS housing for the switch element shall have the capability to receive threaded conduit. Housing cover for surface mounted BMS, if made of cast aluminum, shall be secured by stainless steel screws. Magnet housing cover shall not be readily removable. Protect BMS housing from unauthorized access by a cover operated, corrosion-resistant tamper device. Device shall initiate an alarm when cover is opened as little as 1/8 inch and shall be inaccessible until actuated. BMS shall have a minimum of three pre-adjusted reed switches and three pre-adjusted magnets. Field adjustments in the fixed space between magnet and switch housing shall not be possible. Attempts to adjust or disturb the magnetic field shall cause a tamper alarm. Conductors running from the door to alarm circuits shall be jumpered within a flexible armored cord constructed from corrosion-resistant metal. Each end of the armored cord shall terminate in a junction box or other enclosure. Armored cord ends shall be mechanically secured to the junction boxes by clamps or bushings. Conductors within the armored cord shall be provided with lug terminals at each end. Jumpered conductors and the armored cord shall experience no mechanical strain as the door is removed from fully open to closed. Switch circuit shall initiate an alarm if a short circuit is applied to the door cord.

2.4.12.2 Interior Volumetric Sensors
Passive infrared sensors: Sensors shall detect intruder presence by monitoring the level of infrared energy emitted by objects within a protected zone. Sensor shall initiate an alarm upon observing increased or fluctuating infrared energy caused by the presence and motion of an intruder whose temperature is as little as 3 degrees F different from the background temperature. Sensor shall be passive in nature; no transmitted energy shall be required for detection. Sensor shall be sensitive to infrared energy emitted at wavelengths corresponding to human body and other objects at ambient temperatures. Sensor detection pattern shall be 180 degrees for volumetric units, unless otherwise indicated, and shall be housed in a tamper-alarmed enclosure. Sensor shall provide some means of indicating an alarm condition during installation and calibration. A means of disabling the indication shall be provided within the sensor enclosure. Sensor shall alarm when an intruder moves within the area of protection more than 5 feet at a velocity of 0.1 foot per second, and one step per second, assuming 6 inches/step. Detection sensitivity

shall be irrespective of direction of motion. Sensor shall also alarm at velocities faster than 0.1 foot per second, up to 10 feet/second. Sensor maximum detection range shall be a minimum of 35 feet. Sensor shall not alarm in response to general area thermal variations.

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

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

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

All AACS programming data shall reside on a single database and shall be instantly accessible to every networked PC workstation connected to the ESS. AACS functions shall include validation based on time of day and day of week, special day/holiday scheduling with card validation override, video image storage and retrieval of cardholder photographs, access validation based on positive verification of card, card/PIN, card and video.

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

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

The AACS shall include fully integrated badging capabilities, including image capture, image editing, badge design, and badge printing. The system shall permit the storage of four different images: main photograph, alternate photograph, signature, and fingerprint. The AACS shall allow each cardholder to be assigned to both a badge design formatted for badge printing and a dossier design formatted for standard paper printing. The AACS shall provide for interfacing with external badge programs, in which stored

photo images are displayed in cardholder information window but other badge features are supported by the external program. The Photo imaging components shall include one or more networked PC workstations at which all of the required image capture equipment has been installed.

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

The AACS shall provide ability to display stored 'video image' of cardholder based on card activity. The card reader shall not activate the door lock until positive operator acknowledgment from the SCC.

The AACS software shall be capable of, but not limited to, the following programming:
(1) Time Schedules: Up to 254 user-definable time schedules shall be provided. These time schedules shall determine the day(s) and times that access will be granted or a scheduled event shall occur. Any and all of the time schedules shall be available for defining access privileges and scheduled events. There shall be ALWAYS and NEVER schedules that cannot be altered or removed from the system. Each user-defined time schedule shall have the option of reacting or not reacting to user-defined special days, with the ability to react uniquely to each type of special day.
(2) Special Days: There shall be an unlimited number of user-definable special days. These days shall be used for configuring exceptions to the normal operating rules, typically for specifying holiday operating rules. Each special day shall be assigned to a type, with each type defined by the user.
(3) ACU Daylight Savings Time Adjustment: There shall be a software-configurable, user defined adjustment for Daylight Savings Time. The ACU shall not need to be connected to a PC workstation in order for the adjustment to occur.
(4) Scheduled Events: Any access controlled reader shall be capable of scheduled unlock periods to allow for card-free access. The access controlled reader shall also be capable of requiring one valid access event before beginning a scheduled unlock period. Additionally, any access control point shall be capable of requiring a valid card as well as a PIN code via keypad on a scheduled basis for high security areas. The use of PIN via keypad functions shall not reduce the number of card reader or alarm points available in the ACU(s). Any designated alarm input shall be able to be scheduled Armed and Disarmed. Any relay output shall be capable of scheduled On and Off periods to allow for automatic I/O system control.
(5) Maximum User Capability: Up to 64,000 individual users may be given access cards or codes and have their access controlled and recorded.
(6) Access Groups: Each system user shall be assignable to a maximum of 4 of 256 possible access groups. An access group shall be defined as one or more people who are allowed access to the same areas at the same days and time periods.
(7) Active/Expire Dates: Any card/user may be configured with activation and expiration dates. The card can be assigned to any valid access group and will be activated and expired according to the specified dates.
(8) Maximum Use Settings: Any card/user may be configured with maximum number of uses for that card. The card can be assigned to any valid access group and will be expired according to the specified number of card uses.
(9) Door Outputs: Each access control reader shall have two dedicated relay outputs. Both relays shall provide Normally Open and Normally Closed contacts. The first relay shall be used for electric lock control. The second shall be software configurable to activate for door forced open, door left open too long, duress, passback violations, invalid access attempts and valid unlock conditions. Both relays shall be separately programmable for energize times from 1 second to 10 minutes. The second relay shall allow a delay time to be specified, causing its activation to be delayed after an activating condition occurs.
(10) Anti-Passback: The AACS shall have global anti-passback capability. Any door on the system can be linked to one of 254 user defined passback areas or two 2 pre-defined areas. Each door may be set up to

automatically forgive passback entries at the following intervals: Never, at Midnight, every 12 hours (Midnight and Noon), every 6 hours, every 2 hours, each hour or every 30 minutes. Each door can be configured to deny or grant access for passback violations and individual users can be exempt to the passback rules. The anti-passback features shall be a global function and operate completely independent of the AACS software with the exception of configuring the passback rules. Additionally, the operator shall have the ability to manually forgive an individual user or all users by command from the AACS.
(11) Two Person Rule: Any access control reader on the system shall have the ability to require two valid cards for access. This feature shall be software programmable. Any access control reader on the system that includes a keypad shall also have the ability to require a valid PIN number associated with each of the two valid cards.
(12) User List/Who's In (Muster Reports): The AACS shall be capable of generating dynamic lists of users in certain access-controlled areas, based either upon selected users or selected areas. The lists shall have the option of automatically refreshing after a user-selected interval of time.
(13) Crisis Mode: The AACS shall support "crisis mode", in which the activation of user-selected alarm points causes changes to user access privileges. The changes to user access privileges shall be configurable to restrict normal access to no access or limited access. (14) Door Groups: The system shall allow up to 255 door groups to be configured. Doors belonging to the same group shall be able to be locked, unlocked, disabled and enabled on command from the AACS.
(15) Door Interlocking: The system shall allow a group of doors to be software configured so that if any door in the group is unsecure, all other doors shall be automatically disabled. This feature also known as "mantrap" configuration. The interlocking features shall not require the AACS to be on-line for proper operation.
(16) PIN Required: The AACS shall support the required use of a keypad code, in addition to a valid credential, at user-selected doors, during user-selected schedules.
(17) Remote door control: The SCC operator shall have the capability of manually controlling any access point by issuing a simple command from the AACS. The operator shall have the ability to lock, unlock, enable, disable and pulse any door in this manner. This activity shall cause an entry to be logged displaying the door name, number and time that it was performed. Additionally, the operator shall have the ability to lock, unlock, enable and disable any group of doors in a Door Group by a single command from the AACS.
(18) Key Control: When interfaced with an approved key-control system, the system shall allow users to deny access to certain doors to any users who have keys in their possession.
(19) Guard Tour: The AACS shall support user-defined guard tours. The tour may be configured in a set pattern of tour points, or may follow a mode in which all tour points can be visited in any order within an allotted time. The AACS shall allow a tour to be started by AACS-command, by use of a selected card at a selected reader, or by use of a selected keypad code at a selected keypad. The system shall detect guard late-to-point; point missed, and point out-of-sequence events. The system shall generate a report at the completion of a tour.
(20) Reader Disable: The AACS shall support disabling readers in reaction to a user-selected number of invalid access attempts.
(21) Disable Event Messages: The AACS shall allow users to disable user-selected event messages (Door Forced Open, Door Open Too Long, Door Closed, Request to Exit) for user-selected doors. The AACS shall allow users to disable certain messages (Door Forced Open, Door Open Too Long) according to a user-selected schedule.
(22) I/O Groups: The AACS shall allow up to 255 user-defined I/O (input-output) groups to be defined. Each Input device shall be able to be linked to these groups for arming, disarming, shunting and unshunting as well as output control.
(23) Delays: Each alarm device shall allow a delay to be specified. The delay shall be either an entry type or a dwell type. An entry-type delay shall prevent the input from issuing an alarm event until the delay elapses. If unarmed during the delay period, the alarm condition shall be ignored. A dwell-type delay

