****
USACE / NAVFAC / AFCESA **UFGS-13702N (February 2004)**

Preparing Activity: NAVFAC **Superseding UFGS-13702N (September 1999)**

UNIFIED FACILITIES GUIDE SPECIFICATIONS

References are in agreement with UMRL dated 25 June 2004

Latest change indicated by CHG tags.
****

SECTION TABLE OF CONTENTS

DIVISION 13 - SPECIAL CONSTRUCTION

SECTION 13702N

BASIC INTRUSION DETECTION SYSTEMS (IDS)

02/04

-- End of Section Table of Contents --

****
USACE / NAVFAC / AFCESA	UFGS-13702N (February 2004)
Preparing Activity: NAVFAC	Superseding UFGS-13702N (September 1999)

UNIFIED FACILITIES GUIDE SPECIFICATIONS

References are in agreement with UMRL dated 25 June 2004

Latest change indicated by CHG tags.
****

SECTION 13702N

BASIC INTRUSION DETECTION SYSTEMS (IDS)
02/04

****
NOTE: This guide specification covers the requirements for basic intrusion detection systems (IDS).

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

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

Use of electronic communication is encouraged.

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

****
NOTE: This specification covers basic intrusion detection systems (IDS) consisting of commercial equipment which is limited to a full range of interior point protection devices, duress sensors, volumetric (space) protection sensors, alarm signal data communications media, and alarm reporting and monitoring systems. System requirements shall conform to NAVFAC DM-13.02, "Commercial Intrusion Detection Systems (IDS). For higher security IDS, CCTV, and access control systems, use Section 13703, "Commercial Intrusion Detection Systems (IDS)." If there are questions concerning system design, the Engineering Field Division (EFD), Naval Facilities Engineering Command, should be consulted.
****

****
NOTE: The following information shall be shown on

the project drawings:

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

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

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

4. Single line type electrical riser diagram.

5. Mounting: Details for each device required for complete installation. Include device height and installation of wiring.

****

PART 1 GENERAL

1.1 REFERENCES

****

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

****

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

ASTM INTERNATIONAL (ASTM)

ASTM A 123/A 123M	(2002) Zinc (Hot-Dip Galvanized) Coatings on Iron and Steel Products
ASTM B 32	(2003) Solder Metal

NATIONAL ELECTRICAL MANUFACTURERS ASSOCIATION (NEMA)

NEMA ICS 2	(2000) Industrial Controls and Systems: Controllers, Contactors, and Overload Relays Rated Not More than 2000 Volts AC or 750 Volts DC
NEMA ICS 6	(1993; R 2001) Industrial Control and Systems: Enclosures

NATIONAL FIRE PROTECTION ASSOCIATION (NFPA)

NFPA 70	(2002) National Electrical Code

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

47 CFR 15	Radio Frequency Devices

UNDERWRITERS LABORATORIES (UL)

UL 1449	(1996; Rev thru Jul 2002) Transient Voltage Surge Suppressors
UL 1610	(1998; Rev Aug 2001) Central-Station Burglar-Alarm Units
UL 1635	(1996; Rev thru Jul 1998) Digital Alarm Communicator System Units
UL 1638	(2001; Rev thru Nov 2003) Visual Signaling Appliances - Private Mode Emergency and General Utility Signaling
UL 365	(1997; Rev thru Aug 2001) Police Station Connected Burglary Alarm Units and Systems
UL 464	(2003; Rev thru Oct 2003) Audible Signal Appliances
UL 609	(1996; Rev thru Feb 1999) Local Burglar Alarm Units and Systems
UL 634	(2000) Connectors and Switches for Use with Burglar-Alarm Systems
UL 639	(1997; Rev thru Sep 2002) Intrusion Detection Units
UL 796	(1999; Rev thru Dec 2003) Printed-Wiring Boards

1.2 RELATED REQUIREMENTS

Section 16050N BASIC ELECTRICAL MATERIALS AND METHODS, applies to this section, with the additions and modifications specified herein.

1.3 DEFINITIONS

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 1220 mm 48 inches in height, 34

kg 75 pounds in weight and 0.113 cubic meter 4 cubic feet in volume, moving through protected zones or portals at a velocity of 30 to 3050 mm per second 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] [and] [modify existing] 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. [Existing system was manufactured by [_____], and new equipment shall be compatible with and shall operate accurately and reliably with existing system.] Include materials not furnished by the manufacturer with IDS equipment as specified in Section 16402 INTERIOR DISTRIBUTION SYSTEM.

1.5 SUBMITTALS

****

NOTE: Submittals must be limited to those necessary for adequate quality control. The importance of an item in the project should be one of the primary factors in determining if a submittal for the item should be required.

