

SECTION 28 16 00
INTRUSION DETECTION SYSTEM

PART 1 - GENERAL

1.1 DESCRIPTION

- A. Provide and install an addition to the Intrusion Detection System, hereinafter referred to as IDS, as specified in this section.
- B. This Section includes the following:
 - 1. Intrusion detection with multiplexed, modular, microprocessor-based controls, intrusion sensors and detection devices, and communication links to perform monitoring, alarm, and control functions.
 - 2. Responsibility for integrating electronic and electrical systems and equipment is specified in the following Sections, with Work specified in this Section:
 - a. Division 28 Section "PHYSICAL ACCESS CONTROL".
 - b. Division 28 Section "VIDEO SURVEILLANCE".
- C. Related Sections include the following:
 - 1. Division 28 Section "VIDEO SURVEILLANCE" for closed-circuit television cameras that are used as devices for video motion detection.
 - 2. Division 28 Section "CONDUCTORS AND CABLES FOR ELECTRONIC SAFETY AND SECURITY" for cabling between central-station control units and field-mounted devices and controllers.

1.2 RELATED WORK

- A. Section 01 00 00 - GENERAL REQUIREMENTS. For General Requirements.
- B. Section 07 84 00 - FIRESTOPPING. Requirements for firestopping application and use.
- C. Section 10 14 00 - SIGNAGE. Requirements for labeling and signs.
- D. Section 26 05 11 - REQUIREMENTS FOR ELECTRICAL INSTALLATIONS. Requirements for connection of high voltage.
- E. Section 26 05 19 - LOW VOLTAGE ELECTRICAL POWER CONDUCTORS AND CABLES. Requirements for power cables.
- F. Section 28 05 00 - COMMON WORK RESULTS FOR ELECTRONIC SAFETY AND SECURITY. Requirements for general requirements that are common to more than one section in Division 28.
- G. Section 28 05 13 - CONDUCTORS AND CABLES FOR ELECTRONIC SAFETY AND SECURITY. Requirements for conductors and cables.
- H. Section 28 05 26 - GROUNDING AND BONDING FOR ELECTRONIC SAFETY AND SECURITY. Requirements for grounding of equipment.

- I. Section 28 05 28.33 - CONDUITS AND BACKBOXES FOR ELECTRONIC SAFETY AND SECURITY. Requirements for infrastructure.
- J. Section 28 08 00 - COMMISSIONING OF ELECTRONIC SAFETY AND SECURITY. Requirements for commissioning - systems readiness checklists, and training.
- K. Section 28 13 00 - PHYSICAL ACCESS CONTROL SYSTEMS (PACS). Requirements for physical access control integration.
- L. Section 28 23 00 - VIDEO SURVEILLANCE. Requirements for security camera systems.
- M. Section 28 31 00 - FIRE DETECTION AND ALARM. Requirements for integration with fire detection and alarm system.

1.3 QUALITY ASSURANCE

- A. The Contractor shall be responsible for providing, installing, and the operation of the IDS as shown. The Contractor shall also provide certification as required.
- B. The security system shall be installed and tested to ensure all components are fully compatible as a system and can be integrated with all associated security subsystems, whether the security system is stand-alone or a part of a complete Information Technology (IT) computer network.
- C. The Contractor or security sub-contractor shall be a licensed security Contractor as required within the state or jurisdiction of where the installation work is being conducted.

1.4 DEFINITIONS

- A. Controller: An intelligent peripheral control unit that uses a computer for controlling its operation. Where this term is presented with an initial capital letter, this definition applies.
- B. I/O: Input/Output.
- C. Intrusion Zone: A space or area for which an intrusion must be detected and uniquely identified, the sensor or group of sensors assigned to perform the detection, and any interface equipment between sensors and communication link to central-station control unit.
- D. LED: Light-emitting diode.
- E. NEC: National Electric Code
- F. NEMA: National Electrical Manufacturers Association
- G. NFPA: National Fire Protection Association
- H. NRTL: Nationally Recognized Testing Laboratory.
- I. SMS: Security Management System - A SMS is software that incorporates multiple security subsystems (e.g., physical access control, intrusion

detection, closed circuit television, intercom) into a single platform and graphical user interface.