shall require the input to remain in the alarm state for the full duration of the delay before issuing an alarm condition.
(24) Remote Input control: The operator shall have the capability of manually controlling any alarm/input point by issuing a simple command from the AACS. The SCC operator shall have the ability to shunt, unshunt, disable and restore any input in this manner. This activity shall cause an entry to be logged displaying the input name and time that it was performed. Additionally, the operator shall have the ability to arm, disarm, shunt and unshunt any alarm partition/group by a single command from the SCC. The arm disarm, shunt and unshunt any alarm partition/group from the SCC shall not be permissible in DIA DCID 6/9 applications.
(25) Output Configuration: Each output relay shall be software configurable as a FOLLOWS, LATCH, TIMEOUT, SCHEDULED, TIMEOUT RETRIGGERABLE, LIMIT, or COUNTER type. The SCHEDULED type shall allow a time schedule to automatically control its activation and de-activation. The FOLLOWS, LATCH, TIMEOUT, TIMEOUT RETRIGGERABLE, LIMIT and COUNTER types shall be configured to activate based on the condition of I/O groups. Additionally, a time schedule shall be specified to configure when the output shall actively monitor the I/O groups.
(26) Remote Output control: The operator shall have the capability of manually controlling any output point by issuing a simple command from the SCC. The SCC operator shall have the ability to ENABLE, DISABLE, turn ON and turn OFF any output in this manner based on the output type. A FOLLOWS type output shall not be capable of being turned OFF or ON. This activity shall cause an entry to be logged displaying the output name and time that it was performed. manual control of outputs shall not be permissible in DIA DCID 6/9 applications.
(27) Remote Reset Command: Any ACU shall have the capability of being reset manually or by command issued from the AACS. This reset command shall have the option of simulating the ACU reset settings, or forcing a reset type as specified by the user. The remote reset command shall not cause the ACU to degrade its level of protection to any access points defined.
(28) Dial Out: The ACU shall have the capability of using a modem to automatically connect to the AACS when a critical alarm or service event occurs. The conditions triggering the dial out capability shall be user defined and software configurable.
(29) Time Zone: The AACS shall allow the user to select the time zone in which the ACU is located, so that event times displayed for that ACU will match the local time where the ACU is located.
(30) User-Selected LED Behavior: The AACS shall allow the user to select different behaviors for the LEDs of each access controlled reader.
(31) Traced Cards: The AACS shall be capable of selecting any number of cardholders for the purpose of limiting reports to only traced users. The AACS shall be capable of displaying all traced cardholder events in a user-selected alternate color.
(32) Badge Print Tracking: The AACS shall support setting a print limit for any badge. The software will track the number of times any badge has been printed, as well as display the date and time of the most recent printing.
(33) Intrusion Detection: The AACS shall have the capability to arm and disarm door access control devices and sensors indicated from a card reader with keypad.

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

2.4.13.2 Access Control Subsystem Central Processing

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

2.4.13.3 Access Control Unit (ACU)
The ACU shall be micro-processor based with all access and I/O decisions to be made by the individual ACU(s). The ACU shall be of modular design which will allow for present security requirements and the capability to expand. All field ACU panels shall be configured to intercommunicate via RS-422/485 or RS-232 hardwired, Dial-up, TCP/IP or fiber-optic communication. All field ACU(s) shall be equipped with a tamper contact. One ACU shall be designated a "Primary", responsible for all AACS-to-ACU communications. All other ACU(s) up to a maximum of 16 shall be designated "Secondaries" and shall communicate with the "Primary" via an RS-422/485 hardwire, TCP/IP network or fiber-optic configuration. The ACU shall be capable of, but not limited to, the following:
(1) All ACU(s) shall have built-in surge suppression circuitry on plug-in modular circuit boards. The surge protection, designed as an integral component of the system, shall be self-sacrificing in the event of extreme surges or spikes.
(2) Each ACU shall be capable of supporting at least 2 ports and be expandable in increments of two ports up to a maximum of 8 ports per ACU.
(3) Each ACU port shall be configured by AACS to support any one of the following peripheral devices: Card reader, Alarm Monitoring Module, Output Relay Module. Any combination of these devices can be supported on each ACU, up to a total of 8 devices per ACU.
(4) Each ACU shall have the capability of supporting multiple card reader technologies simultaneously, including Transmissive Infrared, Wiegand, Magnetic stripe, Proximity, Barcode, Keypad, Card/Keypad, Smart Card, and Biometrics. This capability shall be an integral part of the ACU and will not require special external equipment.
(5) Each ACU shall have built-in battery back-up of programmed information and shall be sustainable for a period of not less than ninety days.
(6) Each ACU shall be powered by a 24 VDC power source rated at a minimum of 2 amperes. The power supply shall have a battery back-up for complete system operation in the event of power failure. Provide batteries for all ACU(s) to sufficiently power the ACU for 24 hours continuous service.
(7) Electric strikes, other locking devices and ancillary peripherals shall have a separate power supply. Battery back-up shall be utilized for continued operation in the event of power failure.
(8) There shall be a minimum of a 10,300 event log buffer per ACU. The log buffer shall be used to record and hold access and alarm activity information until the AACS is connected and receives the information. There shall be a software-configurable warning notification of log buffer filling for ACU(s) configured with modem capabilities.

2.4.13.4 Card Reader and Keypad Access Control Devices
Devices shall be tamper alarmed, tamper and vandal resistant, and solid state, containing no electronics which could compromise the access control subsystem should the subsystem be attacked. Devices shall be

surface, semiflush, or weatherproof mountable as specified for each individual location. Card readers shall be the proximity type and shall be capable of reading PIV Class CAC/Keypad, Smart Card type access control cards. Keypads shall contain an integral 12-digit tactile keyboard with digits arranged in numerical order. Keypad shall be integrated into the card reader.

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

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

2.4.14.1 Link Supervision
a. Hardwire direct current line supervision: Provide only for sensor to control unit links which are within ESS protected area. Circuit shall be supervised by monitoring changes in the current that flows through the detection circuit and a terminating resistor of at least 2.2 kohms. Supervision circuitry shall initiate an alarm in response to opening, closing, shorting, or grounding of conductors by employing Class C, standard line security. Class C circuit supervisor units shall provide an alarm response in the annunciator in not more than one second as a result of the following changes in normal transmission line current:
(1) Five percent or more in normal line signal when it consists of direct current from 0.5 through 30 milliamperes.
(2) Ten percent or more in normal line signal when it consists of direct current from 10 microamperes to 0.5 milliampere.
(3) Five percent or more of an element or elements of a complex signal upon which security integrity of the system is dependent. This tolerance will be applied for frequencies up to 100 Hz.
(4) Fifteen percent or more of an element or elements of a complex signal upon which the security integrity of the system is dependent. This tolerance will be applicable for all frequencies above 100 Hz.
b. Hardwire alternating current supervision: Supervision shall not be capable of compromise by use of resistance, voltage, or current substitution techniques. The method shall be employed on circuits which employ a tone modulated frequency-shift keying (FSK), interrogate-and-reply communications method. Supervisory circuit shall be immune to transmission line noise, crosstalk, and transients. Detection circuit shall be terminated by a complex impedance. Supervision of the line shall be maintained by monitoring current amplitude and phase. Complex impedance shall be sized so that current leads or lags the driving voltage by 45 plus or minus 5 degrees. For supervision currents of 0.5 to 30 milliamperes root mean square (rms), an alarm shall result when rms current changes by more than 5 percent, or phase changes by more than 5 degrees. For lines with supervision currents of 0.01 to 0.5 milliampere, an alarm shall result when rms current changes by more than 10 percent, or phase changes by more than 8 degrees. Identified line supervision alarm shall be communicated within one second of the alarm condition.