A "G" following a submittal item indicates that the submittal requires Government approval. Some submittals are already marked with a "G". Only delete an existing "G" if the submittal item is not complex and can be reviewed through the Contractor's Quality Control system. Only add a "G" if the submittal is sufficiently important or complex in context of the project.

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

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

****

Government approval is required for submittals with a "G" designation; submittals not having a "G" designation are [for Contractor Quality Control approval.][for information only. When used, a designation following the "G" designation identifies the office that will review the submittal for the Government.] The following shall be submitted in accordance with Section 01330 SUBMITTAL PROCEDURES:

[The [_____] will review and] [_____] Division, 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.

SD-02 Shop Drawings

IDS components[; G][; G, [_____]]

Overall system schematic[; G][; G, [_____]]

SD-03 Product Data

Interior point sensors[; G][; G, [_____]]

Interior volumetric (space) sensors[; G][; G, [_____]]

Control communicators[; G][; G, [_____]]

Duress alarms[; G][; G, [_____]]

Keypad[; G][; G, [_____]]

Communication cables[; G][; G, [_____]]

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

Communications interface devices[; G][; G, [_____]]

[Central station receiver/printer[; G][; G, [_____]]]

[Bell] [Siren][; G][; G, [_____]]

Batteries[; G][; G, [_____]]

Cipher lock system[; G][; G, [_____]]

Tamper switches[; G][; G, [_____]]

Strobes[; G][; G, [_____]]

SD-06 Test Reports

IDS operational test[; G][; G, [_____]]

IDS final test[; G][; G, [_____]]

SD-07 Certificates

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

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

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

IDS equipment[; G][; G, [_____]]

SD-10 Operation and Maintenance Data

IDS, Data Package 5[; G][; G, [_____]]

Submit in accordance with Section 01781 OPERATION AND MAINTENANCE DATA.

SD-11 Closeout Submittals

Posted operating instructions for IDS[; G][; 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 [420 by 297 mm] [_____] mm [11 by 17 inches] [_____] inches.

1.6.2 Experience and Qualifications

1.6.2.1 Installer's Qualifications

Prior to installation, submit data for approval by the [_____] Division, Naval Facilities Engineering Command, of the installer's experience and qualifications. Show that the installer who will perform the work has a minimum of [2] [_____] years' experience successfully installing IDS of the same type and design as specified herein. Include 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

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.

PART 2 PRODUCTS

2.1 IDS SUBSYSTEMS

Provide a complete integrated IDS 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.

[2.2.1 Intrinsically Safe

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

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

]2.3 INTEGRATED SYSTEM PERFORMANCE REQUIREMENTS

The installed and operating 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.]

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

****
NOTE: Select system capacity parameters based on specific facility design requirements. Include a 25 percent expansion factor to accommodate changes in design caused by reconfiguration of equipment within interior spaces or renovation.

****

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

****
NOTE: For a wireless transmission system delete "d. Line Fault."
****

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

****
NOTE: Each tamper loop requires a dedicated sensor zone in the control communicator. Do not use one tamper loop for an entire building since it would be difficult to trace the violated device or box. Instead, zone tamper loops by areas to more conveniently locate a violated device or box.
****

Enclosures, cabinets, housings, boxes, raceways, and fittings with hinged doors or removable covers which contain circuits of the intrusion detection system, sensor devices, and associated power supplies shall be provided with cover having corrosion-resistant tamper switches. 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 [from the line side of incoming facility power] [at the location indicated]. [Provide a separate, lockable, circuit breaker [adjacent to the power distribution panel] [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. [When radio frequency (RF) operation is required, batteries shall be an integral part of dispersed system elements.] Batteries shall be capable of operation in any position and shall be protected against venting caustic chemicals or fumes within an equipment cabinet. Batteries shall also be capable of continuous operation for up to [4] [_____] 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 system components 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.

2.4.4.2 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 ambient conditions specified by UL for the specific equipment or device.

2.4.4.3 Lightning and Power Surges

Intrusion detection, communication, and power circuits that lead to the control communicator shall be protected against lightning and voltage transients. Surge suppression device shall conform to UL 1449. Rated single pulse transient energy by metal oxide varistor (MOV) (10 times 1000 microseconds joules) shall be 300 in normal mode (line to neutral) and 280 in common mode (line and neutral to ground); maximum single pulse transient current by MOV (8 times 20 microseconds amperes peak) shall be 26,000 in both modes, for 120 volts AC circuits. Breakdown voltage shall be 240 volts DC; maximum clamping voltage shall be 287 volts DC peak; maximum transient current shall be 4500 (8 by 20 microseconds amperes peak by MOV, for communications circuits. The protective device shall be automatic and resettable and shall be active at all times. Fuses shall not be permitted as protection devices. Circuits shall be designed or selected assuming a maximum of 25 ohms to ground.