J. PIR: Passive infrared.

K. RF: Radio frequency.

L. Standard Intruder: A person who weighs 45 kg (100 lb.) or less and whose height is 1525 mm (60 in) or less; dressed in a long-sleeved shirt, slacks, and shoes.

M. Standard-Intruder Movement: Any movement, such as walking, running, crawling, rolling, or jumping, of a "standard intruder" in a protected zone.

N. TCP/IP: Transport control protocol/Internet protocol incorporated into Microsoft Windows.

O. UPS: Uninterruptible Power Supply

P. UTP: Unshielded Twisted Pair

1.5 SUBMITTALS

A. Refer to Section 28 05 00, Part 1.

1.6 APPLICABLE PUBLICATIONS

A. The publications listed below (including amendments, addenda, revisions, supplement, and errata) form a part of this specification to the extent referenced. The publications are referenced in the text by the basic designation only.

B. American National Standards Institute (ANSI)/Security Industry Association (SIA):

PIR-01-00.....Passive Infrared Motion Detector Standard -
Features for Enhancing False Alarm Immunity

CP-01-00.....Control Panel Standard-Features for False Alarm
Reduction

C. Department of Justice American Disability Act (ADA)

28 CFR Part 36.....2010 ADA Standards for Accessible Design

D. Federal Communications Commission (FCC):

(47 CFR 15) Part 15.....Limitations on the Use of Wireless
Equipment/Systems

E. National Electrical Manufacturers Association (NEMA):

250-08.....Enclosures for Electrical Equipment (1000 Volts
Maximum)

F. National Fire Protection Association (NFPA):

70-11.....National Electrical Code

731-08.....Standards for the Installation of Electric
Premises Security Systems

G. Underwriters Laboratories, Inc. (UL):

464-09.....Audible Signal Appliances

609-96.....Local Burglar Alarm Units and Systems

634-07.....Standards for Connectors with Burglar-Alarm
Systems

639-07.....Standards for Intrusion Detection Units

1037-09.....Standard for Anti-theft Alarms and Devices

1635-10.....Digital Alarm Communicator System Units

H. Uniform Federal Accessibility Standards (UFAS), 19841.

1.7 COORDINATION

A. Coordinate arrangement, mounting, and support of intrusion detection
system equipment:

1. To allow maximum possible headroom unless specific mounting heights
that reduce headroom are indicated.
2. To provide for ease of disconnecting the equipment with minimum
interference to other installations.
3. To allow right of way for piping and conduit installed at required
slope.
4. So connecting raceways, cables, wireways, cable trays, and busways
will be clear of obstructions and of the working and access space of
other equipment.

B. Coordinate installation of required supporting devices and set sleeves
in cast-in-place concrete, masonry walls, and other structural
components as they are constructed.

C. Coordinate location of access panels and doors for electronic safety
and security items that are behind finished surfaces or otherwise
concealed.

1.8 EQUIPMENT AND MATERIALS

A. General

1. All equipment associated within the IDS shall be rated for
continuous operation. Environmental conditions (i.e. temperature,
humidity, wind, and seismic activity) shall be taken under
consideration at each facility and site location prior to
installation of the equipment.
2. All equipment shall operate on 120 or 240 volts alternating current
(VAC); 50 Hz or 60 Hz AC power system unless documented otherwise in

subsequent sections listed within this specification. All equipment shall have a back-up source of power that will provide a minimum of 96 hours of run time in the event of a loss of primary power to the facility.

3. The system shall be designed, installed, and programmed in a manner that will allow for ease of operation, programming, servicing, maintenance, testing, and upgrading of the system.
5. All equipment and materials for the system will be compatible to ensure functional operation in accordance with requirements.