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

2.4.14.2 Hardwire

a. Hardwire shall utilize electrical conductor lines. Alarm electrical lines shall not rely on current path except for electrical wires; neutral conductors of electrical distribution systems shall not be used as signal transmitters. Conductors outside the protected area shall be installed in electrical metallic tubing (EMT) as specified in Section 26 20 00 INTERIOR DISTRIBUTION SYSTEM. Supervision circuitry shall not initiate nuisance alarms in response to normal line noise, transients, crosstalk, or in response to normal parametric changes in the line over a temperature range of minus 30 to 125 degrees F. Ambient current levels chosen for line supervision shall be sufficient to detect tampering and shall be within the normal operating range of electrical components. Line supervision and tamper alarms shall be reported regardless of mode of operation. Provide hardwire links as specified in UL 1076 and Section 26 20 00 INTERIOR DISTRIBUTION SYSTEM for interior applications with additions and modifications specified herein. Conductors shall be copper. Conductors for links which also carry AC voltage, shall be No. 12 AWG minimum; single conductors for low-voltage dc links shall be No. 14 AWG minimum. Conductors shall be color coded. Conceal wiring in finished areas of new construction and wherever practical in existing construction if not otherwise precluded by the Government. Identify conductors within each enclosure where a tap, splice, or termination is made. Identify conductors by plastic-coated, self-sticking, printed markers or by heat-shrink type sleeves. Connect sensors, control units, and communication devices so that removal will cause a tamper alarm to sound. Pigtail or "T" tap connections are not acceptable. Each conductor used for identical functions shall be distinctively color coded. Each circuit color code wire shall remain uniform throughout circuit.

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

(1) Connections: Two- or four-wire

(2) Impedance at 1000 Hz: 600 ohms

(3) Transmitting level: 0 to 12 dBm

(4) Transmitting level adjustment: 3 dB increments
(5) Type: Data
(6) Direction: Two-way alternate (half duplex)
(7) Maximum speed: 10.24 kilobaud
(8) Maximum loss at 1000 Hz: 33 dB.
c. Video hardwire links shall be as specified in paragraph entitled "Video Transmission."

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

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

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

PART 3 EXECUTION

3.1 EQUIPMENT INSTALLATION
UL 681, UL 1037, and UL 1076, and the appropriate installation manual for each equipment type. Components within the system shall be configured with appropriate "service points" to pinpoint system trouble in less than 20 minutes.

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

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

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

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

3.2 ADJUSTMENT, ALIGNMENT, SYNCHRONIZATION, AND CLEANING

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

3.3 ESS System Acceptance and Training

3.3.1 ESS System Acceptance Test
ESS System Acceptance testing shall be performed as follows;
a. The NAVFAC and NAVFAC Engineer will conduct final acceptance testing of the system.
b. Prior to the final acceptance test, security contractor shall conduct a complete test of the entire ESS including subsystems and provide the NAVFAC and NAVFAC Engineer with a written report.
c. Following completion of the initial testing and correction of any noted deficiencies, conduct a five-day burn-in test, intent of the burn-in test shall be to prove the ESS by placing it in near real operating conditions. During this period the ESS shall be fully functional and programmed such that all points, interfaces, controls, reports, messages, prompts, etc. can be exercised and validated. Record and correct any system anomaly, deficiency, or failure noted during this period. Scheduling of the final acceptance test shall be based on a review of the results of this burn-in test.
d. Deliver a report describing the results of the functional tests, burn-in tests, diagnostics, calibrations, corrections, and repairs including written certification to the NCIS and NAVFAC that the installed complete ESS has been calibrated, tested, and is fully functional as specified herein.
e. Prior to the final acceptance test, complete all clean-up and patch work requirements. Security equipment closets and similar areas shall be free of accumulation of waste materials or rubbish caused by operations under the Contract At completion of the Work, remove all waste materials, rubbish, contractor tools, construction equipment, machinery and all surplus materials.
f. Upon written notification from the Contractor that the ESS is completely installed, integrated and operational, and the burn-in testing completed, NAVFAC and NCIS will conduct a final acceptance test of the entire system at a mutually acceptable time.
g. During the final acceptance test, no adjustments, repairs or modifications to the system shall be conducted without the permission of NAVFAC or NCIS.
h. During the course of the final acceptance test by the NAVFAC and
NCIS, the Contractor shall be responsible for demonstrating that, without exception, the completed and integrated ESS complies with the contract requirements. Physical and functional requirements of the project shall be demonstrated and shown. This demonstration will begin by comparing as-built drawings conditions of the ESS to requirements outlined in this Section, item by item. Following the Section compliance review, ESS and SCCd equipment will be evaluated.
i. The functionality of the various interfaces between systems will be tested.
j. The installation of all field devices will be inspected. This field inspection will weigh heavily on the general neatness and quality of installation, complete functionality of each device, and compliance with mounting, back box and conduit requirements.
k. All equipment shall be on and fully operational during any and all testing procedures. Provide personnel, equipment, and supplies necessary to perform all site testing. Provide a minimum of two Contractor employees familiar with the ESS for the final acceptance test. One contractor employee shall be responsible for monitoring and verifying alarms while the other will be required to demonstrate the function of each device. Supply at least two radios or portable telephones for use during the test.
l. NAVFAC and NCIS retain the right to suspend, terminate or reschedule testing at any time when the ESS is found to be incomplete or fails to perform as specified. In the event that it becomes necessary to suspend, terminate or reschedule the test, all of the NAVFAC and NAVFAC Engineers fees and expenses related to the test shall be deducted from the Contractor's retainage. In the event it becomes necessary to suspend, terminate or reschedule the test, the

Contractor shall work diligently to complete and/or repair all outstanding items as required by the Contract Documents. The Contractor shall supply NAVFAC and NCIS with a detailed punch list completion schedule outlining task-by-task completion dates and a tentative date for a subsequent retest. During the final acceptance test, no adjustments, repairs or modifications to the system shall be conducted without the permission of NAVFAC and NCIS.

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

3.3.2.1 ESS Administrator Training
a. ACS and IDS Administrator Training shall include:
(1) Two eight-hour on-site training sessions.
(2) Operating system procedures and configuration.
(3) Operator functions.
(4) Database functions and setup.
(5) Cardholder input and deletion procedures.
(6) Report generation.
(7) Applications programs (as applicable).
(8) Graphics generation and manipulation.
(9) Items unique to the ACS and IDS interfaces with other systems

3.3.2.2 ESS Operator Training
Coordinate the operator training syllabus with NCIS prior to conducting operator training.
a. ACS and IDS Operator Training shall include:
(1) Four (one-day) 8 hours on-site training sessions.
(2) System operating procedures.
(3) System configuration orientation.
(4) Alarm acknowledgment.
(5) Alarm response logging.
(6) Graphics functionality.
(7) Items unique to the ACS and IDS interfaces with other systems.

3.3.3 Follow-up Training
a. One, two hour training session each month for two months after initial training.
b. Follow-up training shall begin one month after initial training.
c. Training shall include testing for system competence.