2.4.5 Electromagnetic Interference (EMI)

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

2.4.6 Electromagnetic Radiation (EMR)

****

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

****

Provide only IDS components which are [FCC] [_____] licensed and approved. Provide system components which are electromagnetically compatible.

2.4.7 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.

2.4.8 Safety

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

2.4.9 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.

2.4.9.1 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 9150 mm 30 feet in an area illuminated at 807 lx 75 footcandles. LEDs shall be used in outdoor applications or in the presence of sunlight.

2.4.9.2 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.

2.4.10 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

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.

2.4.11.1 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.

2.4.11.2 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 610 mm 24 inches with a single lock. Where the latch edge of a hinged door is 610 mm 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 the 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 the door is open, but shall be inaccessible when the door is closed.

2.4.11.5 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.

2.4.12 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.

2.4.12.1 Interior Point Sensors

****

NOTE: If a high level of security is required such as DCID 1/21, specify balanced magnetic switches (BMS) in Section 13703, "Commercial Intrusion Detection Systems."

****

a. Door and window open detection

(1) Balanced Magnetic Switches (BMS): Switches shall be [surface mounted] [recessed]. Switches shall have a balanced magnetic field with a high probability of alarm if an external magnet is introduced in defeat attempts. Provide each BMS with an overcurrent protective device, rated to limit current to 80 percent of switch capacity. BMS shall be rated for a minimum lifetime of one million operations. House BMS components in enclosures made of nonferrous materials.

(2) Surface mounted BMS: House components used in outdoor applications in weatherproof enclosures. The switch mechanism

shall have a minimum gap of [10] [19] mm [3/8] [3/4] inch and a maximum gap of [31.75] [63.5] mm [1 1/4] [2 1/2] inches without internal adjustment. [Surface mount BMS housing for the switch element shall have capabilities to receive threaded conduit.] The housing cover for surface mounted BMS, if made of cast aluminum, shall be secured by stainless steel screws. The magnet housing cover shall not be readily removable. [Protect the BMS housing from unauthorized access by a cover operated, corrosion-resistant tamper device. The device shall initiate an alarm when the cover is opened as little as 3.17 mm 1/8 inch and shall be inaccessible until actuated.] [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 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. The switch circuit shall initiate an alarm if a short circuit is applied to the door cord.]

(3) Recessed BMS: The recessed BMS shall have a gap up to 12.7 mm (9.5 mm in steel) (1/2 inch (3/8 inch in steel). Field adjustments in the fixed space between magnet and switch housing shall not be possible. [Ball bearing door trips shall be mounted within vault door headers such that when the locking mechanism is secured, the door bolt engages an actuator, mechanically closing the switch. The door bolt locking mechanism shall be completely engaged before the ball bearing door trip is activated. Provide circuit jumpers from the door.]

b. Glass breakage detection

(1) Breakwire sensors: Sensors shall consist of fine wire embedded in or affixed to the interior of the glazing. Breakage of protected glazing shall result in wire breakage. Wire shall be hard drawn copper and shall not exceed 26 AWG diameter. If affixed to glazing, protect the sensor wire by a clear coating which shall not inhibit sensor functioning. Sensor shall be terminated in insulated connectors which are [concealed] [tamper protected].

(2) Glass breakage sensors: Sensors shall detect window breakage by responding to sonic or vibration frequencies that accompany breaking glass. Sensors shall selectively filter input to detect only frequency of breaking glass and to minimize false alarms from sources such as jangling keys, ringing phones, and slamming doors. Glass breakage sensors shall initiate alarm when the glass they protect is cracked or broken. Sensors shall provide positive detection of breakage of plate, safety, laminated, and tempered glass. Sensor shall have a sensitivity adjustment controlling the output voltage from the detecting element which triggers a solid-state latching device. Provide the sensor with an LED for adjusting the sensitivity. [Sensor shall be contained in a fire-resistant ABS plastic housing and shall be mounted in contact with the window. Supply the sensor with a two-sided polyurethane tape with acrylic adhesive. Provide the sensor with an exterior label to protect the tape from direct sunlight.] [Sensor shall be

contained in a fire-resistant ABS plastic housing and shall be ceiling or wall mounted, as indicated. Sensor shall provide coverage of large glass areas up to 10 675 mm 35 feet wide. Sensor housing shall be tamper resistant and designed for screw mounting.] Sensor shall not initiate alarm in response to seismic vibrations or other ambient stimuli.