1.9 WARRANTY OF CONSTRUCTION.

- A. Warrant IDS work subject to the Article "Warranty of Construction" of FAR 52.246-21.
- B. Demonstration and training shall be performed prior to system acceptance.

PART 2 - PRODUCTS

2.1 FUNCTIONAL DESCRIPTION OF SYSTEM

- A. Supervision: System components shall be continuously monitored for normal, alarm, supervisory, and trouble conditions. Indicate deviations from normal conditions at any location in system. Indication includes identification of device or circuit in which deviation has occurred and whether deviation is an alarm or malfunction.
 1. Alarm Signal: Display at central-station control unit and actuate audible and visual alarm devices.
 2. Trouble Condition Signal: Distinct from other signals, indicating that system is not fully functional. Trouble signal shall indicate system problems such as battery failure, open or shorted transmission line conductors, or controller failure.
 3. Supervisory Condition Signal: Distinct from other signals, indicating an abnormal condition as specified for the particular device or controller.
- B. System Control: Central-station control unit shall directly monitor intrusion detection units and connecting wiring.
- C. System Control: Central-station control unit shall directly monitor intrusion detection devices , perimeter detection units, , controllers associated with perimeter detection units, and connecting wiring in a multiplexed distributed control system or as part of a network.

- D. System shall automatically reboot program without error or loss of status or alarm data after any system disturbance.
- E. Operator Commands:
1. Help with System Operation: Display all commands available to operator. Help command, followed by a specific command, shall produce a short explanation of the purpose, use, and system reaction to that command.
 2. Acknowledge Alarm: To indicate that alarm message has been observed by operator.
 3. Place Protected Zone in Access: Disable all intrusion-alarm circuits of a specific protected zone. Tamper circuits may not be disabled by operator.
 4. Place Protected Zone in Secure: Activate all intrusion-alarm circuits of a protected zone.
 5. Protected Zone Test: Initiate operational test of a specific protected zone.
 6. System Test: Initiate system-wide operational test.
 7. Print Reports.
- F. Timed Control at Central-Station Control Unit: Allow automatically timed "secure" and "access" functions of selected protected zones.
- G. Automatic Control of Related Systems: Alarm or supervisory signals from certain intrusion detection devices control the following functions in related systems:
1. Switch selected lights.
 2. Open a signal path between certain intercommunication stations.
 3. Shift sound system to "listening mode" and open a signal path to certain system speakers.
 4. Switch signal to selected monitor from closed-circuit television camera in vicinity of sensor signaling an alarm.
- I. Response Time: 2 seconds between actuation of any alarm and its indication at central-station control unit.
- J. Circuit Supervision: Supervise all signal and data transmission lines, links with other systems, and sensors from central-station control unit. Indicate circuit and detection device faults with both protected zone and trouble signals, sound a distinctive audible tone, and illuminate an LED. Maximum permissible elapsed time between occurrence of a trouble condition and indication at central-station control unit

is 20 seconds. Initiate an alarm in response to opening, closing, shorting, or grounding of a signal or data transmission line..

- K. Programmed Secure-Access Control: System shall be programmable to automatically change status of various combinations of protected zones between secure and access conditions at scheduled times. Status changes may be preset for repetitive, daily, and weekly; specially scheduled operations may be preset up to a year in advance. Manual secure-access control stations shall override programmed settings.
- L. Manual Secure-Access Control: Coded entries at manual stations shall change status of associated protected zone between secure and access conditions.