3.3.4 Training Operating and Maintenance Personnel
Furnish instruction for operating staff in system operation and operator troubleshooting and preventive maintenance procedures. Instruction shall consist of 3 man-days, 8 hours per day, and shall be held during normal duty hours. Commence instruction after system is fully operational, and complete instruction prior to system acceptance and turnover to the Government. Furnish maintenance instruction for Government maintenance personnel in adjustment, operation, and maintenance of each system equipment. Attendance at equipment manufacturer's recommended maintenance training schools may be substituted for this training. Costs associated with such schooling, less travel and per diem, shall be borne by the Contractor. Complete maintenance instruction prior to system acceptance and turnover to the Government.

3.4 FIELD APPLIED PAINTING

Paint electrical equipment as required to match finish of adjacent surfaces or to meet the indicated or specified safety criteria. Painting shall match existing.

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

-- End of Section --

SECTION 28 16 00.00 20
BASIC INTRUSION DETECTION SYSTEMS (IDS) -

PART 1 GENERAL
1.1 REFERENCES
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.

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

INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS (IEEE)
- IEEE 100 (2000; Archived) The Authoritative Dictionary of IEEE Standards Terms

NATIONAL ELECTRICAL MANUFACTURERS ASSOCIATION (NEMA)
- NEMA ICS 2 (2000; R 2005; Errata 2008) Standard for Controllers, Contactors, and Overload Relays Rated 600 V
- NEMA ICS 6 (1993; R 2011) Enclosures

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

UNDERWRITERS LABORATORIES (UL)
- UL 1076 (1995; Reprint Sep 2010) Proprietary Burglar Alarm Units and Systems
- UL 1610 (1998; Reprint Sep 2010) Standard for Central-Station Burglar-Alarm Units
- UL 1635 (1996; Reprint Jan 2010) Digital Alarm Communicator System Units
- UL 1638 (2001; Reprint Oct 2013) Visual Signaling Appliances - Private Mode Emergency and General Utility Signaling
- UL 609 (1996; Reprint Sep 2010) Local Burglar Alarm Units and Systems
- UL 634 (2007; Reprint Mar 2013) Connectors and Switches for Use with Burglar-Alarm Systems
- UL 639 (2007; Reprint May 2012) Standard for Intrusion Detection Units
- UL 681 (2014) Installation and Classification of Burglar and Holdup Alarm Systems
- UL 796 (2010; Reprint Sep 2013) Standard for Printed-Wiring Boards

1.2 STANDARD PRODUCTS

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

1.3 DEFINITIONS

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

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

b. Element: Constituent part of a complex signal such as AC or DC voltage or current, AC phase, or frequency duration.

c. Fail-safe: Capability to monitor for system functions and to report an alarm when a failure is detected in a critical system function.

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

e. Intruder: Animate object at least 48 inches in height, 75 pounds in weight and 4 cubic feet in volume, moving through protected zones or portals at a velocity of 0.1 to 10 feet per second.

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

1.4 SYSTEM DESCRIPTION

Provide new basic intrusion detection system (IDS), including associated equipment and appurtenances. Provision of IDS shall include supervising installation of rigid or flexible conduit for IDS during site preparation, running system wires and cables, and system component installation, component testing, and system checkout. Each system shall be complete and ready for operation. Equipment, materials, installation, workmanship, inspection, and testing shall be as specified herein. Include materials not furnished by the manufacturer with IDS equipment as specified in Section 26 20 00 INTERIOR DISTRIBUTION SYSTEM.

1.5 SUBMITTALS

Government approval is required for submittals with a "G" designation; submittals not having a "G" designation are for Contractor Quality Control approval. When used, the "A/E" designation following the "G" designation identifies that the submittal shall be reviewed by the Architect/Engineer. Submittals with an "S" are for inclusion in the Sustainability Notebook, in conformance to Section 01 33 29.00 25 SUSTAINABILITY REQUIREMENTS. The following shall be submitted in accordance with Section 01 33 00 SUBMITTAL PROCEDURES:

The Electrical Engineer will review and Naval Facilities Engineering Command will approve submittals requiring special review in this section. Drawings and descriptive data shall be approved prior to procurement, fabrication, and installation. A schedule of required submittals shall be prepared to be integrated with the overall construction management schedule to ensure adequate review and necessary corrective work before installation.

Include wiring diagrams and installation details of equipment indicating proposed location, layout and arrangement, control panels, accessories, piping, ductwork, and other items that must be shown to ensure a coordinated installation. Wiring diagrams shall identify circuit terminals and indicate the internal wiring for each item of equipment and the interconnection between each item of equipment. Drawings shall indicate adequate clearance for operation, maintenance, and replacement of operating equipment devices.

Submittals shall include the nameplate data, size, and capacity. Submittals shall also include applicable federal, military, industry, and technical society publication references.

SD-02 Shop Drawings
IDS components; G
Overall system schematic; G

SD-03 Product Data
Interior point sensors; G
Interior volumetric (space) sensors; G A/E
Control communicators; G
Duress alarms; G
Keypad; G
Communications interface devices; G
Batteries; G
Tamper switches; G
Strobes; G

SD-06 Test Reports
IDS operational test plan; G

SD-07 Certificates
IDS operational test plan; G
Installer's qualifications; G
Instructor's qualifications; G
IDS equipment; G

SD-10 Operation and Maintenance Data
IDS, Data Package 5; G
Submit in accordance with Section 01 78 24.00 20, FACILITY ELECTRONIC OPERATION AND MAINTENANCE SUPPORT INFORMATION (eOMSI).

SD-11 Closeout Submittals
As-Built drawings for IDS; G
Posted operating instructions for IDS; G

1.6 QUALITY ASSURANCE

1.6.1 Drawings

1.6.1.1 IDS Components
Provide drawings that clearly and completely indicate the function of each component of the IDS. Indicate termination points of devices and indicate interconnections required for operation of the system. Indicate interconnection between modules and devices. In addition, provide a layout drawing which shows spacing of components, location, and details of mounting and positioning.

1.6.1.2 Overall System Schematic
The overall system schematic shall indicate the sequence of operation, the relationship of integrated components on one diagram, and show power source, system controls, impedance matches, plus number, size, identification, and maximum lengths of interconnecting wires. Drawings shall not be less than 11 by 17 inches.

1.6.2 Experience and Qualifications

1.6.2.1 Installer's Qualifications
Prior to installation, submit data for approval by the Naval Criminal Investigative Service, of the installer's experience and certified qualifications. Show that the installer who will perform the work has a minimum of 3 years' experience successfully installing IDS of the same type and design as specified herein. Include names, locations, and points of contact of at least five installations of the same type and design as specified herein where the installer has installed such systems. Indicate the type of each system and certify that each system has performed satisfactorily in the manner intended for a period of not less than 1 year(s).

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

1.6.3 IDS Operational Test Plan
Submit for approval at least 30 days prior to commencement of formal operational testing. Include detailed procedures for operational testing of each IDS component and subsystem, and for performance of an integrated system test.

1.6.4 IDS Equipment
Submit manufacturer's certification of UL listing.

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

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

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

1.6.6 Standard Products
Provide materials and equipment that are products of manufacturers regularly engaged in the production of such products which are of equal material, design and workmanship. Products shall have been in satisfactory commercial or industrial use for 2 years prior to bid opening. The 2-year period shall include

applications of equipment and materials under similar circumstances and of similar size. The product shall have been on sale on the commercial market through advertisements, manufacturers' catalogs, or brochures during the 2-year period. Where two or more items of the same class of equipment are required, these items shall be products of a single manufacturer; however, the component parts of the item need not be the products of the same manufacturer unless stated in this section.

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

1.6.6.2 Material and Equipment Manufacturing Date
Products manufactured more than 3 years prior to date of delivery to site shall not be used, unless specified otherwise.