(3) Screening: Construct security screens from a maximum of 26 AWG insulated hard-drawn copper. Connect screens to an alarm circuitry by means of flexible armored cords. Security screen circuitry shall provide end-of-line resistors in series or equivalent methods ensuring alarm activation if short-circuiting of the screen is attempted. [If screen corners are not installed as a breakwire sensor (wire traps), provide tamper switches. Provide tamper switches in frames as required with not less than one switch on each side if dimensions are 610 mm 2 feet square or less, and two switches if dimensions exceed 610 mm 2 feet square. Tamper switches shall be corrosion resistant, spring operated, and shall initiate an alarm with a movement of 50 mm 2 inches or less and before access to the switch is possible. Electrical characteristics of the switch shall match alarm system requirements.]

c. Object protection

(1) Capacitance proximity sensor: Sensor shall consist of two solid-state synchronous oscillators, a reference oscillator, and a detecting oscillator. The detecting oscillator shall be electrically connected to the sensing wire (antenna) circuitry, such that the capacitance of the antenna circuitry determines the frequency and phase of oscillation. If an intruder approaches the protected objects, the oscillator shall detune with respect to the reference oscillator, initiating an alarm. The system shall provide means of indicating an alarm condition at the protected objects during installation and calibration. Provide the indicator with a disabling device within a tamperproof enclosure. The number of objects protected by a single capacitance detector shall not exceed the unit's maximum capacitance at the desired sensitivity. Protected objects shall be insulated from ground by insulating pads which shall have a dielectric constant such as glass or thermoplastic materials. [If screen grids or radiators are employed as antennas, insulate from ground. Wires used for grids shall be larger than No. 14 AWG, 30 percent copper-clad steel covered with a minimum of 0.397 mm 1/32 inch vinyl coating. Space grid elements at 150 mm 6 inches maximum, and construct in a symmetrical manner.] Provide sensor with sensitivity controls inaccessible to operating personnel. Sensor shall be insensitive to human body movements in excess of 915 mm 36 inches from the antenna circuit. Sensor sensitivity to alarm-producing stimuli shall be readily adjustable from contact to 915 mm 36 inches with a heavily gloved hand. Sensor shall not initiate nuisance alarms in response to normal ambient conditions. [Provide sensors with tamper switches. Interconnecting lines and tamper switches shall remain under constant supervision, even when the system is set for authorized access.] Sensor shall not reset upon restoration of SECURE mode if the antennas were altered during authorized entry to disable detection capability.

d. Floor, wall, and ceiling protection

(1) Vibration sensors: Sensors shall sense and selectively amplify signals generated by forced penetration of a protective structure. Sensors shall initiate alarms upon detecting drilling, cutting, or blasting through walls, or other methods of forced entry through a structure. Mount vibration sensors directly contacting the surface to be protected. Sensors shall be designed to give peak response to structurally conveyed vibrations associated with forcible attack on the protected surface. Provide at least one sensor on each monolithic slab or wall section, even though spacing closer than that required for midrange sensitivity may result. House sensors in protective mountings and fasten to the surface with concealed mounting screws or an epoxy. [Provide sensors with tamper switches.] Removal of a sensor from the surface shall initiate an alarm. An adjustable alarm discriminator shall function to prevent incidental vibrations which may occur from triggering the alarm circuit. Adjust the discriminator on the job to the precise needs of the application. Connect sensors to an electronic control unit by means of wiring or fiber optics cable run in [rigid steel conduit] [EMT]. Sensor sensitivity shall be individually adjustable unless sensor is designed to accommodate vibration ranges of the specific surface type on which it will be mounted. Sensitivity adjustments shall not be accessible without removing the cover on the sensor. Sensor shall not be responsive to airborne sound.

(2) Gridwire sensors: Provide strands of hard-drawn copper wire stapled to a wall, door, or ceiling and attached to a terminal strip enclosure. Enclosure shall be tamper switch protected both on the cover and with a pry-off tamper switch on the rear of the enclosure. When correctly arranged, installed, and connected into an electrically supervised detector circuit, the cutting, breaking, or grounding of gridwire shall initiate an alarm. Install gridwire in a pattern of 100 mm 4 inches on center over a wall, door, or ceiling area generally not exceeding 1220 by 2440 mm 4 by 8 feet in dimensions, for each terminal strip. Cover the grid pattern by a cosmetic material such as paneling. Hard-drawn gridwire used in fabricating security sensors shall not exceed 17.8 N 4 pounds tensile strength and shall be capable of carrying a current of 60 milliamperes at 60 volts with a temperature rise of not more than one degree C 2 degrees F. Wire shall not be larger than 26 AWG.

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

(3) Protection of utility inlet openings: Provide protection by a sensor of the [breakwire] [wire trap] type consisting of up to

26 AWG hard-drawn copper wire with a tensile strength of 17.8 N 4 pounds maximum interlaced throughout the opening such that no opening between wires shall be larger than 100 mm 4 inches on center. Terminate sensor so that attempts to cut the wire or otherwise enlarge openings between wires shall cause an alarm. Sensor termination shall be [concealed] [tamper protected].

2.4.12.2 Interior Volumetric (Space) Sensors

****
NOTE: Include a schedule of sensors on the plans when the size of areas and pattern coverage is different from one sensor to another.
****

a. 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 1.6 degrees C 3 degrees F different from the background temperature. Sensor shall be passive in nature; no transmitted energy shall be required for detection. Sensor shall be sensitive to infrared energy emitted at wavelengths corresponding to the human body and other objects at ambient temperatures. Detection pattern for wall-mounted sensors shall be 15 m by 15 m 50 ft by 50 ft, unless otherwise indicated[, and] [shall be housed in a tamper-alarmed enclosure]. Detection pattern for ceiling-mounted sensors shall be 6.28 rad 360 degrees, 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 if an intruder moves within the area of protection more than 1525 mm 5 feet at a velocity of 30 mm per second 0.1 foot per second, and one step per second, assuming 150 mm 6 inches per step. Detection sensitivity shall be irrespective of the direction of motion. Sensor shall also alarm at velocities faster than 30 mm per second 0.1 foot per second, up to 3050 mm per second 10 feet per second. Sensor optimum detection range shall be [a minimum of 10675 mm 35 feet] [as indicated]. Sensor shall not alarm in response to general area thermal variations. Sensor shall have RFI and white light immunity.

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

(1) Passive infrared (PIR) sensor section: Sensor shall detect intruder presence by monitoring the level of infrared energy emitted by objects within a protected zone. Sensor shall initiate an alarm upon observing increased or fluctuating infrared energy caused by the presence and motion of an intruder whose temperature is as little as 1.6 degrees C 3 degrees F different from the background temperature. Sensor shall be passive in nature; no transmitting energy shall be required for detection. Sensor shall be sensitive to infrared energy emitted at wavelengths corresponding to the human body or other objects at ambient temperatures. Sensor detection pattern shall be 15 m by 15 m 50

ft by 50 ft, unless otherwise indicated. Sensor shall have RFI and white light immunity.

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

(3) Additional dual technology sensor requirements: The enclosure containing two sensor sections shall be tamper alarmed. Both microwave and PIR sections shall activate simultaneously to generate an alarm. Only an intrusion characterized by volumetric motion and radiant body heat shall be detected. Sensor shall provide some means of indicating an alarm condition during installation and calibration. A means of disabling the indicator shall be provided within the sensor enclosure. Sensor shall alarm if an intruder moves within the area of protection more than 1525 mm 5 feet at a velocity of 30 mm per second 0.1 foot per second, and one step per second, assuming 150 mm 6 inches per step. Detection sensitivity shall be irrespective of the direction of motion. Sensor shall also alarm at velocities faster than 30 mm per second 0.1 foot per second, up to 3050 mm per second 10 feet per second. Sensor shall not alarm in response to general area thermal variations. Mount sensors [near the ceiling on vibration-free surfaces] [as indicated]. Electronic circuitry shall be solid state and mounted on printed circuit boards. Sensor elements shall contain circuitry for transmitter drive, signal processing, tamper circuitry, and power supplies. Circuitry shall provide an alarm relay with Form C contacts capable of carrying 2 amperes at 100 volts DC minimum.

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

d. Photoelectric sensors: Sensors shall detect intruder presence by

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

2.4.12.3 Duress Alarms

UL 639.

a. Hardwire duress alarms: Install at points within the protected area as indicated. Alarms shall be capable of being secretly activated by the foot or hand of an average adult in both standing and seated positions. Alarms shall not be visible or audible from the sensor. 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] [silent at the reporting location and clearly distinguishable from intrusion detection alarms at the central monitoring station].

b. Radio frequency duress alarms: Duress alarms shall consist of a compact and lightweight transmitter enclosed in a case that can be easily worn at the waist on a belt. Transmitter shall have a

unique identification code. Transmitter shall be capable of transmitting 2 watts of RF power. Transmitter shall transmit up to [500] [_____] times on the power provided by internal batteries. A small, flexible PVC-encased antenna shall be mounted 12.7 mm 1/2 inch away from the transmitter to ensure reliable propagation of the alarm signal and rotation of 6.28 rad 360 degrees without damage to the sensor. Provide transmitter in a corrosion-resistant case. Transmitter shall be available in both VHF and UHF radio bands. Transmitter shall be FM modulated to ensure reception and decoding of the alarm signal. The signal transmitted shall readily interface with the IDS communications subsystem as specified in paragraph entitled "Radio Frequency Link." Activation of the sensor shall be by hand-operated switch protected from accidental activation, yet easily activated by hand when worn at the waist on a belt. [Sensor activation shall be automatic when mounted on a belt and when the wearer is in a horizontal position for an adjustable time interval of longer than [1] [5] [15] [_____] minutes. Adjustment of time interval activation shall not be accessible to operations personnel.]