1.7 WARRANTY
The equipment items shall be supported by service organizations which are reasonably convenient to the equipment installation in order to render satisfactory service to the equipment on a regular and emergency basis during the warranty period of the contract

PART 2 PRODUCTS

2.1 IDS SUBSYSTEMS
Provide a complete integrated IDS compatible with the base Lenel systems consisting of the following major subsystems:
a. Detection
b. Arm/disarm multiple function keypad
c. Communications
d. Assessment
e. Alarm reporting
f. Power

2.2 INTEGRATED SYSTEM FUNCTIONAL REQUIREMENTS
Ensure that the IDS is fully integrated with the physical security and other elements of the overall facility security system. Except for multiple function keypads, other subsystems may be housed in a single enclosure. Specific subsystem functional requirements are as follows:

a. Detection subsystem: Subsystem shall consist of sensors to detect intrusion attempts and provide means to indicate a duress condition.
b. Arm/disarm multiple function keypad: Subsystem shall consist of electronic digital keypads to monitor and control personnel movement through normal access routes in and out of the facility and between protected areas within the facility.
c. Communications subsystem: Subsystem shall consist of elements required to ensure that pertinent data is transferred from the point of origin to the point where appropriate actions can be taken.
d. Assessment subsystem: Subsystem shall consist of electronic devices required to visually and audibly verify the validity of IDS alarms at two separate locations.
e. Alarm reporting subsystem: Subsystem shall consist of electronic devices to control, process, integrate, and annunciate IDS data at two separate locations.
f. Power subsystem: Subsystem shall consist of components required to ensure continuous operation of the entire IDS.

2.3 INTEGRATED SYSTEM PERFORMANCE REQUIREMENTS

The installed and operating IDS shall be integrated into the overall facility to detect intrusion and shall perform as an entity, as specified below.

2.3.1 Detection Coverage

Provide and adjust sensors so that coverage is overlapping and maximized without mutual interference. IDS coverage shall include the facility perimeter and critical spaces within the facility as indicated.

2.3.2 Detection Resolution (Sensitivity)

Sensitivity shall be capable of the following:

a. Locating intrusions at individually protected assets or at an individual portal;
b. Locating intrusions within volume/areas to within the coverage on any single volumetric sensor; and
c. Locating failures or tampering at individual sensors.

2.3.3 Detection Alarm and Reporting Capacity

The IDS shall have the capacity to collect, communicate, and display a minimum of 8 programmable sensor zone alarms and to enable control of one or more response devices in each of the sensor zones. When a sensor zone includes a combination of multiple detection devices, the system shall maintain the capability to identify individual detection devices in an alarm state. A single alarm shall be annunciated within approximately 2 seconds after sensor transducer or other detection device activation.

2.3.4 Alarms

Alarm shall include, but not be limited to, the following:

a. Intrusion detection
b. Tamper
c. Fail-safe
d. Line fault
e. AC power loss
f. Low battery in control communicator.

2.3.4.1 Intrusion Detection

Sense and respond with visible and audible signals the activation of detection sensors.

2.3.4.2 Tamper

Tamper protection can be physical protection, line supervision, encryption, and tamper alarming of enclosures and components. All intrusion detection, access control, assessment systems and their associated data transmission media must be protected commensurate with the classification of asset being protected. All intrusion detection sensors and access control readers must have tamper resistant enclosures and integral tamper protection switches. All enclosures, cabinets, housings, and boxes, having hinged doors or removable covers that contain processors or connections must have tamper protection switches. All tamper alarm signals must be monitored continuously whether the system is in the access or secure mode of operation. Tamper alarms shall be annunciated to be clearly distinguishable from intrusion detection alarms. Tamper switches on doors which must be opened to make normal maintenance adjustments to the system and to service the power supplies shall be of the push/pull-set, automatic-reset type. Tamper switches shall have the following features:

a. Inaccessibility until the switch is activated;
b. Under electrical supervision at all times, irrespective of the protection mode in which the circuit is operating;
c. Spring-loaded and held in the closed position by the door or cover protected; and
d. Wired to break the circuit when the door or cover is disturbed.

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

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

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

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

2.3.5.1 Primary Power
Furnish 120 volt AC service, transformed through a two-winding isolation transformer and rectified to low-voltage DC for system operation. Obtain primary power at the location indicated. Provide a circuit dedicated to power IDS from a panelboard at the location indicated. Label the circuit breaker in that panelboard: "Alarm System Do Not Turn Off."

2.3.5.2 Backup Power
Provide backup power to the primary power by dedicated batteries in remotely located system elements such as individual sensors and in control communicators. Batteries shall be capable of operation in any position and shall be protected against venting caustic chemicals or fumes within an equipment cabinet. Batteries shall also be capable of continuous operation for up to 8 hours without recharge or replacement. If the sensors power requirements exceed the allowable UL rated capacity of the control communicator battery, provide the number of separate power supplies required to power the sensors. Provide each power supply with its own rechargeable battery and charger.

2.4 SYSTEM PERFORMANCE REQUIREMENTS
Provide commercial of the shelf (COTS)system components compatible with base Lenel systems to operate as described herein within the context of the integrated system performance previously described. Where inconsistencies occur between the following component performance requirements and integrated system level performance descriptions, integrated system performance descriptions shall take precedence.

2.4.1 Modularity

Provide system components to facilitate modular subassembly and part replacement. Electronic components of the system shall be of the solid-state type, mounted on printed circuit boards conforming to UL 796. Circuitry shall not be so densely placed as to impede maintenance. Power-dissipating components shall incorporate safety margins of not less than 25 percent with respect to dissipation ratings, maximum voltages, and current-carrying capacity. Light duty relays and similar switching devices shall be solid-state or hermetically sealed electromechanical type.

2.4.2 Reliability
Provide only components in current manufacturing production. Components shall be manufactured to meet requirements specified herein and shall be free from characteristics and defects which affect appearance or serviceability or which render equipment unsuitable for the intended purpose. Provide components designed for continuous operation at specified conditions.

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

2.4.4 Environmental Conditions

2.4.4.1 Interior Conditions
Equipment installed in environmentally protected interior areas shall meet performance requirements specified by UL for the specific equipment or device.

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

2.4.6 Safety
IDS components shall conform to application rules and requirements of NFPA 70 and applicable Underwriters Laboratories publications.

2.4.7 Human Engineering
Aural considerations shall include location of annunciators, tone pitch, quality, and intensity. The number of different audible signals shall not exceed four. Component design shall provide for ease of accessibility for maintenance.

2.4.7.1 Visual Annunciators
Annunciators shall be either liquid crystal displays (LCDs) or light emitting diodes (LEDs). Annunciators shall be so connected in the circuit that failure of the annunciator, socket, or protective circuitry shall not result in an improper or indeterminate signal. LCDs and LEDs shall be compatible with standby power supplies. LEDs shall be brightly lit and visible from a distance of 30 feet in an area illuminated at 75 footcandles. LEDs shall be used in outdoor applications or in the presence of sunlight.

2.4.7.2 Controls
Provide to ensure ease of operation of specified characteristics. Where applicable, clockwise rotation of controls shall result in an increasing function. Controls, switches, visual signals, and indicating devices, input and output connectors, terminals, and test points shall be clearly marked or labeled on hardware to permit quick identification, intended use, and location. Terminal markings and labels shall be of a permanent and legible type and located to be visible when the associated system wiring is in place. Identification markings shall be associated with each adjustment device or item requiring periodic

maintenance. Safety warning or cautions shall be marked in conspicuous red letters. Control and indicator identifications that are exposed outside enclosures shall be permanent, machine-engraved letters, and painted to contrast with the background color. Controls not required for operation of the system shall be inaccessible to the system operator.

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

2.4.9 Component Enclosures
Annunciator housings, power supply enclosures, sensor control and terminal cabinets, control communicators, wiring gutters, and other component housings, collectively referred to as enclosures, shall be formed and assembled to be sturdy and rigid.

2.4.9.1 Metal Thickness
Thicknesses of metal in cast and sheet metal enclosures of all types shall not be less than those 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.

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

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

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

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

2.4.10 Detection Sensors
Sensors shall detect penetration of the facility perimeter and protected zones by unauthorized personnel or intruders, and shall conform to UL 634 or UL 639, as applicable. Unless otherwise specified, required sensor power shall be plus 12 volts DC.

2.4.10.1 Interior Point Sensors
a. Door open detection
(1) Surface mounted balanced magnetic switches: Provide balanced magnetic switches specified in Section 28 20 00.00 20 ELECTRONIC SECURITY SYSTEMS (ESS), COMMERCIAL.