2.4.13 Communications

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

2.4.13.1 Sensor to Control Communicator Link Supervision

Provide hardwire direct current line supervision for sensor to control communicator 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.

2.4.13.2 Control Communicator Hardwire Link

The control communicator to central alarm reporting processor communications link shall operate over a maximum of [2] [4] [_____] 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] [5.12] [10.24] [_____] kilobaud

h. Maximum loss at 1000 Hz: 33 dB.

2.4.13.3 Radio Frequency Link

****

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

The 138 to 150.8 MHz band is the preferred range since specific frequencies in this range are reserved for DOD use. Frequencies in the 162 to 174 MHz and 450 to 470 MHz bands are shared with other users on a first-come, first-serve basis. To avoid potential contract delays, the frequency assignment should be included in the specification when

possible. For additional information, contact the base radio officer or the Naval Electromagnetic Spectrum Center at (202) 433-0689. OPNAVINST 2400.20E is issued by OPNAV Code N60 (previous Code OP941), telephone (703) 695-7284.

****

The system shall be a full duplex, supervised RF polling specifically designed for alarm data communications with components manufactured by one manufacturer. The system shall operate in the very high frequency (VHF), [134 to 154] [_____ to _____] MHz band. The system shall interface directly with the IDS hardwire data link from control communicator to the central alarm reporting location. The system shall also translate (reduce) the data rate for RF transmission, modulate and demodulate the data signal, and transmit and receive IDS data. Provide a factory-tested complete RF link which both automatically and upon operator command transmits a signal with a unique identification from the central alarm monitoring location to control communicator locations. Message receipt at control communicator location shall be ignored by other control communicators except the addressee. The communicator with the correct address shall decode the interrogation signal and respond to interrogation with status of reporting sensors. If the addressee fails to respond, reinterrogate. Failure to respond a second time shall cause a line supervision alarm. Remote units in the RF system shall be individually polled in turn. Polling response time and transmission data rate, data error rate, and equipment reliability shall ensure that overall IDS alarm annunciation time reliability is not degraded. Provide RF transmitters, receivers, or transceivers in sufficient quantities to meet specified requirements. RF link transmissions shall be on one or more of the frequencies within the specified band as required to meet the specified requirements and shall neither interfere with other IDS components nor facility electronic components. Provide transmitters which are in accordance with applicable requirements of 47 CFR 15. Message types and content shall be identical to those transmitted by other portions of the IDS data communications subsystem. IDS alarms sent by RF link shall not fail to be transmitted by RF link due to events occurring in "off air" periods. The RF link shall provide message transmission priority in the following order:

a. Intrusion alarms

b. Tamper alarms

c. Access denial alarms

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

Provide [omnidirectional, coaxial, half-wave dipole] [_____] antennas for alarm transmitters and transceivers with a driving point impedance to match transmission output. Antennas and antenna mounts shall be corrosion resistant and designed to withstand wind velocities of [161] [_____] km/h [100] [_____] mph and physical damage caused by vandalism. Antennas shall not be mounted to any portion of the facility fence or roofing system. Antennas shall be furnished from the same manufacturer as the rest of the RF link. Provide coaxial cable in lengths as required. Cable shall use PL-type fittings or connectors, properly protected against moisture. Cables shall match the output impedance of the transmitters.

2.4.14 Control Communicators

****
NOTE: Locate control communicator in secure, indoor, dry location. To determine the number of zones required for a specific project, consider the following as a minimum: one zone for entry/exit doors, one zone for window switches and doors that are not entry/exit type, one zone for motion sensors, one zone for glass break sensors, one or more zones for tamper, and one zone for duress alarm (if used). Increase the number of zones as the size of the building/area increases.
****

Control communicator shall be UL listed as Grade A Mercantile and Grade B Central Station and shall conform to UL 365, UL 609, or UL 1610, as applicable. Communicator shall provide for connection and control of IDS sensors and shall report status to multiple function keypads [and] [existing] [central alarm reporting unit]. Provide control communicator in a locked enclosure that is tamper protected so that openings cannot be created to defeat the system.

2.4.14.1 Functions

Each control communicator shall provide power and data interfaces to and control of a group of up to [8] [12] [_____] sensor zones and shall perform the following functions:

a. Continuously monitor the status (secure or alarm) of sensor zone status outputs connected to each control communicator zone input by monitoring the current through the end-of-line resistor.

b. Continuously supervise lines connecting each sensor zone status output to each control communicator zone input.

c. Retain activated sensor zones in memory. Display activated sensor zones. Require a command to be entered on keypad to clear memory.

2.4.14.2 Features

a. Multiple function keypad, suitable for remote mounting from the control communicator and having light emitting diode (LED) or liquid crystal display (LCD) readout of alarm and trouble conditions by zone. Alphanumeric English language display, with keypad programmability, and EE-PROM memory are preferred.

b. Trouble indications distinguishable from intrusion alarms.

c. Minimum of four zones selectable as fast/normal (50/750 milliseconds) for use with glass break, vibration, and shock detectors. Program glass break zones as "trouble" when disarmed and "alarm" when armed.

d. Minimum of four zones selectable as entry and exit or interior follower (time delayed interior zone when entry is gained through normal entry and exit point).

e. Distinct duress code, selectable as silent panic (does not sound

alarm on premises). Program as 24-hour alarm zone.

f. Complete system test activated at the keypad.

g. Capability for opening and closing reports to remote monitoring location.

h. Adjustable entry and exit delay times.

i. Integral battery charger.

j. Rechargeable 6 ampere-hour minimum sealed lead-acid battery.

k. Minimum of two relay outputs, fused.

l. Siren/bell output, fused and supervised.

m. Capability for a minimum of two multiple function keypads.

n. Capability to shunt or bypass selected interior zones while arming perimeter protection and remaining interior zones.

o. Capability for a minimum of seven assignable pass codes, keypad programmable from suppressed master code.

2.4.15 [Bell] [Siren]

****
NOTE: Choose one of the following options.
****

[a. Bell: Provide UL listed 255 mm 10 inch bell rated for 6 to 12 volts DC and having a sound output of 84 dB minimum. Bell shall conform to UL 464 and UL 609, as applicable. Provide bell in steel enclosed, weather-resistant box having tamper switches on front cover and on back of box.]

[b. Siren: Provide 30 watt, 8 ohm speaker and siren driver rated for 6 to 12 volts DC and having two distinct sound outputs. Siren shall produce a sound level output of 103 to 106 dB at 3050 mm 10 feet. Siren shall conform to UL 464 and UL 609, as applicable. Provide siren in metal enclosed, weather-resistant box having tamper switches on front cover and on back of box.]

2.4.16 Strobes

Provide for visual indication of alarm activation. Strobe shall flash simultaneously with [siren] [bell] 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.

2.4.17 Central Station Receiver/Printer

Provide a microprocessor based digital alarm receiver conforming to UL 1610 to receive and display information transmitted by alarm control panels/communicators over the standard telephone network. Receiver shall be capable of handling Ademco low or high speed, Sescoa, Radionics, and BFSK formats with either three- or four-digit subscriber identification and four plus two formats on the same line card. [Receiver shall also

interface to derived channel telephone company networks.] Receiver shall have built-in battery backup and shall be able to monitor a minimum of 999 accounts. Telephone connection shall be RJ31X jack. AC input shall have built-in MOV surge protection.

2.4.17.1 Printer

Printer shall conform to UL 1610 and shall provide a hard copy record of incoming information including time, date, account number, and code number. Printer shall have built-in battery backup and built-in MOV surge protection on AC input. Clock shall be 24-hour real time. Calendar shall be 100 year with leap years built in.

2.4.17.2 Operation

When the receiver receives a transmission over standard telephone network lines from a remote communicator, the receiver shall immediately answer the incoming call and acknowledge the call by returning a tone signal (handshake) to the communicator. Upon receipt of the handshake, the communicator shall transmit one or two rounds of coded pulses which are the account and code numbers. When a valid statement of data is received from the communicator, the receiver's internal audible signal shall sound to alert the monitoring person that a valid round of data is on line. The receiver shall also alert the printer and shall display on the receiver's front panel the account number and code number of the communicator. When the receiver has received the communicator's data, the receiver shall send a signal to the communicator causing the communicator to hang up (kiss off). The receiver shall then automatically shut itself down within 10 seconds.