2.4.10.2 Interior Volumetric (Space) Sensors
Passive infrared (PIR) sensors: Sensors shall detect intruder presence by monitoring the level of infrared energy emitted by objects within a protected zone. Sensor shall initiate an alarm upon observing increased or fluctuating infrared energy caused by the presence and motion of an intruder whose temperature is as little as 3 degrees F different from the background temperature. Sensor shall be passive in nature; no transmitted energy shall be required for detection. Sensor shall be sensitive to infrared energy emitted at wavelengths corresponding to the human body and other objects at ambient temperatures. Detection pattern for ceiling-mounted sensors shall be 360 degrees, unless otherwise indicated, and have a tamper resistant enclosure and integral tamper switch. Sensor shall provide some means of indicating an alarm condition during installation and calibration. A means of disabling the indication shall be provided within the sensor enclosure. Sensor shall alarm if an intruder moves within the area of protection more than 5 feet at a velocity of 0.1 foot per second, and one step per second, assuming 6 inches per step. Detection sensitivity shall be irrespective of the direction of motion. Sensor shall also alarm at velocities faster than 0.1 foot per second, up to 10 feet per second. Sensor optimum detection range shall be a minimum of 35 feet. Sensor shall not alarm in response to general area thermal variations. Sensor shall have RFI and white light immunity.

2.4.10.3 Duress Alarms
UL 639.
a. Hardwire duress alarms: Install at points within the protected area as indicated. Alarms shall be capable of being activated by the hand of an average adult in both standing position. Alarms shall not be visible or audible from the sensor. The alarm signal shall lock-in upon activation until manually reset with a key or similar device and shall be readily identifiable by the IDS. Sensors shall be easy to operate and designed to minimize the possibility of accidental activation. Hardwire duress alarms shall be rated for a minimum lifetime of 50,000 operations. Securely mount sensors in rugged, corrosion-resistant housing. Duress alarms shall be annunciated to be clearly distinguishable from other intrusion detection alarms at the control communicator.
b. Keypad activated duress alarms: Duress alarms shall consist of programmable keypad activated push buttons or a keypad activated Duress code, a user code programmed as a Duress code. Dedicated keys on the keypad shall be individually enabled via programming to initiate an alarm signal. Each programmed key shall also have the capability to initiate an auxiliary output for additional alarm signaling.

2.4.11 Communications
Communications shall link together the subsystems of the IDS. IDS communications links shall be via hardwire (cable). Communications links shall be supervised. Common communications interface devices shall be provided throughout the IDS. Sensor to Premise Control Unit (PCU) interface shall be by dry relay contact normally open or normally closed, except as specified otherwise. PCU to central alarm reporting Digital Receiver shall be digital, asynchronousor multiplexed data. The system shall be capable of communication using the IBM Synchronous Data Link Control format, and at least two other standard industry formats. The system shall be capable of supporting Network communication with digital dialer backup, existing Ethernet or token ring data networks, satellite communication, fiber optic networks, local area networks, wide area networks, cellular communication, and retail data networks. The PCU shall be capable of asynchronous network communication with a retry time between 3 and 15 seconds for a total of one (1) minute. If communication is unsuccessful the PCU shall be capable of attempting backup communication through any of the available communication methods to the same receiver or a backup

receiver. Network communication between the PCU and the receiver shall be in a proprietary communication format. The PCU shall be capable of supporting Dynamic Host Communication Protocol (DHCP) Internet Protocol (IP) addressing. Underwriters Laboratories (UL) shall list network communication by the PCU for Grade AA High-Line Security. The PCU shall be capable of two-way network communication using standard Ethernet 10BaseT in a LAN, WAN, or Internet configuration. The PCU shall be capable of communication by means of a 128 Bit AES Rijndael Encryption process certified by NIST (National Institute of Standards and Technology) to a Digital receiver with a built-in Encryption Alarm Router. The PCU shall be capable of meeting DCID 6/9 and UL 2050 standards. The PCU shall be capable of having communication set to Network operation. When a trap is set in Remote Link, the software shall be capable of sending a panel trap message with the panel account number to the Digital receiver. The digital receiver shall store the trap and monitor the PCU for the next message. When the PCU sends its next message, the receiver shall then send a message to the PCU to contact Remote Link at the IP address contained in the original trap message. The trap message shall be stored in the digital receiver for up to four hours. If the trap message is not sent to the PCU within the four-hour window, the PCU trap message shall be discarded and a new trap message must be sent from Remote Link.

2.4.11.1 Sensor to PCU Link Supervision

Provide hardwire direct current line supervision for sensor to PCU links which are within the IDS protected area. Circuit shall be supervised by monitoring changes in the current that flows through the detection circuit and a terminating resistor of at least 1.0 kohm. Supervision circuitry shall initiate an alarm in response to opening, closing, shorting, or grounding of the conductors by employing Class C, Standard Line Security. Class C circuit supervisor units shall provide an alarm response in the annunciator in not more than one second as a result of the following changes in normal transmission line current:

a. Five percent or more in normal line signal when it consists of direct current from 0.5 milliamperes 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 any 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 any element or elements of a complex signal upon which security integrity of the system is dependent. This tolerance will be applicable for frequencies above 100 Hz.

2.4.11.2 Control Communicator Hardwire Link

The control communicator to central alarm reporting processor communications link shall operate over a maximum of 2 standard voice grade telephone leased or proprietary lines. Digital communicator shall conform to UL 1635. The link shall be capable of operating half duplex over a Type 3002 data transmission pair and shall 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 shall be as follows:

a. Connections: Two- or four-wire
b. Impedance at 1000 Hz: 600 ohms
c. Transmitting level: 0 to 12 dBm
d. Transmitting level adjustment: 3 dB increments
e. Type: Data
f. Direction: Two-way alternate (half duplex)
g. Maximum speed: 1.2 kilobaud
h. Maximum loss at 1000 Hz: 33 dB.

2.4.12 Premise Control Unit (PCU)
PCU shall include a command processor installed in an attack and tamper resistant enclosure. The PCU shall be packaged and include a power transformer, battery(s), network connection cable, keypad(s), keypad connection cable(s) and additional components as required. All system electronic components shall be solid-state type, mounted on printed circuit boards. Light duty relays and similar switching devices shall be solid-state type or electromechanical. The PCU shall have an over current notification LED that lights when devices connected to the Keypad Bus or communication Bus(es) draw more current than the PCU is rated for. When the over current LED lights, the communications Bus(es) and Keypad bus are to shut down. The PCU shall provide at a minimum but not limited to, the following capabilities;
a. The PCU areas and zones shall be programmable, and the system shall store, log, display, and transmit specific custom designations for system areas, zones, and user names.
b. The PCU, user interfaces, zone input devices, relay output devices, and the signal receiving equipment shall be engineered, manufactured, assembled, and must be distributed from a location within the United States of America.
c. The system shall support user interaction by way of a keypad, web browser, system software, key switch, or radio frequency wireless control, using integrated or auxiliary devices provided by the system manufacturer.
d. The PCU shall support zone input connections, system keypads, system zone expansion modules, and wireless zone input modules, and must support zone input connections by way of at least two competitive products. The system shall offer a seamless integrated compatibility with hard-wire and/ or wireless zone expansion equipment for at least 200 wireless zones and/ or a maximum of 574 hardwired zones.
e. The PCU shall be capable of offering at least 5 zone expansion buses, each of which can support the connection of up to 15,000 feet of four-wire cable. Zone expansion and keypad data buses that exceed 2,500 feet of cable must include splitter/repeater modules to boost data voltage and maintain data integrity.
f. The PCU shall provide a seamless capability to provide a minimum of 500 addressable relays, which can be located at any connection location upon a zone expansion bus.
g. PCU relay outputs shall have the capability of being triggered as a result of a command from the user interface, changes in system status, changes in zone status, or by a programmable schedule.
h. PCU relay output states shall be programmable for momentary, maintained, pulsed, or must follow the state of an associated zone input.
i. The PCU shall be completely programmable remotely using remote annunciators, and/ or using upload/ download software that communicates using SDLC 300 baud, 2400 baud, or IP Addressed data network. On-site programming from a personal computer shall also be permitted.
j. The PCU shall be equipped with an anti-reversing circuit breaker to prevent damage due to accidental reversal of battery leads.

2.4.12.1 Input/Output Capacity
a. The PCU shall be capable of monitoring a maximum of 574 individual
zones and controlling a maximum of 502 output relays.
b. The PCU shall have, as an integral part of the assembly, 2 SPDT Form C relays rated at 1 Amp at 30 VDC and four open collector 12 VDC outputs rated at 50mA each. It shall also have the capacity of a maximum of 125 output expander modules with 500 switched ground, open collector outputs, 50mA maximum and 502 auxiliary relays (Form C rated at 1.0 Amp at 30 VDC).
c. The PCU shall also provide 100 programmable output schedules, and include an integral bell alarm circuit providing at least 1.5 Amps of steady, pulsed, or temporal bell output. Output type shall be programmable by zone type. Relays and voltage outputs shall be capable of being independently programmed to turn on and/or off at selected times each day.

2.4.12.2 User/Authorization Level Capacity
The system shall be capable of operation by 10,000 unique Personal

Identification Number (PIN) codes with each code having one 1 of ninety-nine 99 custom user profiles. This allows for limitation of certain functions to authorized users. The operation of all keypads shall be limited to authorized users.

2.4.12.3 Keypad

a. The PCU shall support a maximum of sixteen 16 keypads with alphanumeric display. Each keypad shall be capable of arming and disarming any system area based on a pass code or Proximity key authorization. The keypad alphanumeric display shall provide complete prompt messages during all stages of operation and system programming and display all relevant operating and test data.

b. Communication between the PCU and all keypads and zone expanders shall be multiplexed over a non-shielded multi-conductor cable, as recommended by the manufacturer. This cable shall also provide the power to all keypads, zone expanders, output expanders, and other power consuming detection devices.

c. If at any time a keypad does not detect polling, the alphanumeric display shall indicate "SYSTEM TROUBLE". If at any time two devices are programmed for the same address, the alphanumeric keypad shall display "4 WIRE BUS TROUBLE". If at any time a keypad detects polling but not for its particular address, the alphanumeric display shall indicate "NON POLLED ADDR". The system shall display all system troubles at selected keypads with distinct alphanumeric messages.

d. The keypad shall include self-test diagnostics enabling the installer to test all keypad functions: display test, key test, zone test, LED test, relay test, tone test, and address test.

e. The keypad shall provide an easy-to-read English text display. The text shall exactly match the text seen in all software reports and keypad displays.

f. The keypad user interface shall be a simple-to-use, menu-driven help system that is completely user friendly.

g. The PCU shall support sub-control keypads with four 4 built-in zones and capable of functioning in the following modes:

(1) Monitors all four 4 keypad zones independently with a maximum of 125 keypads attached to the PCU.

(2) PCU assigns one 1 zone to each keypad and monitors all keypad zones as a single zone with a maximum of 500 keypads attached to the PCU.

(3) Stand-alone mode allowing keypad to operate as a self-contained security system independent of the PCU.

2.4.12.4 Zone Configuration

a. A minimum of 4 Class B ungrounded zones shall be available at each keypad or zone expander on the system. The system shall have the capacity for a maximum of sixteen 16 keypads and a maximum of 125 four (4) zone expanders or 500 single zone expanders. It shall also have the capacity of a maximum of 125 supervised relay output expanders. All Class B zones shall be 2-wire, 22 AWG minimum, supervised by an end-of-line (EOL) device and shall be able to detect open and short conditions in excess of 500ms duration.

b. Each zone shall function in any of the following configurations: Night, Day, Exit, Fire, Supervisory, Emergency, Panic, Auxiliary 1, Auxiliary 2, Fire Verification, Cross Zone, Priority, and Key Switch Arming.

c. The digital SLCs and the annunciator/keypad bus shall be able to operate at a maximum wiring distance of 2500 feet from the control panel on unshielded, non-twisted cable. This distance may be extended to a total of 15,000 feet when bus repeater modules are installed.

d. The PCU shall have the capability to incorporate up to 200 zone expander points.

2.4.13 Chime

Provide chime for keypad audible indication of device activation. Audible chime shall sound when select devices activate in order to alert personnel of access into an area during normal access times. The audible chime may be activated when a magnetic switch is activated at a main entrance leading into a un-secured area during working hours.

2.4.14 Strobes
Provide for visual indication of alarm activation. Strobe shall flash and shall be 75 candela minimum with flash rate of 60 per minute. Strobe shall be designed to operate on 12 volts DC and shall conform to UL 1638.

2.4.15 Standalone Electronic Door Access
The PCU shall be capable of integrating area access control capability where specified into the same PCU with the ability to have up to 10,000 user credentials. User access is limited to custom profiles and/or schedules. Anti-passback shall be available. Networked version shall support a Two-Man Rule feature. The system shall support up to sixteen 16 access doors, connected to the system using a manufacturer-approved interface module. Access Control equipment shall communicate to the system by way of the PCU keypad bus.

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

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

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

PART 3 EXECUTION

3.1 EQUIPMENT INSTALLATION
UL 609, UL 639, UL 681 UL 1076 and UL 1610, and the appropriate installation manual for each equipment type. Components within the system shall be configured with appropriate "service points" to pinpoint system trouble in less than 20 minutes.

3.1.1 Cable/Wire Runs
NFPA 70; Section 26 20 00 INTERIOR DISTRIBUTION SYSTEM, and as specified herein.

3.1.2 Soldering
ASTM B32. For soldering electrical connections, use composition Sn60, for general purposes; use composition Sn62 or Sn63, for special purposes. Flux shall conform to ASTM B32.

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

3.1.4 Tamper Switches

Tamper switches shall be an integral part of all intrusion sensor devices. An initiation of an alarm signal will occur when the door or cover is moved as little as 1/4 inch from the normally closed position. Tamper switches shall also be Located within enclosures, cabinets, housings, boxes, raceways, and fittings to prevent direct line of sight to any internal components and to prevent tampering with switch or circuitry. Conceal tamper switch mounting hardware so that the location of the switch within the enclosure cannot be determined from the exterior.

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

3.2 FIELD QUALITY CONTROL

3.2.1 IDS Operational Test Plan
Test shall ensure that the requisite degree of intrusion detection is provided. Initially, test each sensor and subsystem component individually. Test glass breakage sensors by using test units supplied by the manufacturer which simulate glass breakage. When the function of each component within a particular subsystem, such as each sensor within a particular zone, is verified, certify that subsystem of the entire IDS has satisfactorily met the specifications. Test each subsystem similarly until each detection zone has been certified. When subsystem certification is complete, test the entire integrated system to ensure that subsystem elements are compatible and function as a complete system. The integrated system test shall be accomplished in linear fashion, end-to-end, and shall verify that each simulated intrusion performed within each detection zone produces an appropriate alarm or signal, and that alarm is correctly annunciated at the keypad. Provide for approval, not later than 30 days prior to formal inspection and test, a detailed operational test plan of how each component, subsystem, and entire IDS will be tested. When tests are complete and corrections made, submit a signed and dated certificate with a request for formal inspection and tests.