2.4.18 Cipher Lock System

Coded door locks shall be the electronic type consisting of at least 10 coded buttons and a separate annunciator button for visitor operation. The system shall be such that at least four buttons shall have to be pressed in predetermined order to release the electric strike. The button array shall be the surface-mounted type and shall include a spyproof rim. The control cabinet shall include provisions for setting or changing the entry code without use of special tools or skills and shall contain a sound producing device for the annunciator button on the button array. The control cabinet shall include a battery pack and shall be designed to automatically switch to battery power when line power is interrupted. The battery pack shall be of the rechargeable type designed to be maintained at full charge by line power. Provide cipher lock system complete with mounting hardware, rim (surface) type electric strike specifically designed for the latching device specified and pre-finished cable for a complete and operational system. Design system to operate from a 120 volt AC power source and include conduit mounting provisions in the control box.

PART 3 EXECUTION

3.1 EQUIPMENT INSTALLATION

UL 609, UL 639, 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 16402 INTERIOR DISTRIBUTION SYSTEM, and as specified herein.

3.1.2 Soldering

ASTM B 32. For soldering electrical connections, use composition Sn60, for general purposes; use composition Sn62 or Sn63, for special purposes. Flux shall conform to ASTM B 32.

3.1.3 Galvanizing

Ferrous metal shall be hot-dip galvanized in accordance with ASTM A 123/A 123M. Screws, bolts, nuts, and other fastenings and supports shall be corrosion resistant.

3.1.4 Tamper Switches

Install tamper switches to initiate an alarm signal when the door or cover is moved as little as 6.35 mm 1/4 inch from the normally closed position. Locate tamper switches 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 Fungus Treatment

Completely treat system components for fungus resistance. Treating materials containing mercury-bearing fungicide shall not be used. Treating materials shall not increase the flammability of the material or surface being treated nor cause skin irritation or other personnel injury during fabrication, transportation, operation, or maintenance of the equipment, or during use of the finished items when used for the purpose intended.

3.1.6 Conduit

Install in accordance with NFPA 70 and Section 16402 INTERIOR DISTRIBUTION SYSTEM.

3.1.7 Underground Cable Installation

Underground conductors connecting protected structures and objects to the central alarm updating and display unit shall be run direct burial or in conduit as specified in Section 16302N UNDERGROUND TRANSMISSION AND DISTRIBUTION. Coaxial cable shall not be spliced. If permitted, cables connecting protected structures and objects to the security control console shall be sized such that initially only approximately 60 percent of the circuit pairs will be used. Cable pairs not used shall be reserved for future use of additional detection circuits.

3.2 FIELD QUALITY CONTROL

3.2.1 IDS Operational Test

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 [and central station receiver]. 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 Formal Inspection and Test

3.2.2.1 Final Inspection

[The Contracting Officer] [An authorized representative of the Contracting Officer of the [_____] Division, Naval Facilities Engineering Command,] will witness formal tests after receipt of written certification that preliminary tests have been completed and that the system is ready for final inspection. Repeat preliminary tests and functional and operational tests conducted, as requested by the Contracting Officer. Correct defects and conduct additional tests to demonstrate that the system conforms to this section.

3.2.2.2 Final Test

Test each sensor within a detection zone and then test the entire zone in accordance with applicable test procedures in the test plan for the sensors incorporated within that zone. As the test in that zone is proceeding, modifications or adjustments are prohibited. If, subsequent to the test, a modification or adjustment is necessary, retest the zone in the presence of the authorized representative of the Contracting Officer. Test other components individually within each subsystem. Component/subsystem failure shall require retesting after needed repairs or adjustments have been accomplished. In the interest of efficiency, major elements in a subsystem may be tested even if corrections for minor elements have not been completed. [When testing is complete, the test plan, together with procedures and data sheets, shall become the basis of the final acceptance report. The test report documents and verifies the Government's acceptance and approval of equipment and installation required by the contract.]

3.2.2.3 Fuses and Lamps

The Contractor is responsible for replacing blown fuses and burned out lamps during testing and will have on hand, prior to scheduling tests, not less than six spare lamps and fuses for each type, size, and rating of fuses and lamps used in the equipment provided under this section. Spare fuses and lamps not used during testing shall be turned over to the Contracting Officer.

3.2.2.4 Training Operating and Maintenance Personnel

Furnish instruction for operating staff in system operation and operator troubleshooting and preventive maintenance procedures. Instruction shall

consist of [one] [_____] man-day[s], 8 hours per day, and shall be held during normal duty hours. Commence instruction after the system is fully operational, and complete the instruction prior to system acceptance and turnover to the Government.

3.2.2.5 Posted Operating Instructions

Post IDS operating instructions as stated in Section 16050N BASIC ELECTRICAL MATERIALS AND METHODS.

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.

-- End of Section --