3.2.2 System Acceptance Test

3.2.2.1 Posted Operating Instructions
System Acceptance testing shall be performed as follows;
a. The NAVFAC and NAVFAC Engineer will conduct final acceptance testing of the system.
b. Prior to the final acceptance test, security contractor shall conduct a complete test of the entire IDS system and provide the NAVFAC and NAVFAC Engineer with a written report.
c. Following completion of the initial testing and correction of any noted deficiencies, conduct a five-day burn-in test, intent of the burn-in test shall be to prove the IDS by placing it in near real operating conditions. During this period the IDS shall be fully functional and programmed such that all points, interfaces, controls, reports, messages, prompts, etc. can be exercised and validated. Record and correct any system anomaly, deficiency, or failure noted during this period. Scheduling of the final acceptance test shall be based on a review of the results of this burn-in test.
d. Deliver a report describing the results of the functional tests, burn-in tests, diagnostics, calibrations, corrections, and repairs including written certification to the NAVFAC and NAVFAC Engineer that the installed complete IDS has been calibrated, tested, and is fully functional as specified herein.
e. Prior to the final acceptance test, complete all clean-up and patch work requirements. Security equipment closets and similar areas shall be free of accumulation of waste materials or rubbish caused by operations under the Contract At completion of the Work, remove all waste materials, rubbish, contractor tools, construction equipment, machinery and all surplus materials.
f. Upon written notification from the Contractor that the IDS is completely installed, integrated and operational, and the burn-in testing completed, the NAVFAC and NAVFAC Engineer will conduct a final acceptance test of the entire system at a mutually acceptable time.

g. During the final acceptance test, no adjustments, repairs or modifications to the system shall be conducted without the permission of the NAVFAC.
h. During the course of the final acceptance test by the NAVFAC and NAVFAC Engineer, the Contractor shall be responsible for demonstrating that, without exception, the completed and integrated IDS complies with the contract requirements. Physical and functional requirements of the project shall be demonstrated and shown. This demonstration will begin by comparing as-built drawings conditions of the IDS to requirements outlined in this Section, item by item. Following the Section compliance review, IDS and SCCd equipment will be evaluated.
i. The functionality of the various interfaces between systems will be tested.
j. The installation of all field devices will be inspected. This field inspection will weigh heavily on the general neatness and quality of installation, complete functionality of each device, and compliance with mounting, back box and conduit requirements.
k. All equipment shall be on and fully operational during any and all testing procedures. Provide personnel, equipment, and supplies necessary to perform all site testing. Provide a minimum of two Contractor employees familiar with the IDS for the final acceptance test. One contractor employee shall be responsible for monitoring and verifying alarms while the other will be required to demonstrate the function of each device. Supply at least two radios or portable telephones for use during the test.
l. The NAVFAC and NAVFAC Engineer retain the right to suspend, terminate or reschedule testing at any time when the IDS is found to be incomplete or fails to perform as specified. In the event that it becomes necessary to suspend, terminate or reschedule the test, all of the NAVFAC and NAVFAC Engineers fees and expenses related to the test shall be deducted from the Contractor's retainage. In the event it becomes necessary to suspend, terminate or reschedule the test, the Contractor shall work diligently to complete and/or repair all outstanding items as required by the Contract Documents. The Contractor shall supply the NAVFAC and NAVFAC Engineer with a detailed punch list completion schedule outlining task-by-task completion dates and a tentative date for a subsequent retest. During the final acceptance test, no adjustments, repairs or modifications to the system shall be conducted without the permission of the NAVFAC Engineer and NAVFAC.

3.3 ADJUSTMENT/ALIGNMENT/SYNCHRONIZATION/CLEANING
Subsequent to installation, clean each system component of dust, dirt, grease, or oil incurred during installation or accrued subsequent to installation from other project activities. Prepare for system activation by following manufacturer's recommended procedures for adjustment, alignment, or synchronization. Prepare each component in accordance with appropriate provisions of the component's installation, operations, and maintenance manuals.

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

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

(vii) **DATES AND PLACES OF DELIVERY AND ACCEPTANCE**: Vendor is responsible for transport of all components of the Intrusion Detection System (CLIN 0001) to the job site on the commencement date of Installation. Installation Site: Naval Weapons Station, Bldg C46, Earle, NJ. Installation shall begin on or before **19 September 2016** . Base access will be coordinated with Project Manager after award of contract.

(viii) DATE, PLACE, TIME OFFERES ARE DUE: Proposals are to be e-mailed to Beverly.Mayes.ctr@ncis.navy.mil by 9:00 am EST on August 31, 2016. For information regarding this solicitation contact Beverly Mayes at (571) 305-9292 or Beverly.Mayes.ctr@ncis.navy.mil and reference this combined synopsis/solicitation N6328516SUE045. All Questions shall be submitted in writing no later than 11:00 am EST 30 August 2016.

The following provision applies to this acquisition:

FAR 52-212-1 Instructions to Offerors - Commercial Items

FAR 52.212-2 Evaluation - Commercial Items: This provision is incorporated by reference, and paragraph (a) is modified to read as follows:

(a) This is a competitive best value source selection in which the Government will award a contract resulting from this solicitation to the responsible offeror whose offer conforming to the solicitation will be most advantageous to the Government, price, and other factors considered. The Installation Schedule will be significantly more important than price. The Government intends to award without discussions with respective offerors. The Government, however, reserves the right to conduct discussions if deemed in its best interest.

All offers will be ranked according to their Installation Schedule, and then will be evaluated by price and technical acceptability. The following listed are evaluation factors that shall be used in the evaluation process.

1. Installation Schedule: Installation must begin no later than 22 August 2016. For this requirement installation means the contractor will be onsite ready to begin work and all IDS equipment and components must be onsite.

2. Price

3. Technical Capability: Technical Acceptability is achieved when the offeror provides proof that their proposal meets the attached Statement of Work. Installers must be LENEL certified

(b) A written notice of award or acceptance of an offer, mailed or otherwise furnished to the successful offeror, shall result in a binding contract without further action by either party. Before the offer's specified expiration time, the Government may accept an offer (or part of an offer), whether or not there are negotiations after its receipt, unless a written notice of withdrawal is received before award.
(End of Provision)

The following FAR clauses apply to this acquisition:

FAR 52.236-2	Differing Site Conditions
FAR 52.236-3	Site Investigation and Conditions Affecting the Work
FAR 52.212-4	Contract Terms and Conditions - Commercial Items
FAR 52.212-5	Contract Terms and Conditions Required to Implement Statutes or Executive Orders - Commercial Items.

The following FAR clauses in paragraph (b) and paragraph (c) of FAR 52.212-5 are applicable:

Paragraph (b)

FAR 52.219-6	Notice of Total Small Business Aside,
FAR 52.219-13	Notice of Set-Aside of Orders,
FAR 52.219-28	Post Award Small Business Program Rerepresentation,
FAR 52.222-3	Convict Labor
FAR 52.222-19	Child Labor
FAR 52.222-21	Prohibition of Segregated Facilities,
FAR 52.222-26,	Equal Opportunity,
FAR 52.222-35	Equal Opportunity for Veterans,
FAR 52.222-36	Affirmative Action for Workers with Disabilities,
FAR 52.222-37	Employment Reports on Veterans,
FAR 52.222-40	Notification of Employee Rights Under the National Labor Relations Act
FAR 52.222-50	Combating Trafficking in Persons
FAR 52.223-18,	Encouraging Contractor Policies to Ban Text Messaging while Driving,
FAR 52.225-13	Restrictions On Certain Foreign Purchases,
FAR 52.232-33	Payment By Electronic Funds Transfer-System for Award Management.
FAR 52-225-13	Restrictions on Certain Foreign Purchases
FAR 52.236-14	Availability and Use of Utility Services.

Paragraph (c)

52-222-41	Service Contract Labor Standards
52.222-42	Statement of Equivalent Rates for Federal Hires
52.222-44	Fair Labor Standards Act and Service Contract Labor Standards – Price Adjustment

The following DFARS clauses cited are applicable to this solicitation:

DFARS 252.203-7000 Requirements Relating to Compensation of Former DoD Officials
DFARS 252.203-7002 Requirement to Inform Employees of Whistleblower Rights

DFARS 252.203-7997(Dev) Prohibition on Contracting with Entities that Require Certain Internal Confidentiality Agreements

DFARS 252.204-7003 Control of Government Personnel Work Product

DFARS 252.204-7004 System for Award Management

DFARS 252-204-7008 (Dev) Compliance with Safeguarding Covered Defense Information Controls

DFARS 252-204.7012 Safeguarding Covered Defense Information and Cyber Incident Reporting

DFARS 252.204-7015 Disclosure of Information to Litigation Support Contractors

DFARS 252.223-7008 Prohibition of Hexavalent Chromium

DFARS 252-225-7001 Buy American and Balance of Payments Program

DFARS 252-225-7002 Qualifying Country Sources as Subcontractors

DFARS 252.232-7003 Electronic Submission of Payment Request

DFARS 252.232-7006

DFARS 252.232-7010 Levies on Contract Payments

DFARS 252.244-7000 Subcontracts for Commercial Items

DFARS 252.247-7023 Transportation of Supplies by Sea - Basic