2.2 SYSTEM COMPONENT REQUIREMENTS

- A. Compatibility: Detection devices and their communication features, connecting wiring, and central-station control unit shall be selected and configured with accessories for full compatibility with the following equipment:
 - 1. Data Gathering Panel, Output Module, Input Module, 28 13 00 PHYSICAL ACCESS CONTROL SYSTEM.
- B. Surge Protection: Protect components from voltage surges originating external to equipment housing and entering through power, communication, signal, control, or sensing leads. Include surge protection for external wiring of each conductor entry connection to components.
- C. Interference Protection: Components shall be unaffected by radiated RFI and electrical induction of 15 V/m over a frequency range of 10 to 10,000 MHz and conducted interference signals up to 0.25-V RMS injected into power supply lines at 10 to 10,000 MHz.
- D. Tamper Protection: Tamper switches on detection devices, controllers, annunciators, pull boxes, junction boxes, cabinets, and other system components shall initiate a tamper-alarm signal when unit is opened or partially disassembled and when entering conductors are cut or disconnected. Central-station control-unit alarm display shall identify tamper alarms and indicate locations.
- E. Self-Testing Devices: Automatically test themselves periodically, but not less than once per hour, to verify normal device functioning and alarm initiation capability. Devices transmit test failure to central-station control unit.

- F. Antimasking Devices: Automatically check operation continuously or at intervals of a minute or less, and use signal-processing logic to detect blocking, masking, jamming, tampering, or other operational dysfunction. Devices transmit detection of operational dysfunction to central-station control unit as an alarm signal.
- G. Addressable Devices: Transmitter and receivers shall communicate unique device identification and status reports to central-station control unit.
- H. Remote-Controlled Devices: Individually and remotely adjustable for sensitivity and individually monitored at central-station control unit for calibration, sensitivity, and alarm condition.

2.3 ENCLOSURES

- A. Interior Sensors: Enclosures that protect against dust, falling dirt, and dripping noncorrosive liquids.
- B. Interior Electronics: NEMA 250, Type 12.
- C. Screw Covers: Where enclosures are accessible to inmates, secure with security fasteners of type appropriate for enclosure.

2.4 EQUIPMENT ITEMS

- A. General:
 - 1. All requirements listed below are the minimum specifications that need to be met in order to comply with the IDS.
 - 2. All IDS sensors shall conform to UL 639, Intrusion Detection Standard.
 - 3. Ensure that IDS is fully integrated with other security subsystems as required to include, but not limited to, the CCTV, PACS, EPPS, and Physical Access Control System and Database Management. The IDS provided shall not limit the expansion and growth capability to a single manufacturer and shall allow modular expansion with minimal equipment modifications.
- B. IDS Components: The IDS shall consist of, but not be limited to, the following components:
 - 1. Control Panel
 - 2. Interior Detection Devices (Sensors)
 - 3. Power Supply
 - 4. Enclosures

2.5 CONTROL PANEL

- A. The Control panel shall be the main point of programming, monitoring, accessing, securing, and troubleshooting the IDS. Refer to American

National Standards Institute (ANSI) CP-01 Control Panel Standard-Features for False Alarm Reduction.

- B. The Control Panel shall provide a means of reporting alarms to a Physical Access Control System and Database Management via a computer interface or direct connection to an alarm control monitoring panel.
- C. The Control panel shall utilize a Multifunctional Keypad, Input and Output Modules for expansion of alarm zones, interfacing with additional security subsystems, programming, monitoring, and controlling the IDS.
- D. The Control panel shall meet or exceed the following minimum functional requirements for programming outputs, system response, and user interface:
 - 1. Programming Outputs:
 - a. 2 Amps alarm power at 12 VDC
 - b. 1.4 Amps auxiliary power at 12 VDC
 - c. Four alarm output patterns
 - d. Programmable bell test
 - e. Programmable bell shut-off timer
 - 2. System Response:
 - a. Selectable point response time
 - b. Cross point capability
 - c. Alarm verification
 - d. Watch mode
 - e. Scheduled events arm, disarm, bypass and un-bypass points, control relays, and control authority levels
 - 3. User Interface:
 - a. Supervises up to eight command points (e.g. Up to 16 unsupervised keypads can be used)
 - b. Provides custom keypad text
 - c. Addresses full function command menu including custom functions
 - d. Allows user authority by defined area and 16-character name
 - e. Provides for 14 custom authority control levels allowing user's authority to change, add, delete pass codes, disarm, bypass points, and start system tests.
 - 4. The Control panel shall meet or exceed the following technical characteristics:

Input Voltage via 110 VAC or 220 VAC Step-down Transformer	16 or 18 VAC
--	--------------

Operating Voltage	12 VDC
Output Voltage	12 VDC @ 2 A max
Direct Hardwire Zones	7
Partitions	8
Multifunctional Keypads	16 (2 per partition)
Communications Port	RJ-11

- E. A multifunctional keypad shall be utilized as a user interface for arming, disarming, monitoring, troubleshooting, and programming the alarm control panel.
- F. Keypads shall have the following features:
1. Multiple function keypads suitable for remote mounting, no greater than 1333 m (4000 ft), shall be provided from the control panel and have a light emitting diode (LED) readout of alarm and trouble conditions by zone.
 2. An alphanumeric English language display, with keypad programmability, and EE-PROM memory, shall also be provided.
 3. Trouble alarm indicators shall be distinguishable from intrusion alarms.
 4. A minimum of four (4) zones selectable as entry and exit with programmable time delay.
 5. Complete system test activated capability at the keypad.
 6. Capability for opening and closing reports to a remote monitoring location.
 7. Adjustable entry and exit delay times.
 8. Capability for a minimum of two (2) multiple function keypads.
 9. Capability to shunt or bypass selected interior zones while arming perimeter protection and remaining interior zones.
 10. Capability for a minimum of seven assignable pass-codes that are keypad programmable from a suppressed master code.
 11. The control panel shall have a communications port that will allow for communications with a computer for programming, monitoring, and troubleshooting purposes. The communications port will be, at a minimum, and RJ-11 or better.
 12. The control panel will have a systems success probability of 95% or better, and shall include the following success considerations:
 - a. False Alarm: Shall not exceed one (1) false alarm per 30 days per sensor zone.

- b. Nuisance Alarm: Shall not exceed a rate of one (1) alarm per seven (7) days per zone within the first 60 days after installation and acceptance. Sensor adjustments will be made and then shall not exceed one (1) alarm per 30 days.
- 13. The Control Panel will be able to detect either a line fault or power loss for all supervised data cables.
 - a. Line Fault Detection: Communication links of the IDS shall have an active mode for line fault detection. Fault isolation at the systems level shall have the same geographic resolutions as provided for intrusion detection. The line fault alarm shall be clearly distinguishable from other alarms.
 - b. Power Loss Detection: Provide the capability to detect when critical components experience temporary or permanent loss of power and annunciate to clearly identify the component experiencing power loss.

2.6 KEYPADS

A. Keypads shall meet or exceed the following technical characteristics:

Connections	4-wire flying lead for data and power
Operating Temperature	0°C to +50°C (+32°F to +122°F)
Display Window	8-point LED
Indicators: Illuminated keys	Armed Status-LED
	Point Status-LED
	Command Mode-LED
	Power-LED
Voltage	Nominal 12 VDC

2.7 INPUT MODULE

A. An input module shall be utilized to connect additional detection devices to the control panel. This module will meet or exceed the following technical characteristics:

Operating Voltage	8.5 to 14.5 VDC Nominal
Zone Inputs	Style A (Class B) Supervised
Operating Temperature	0 to 40 degrees C (32 to 140 degrees F)

2.8 OUTPUT MODULE

- A. An output module shall be utilized to interface the control panel with other security subsystems. The output module shall meet or exceed the following technical characteristics:

Operating Voltage	8.5 to 14.5 VDC Nominal
Output Relays	"Form C" Dry Relay Contracts
Relay Contact Rating	4A @ 24 VDC
	4A @ 24 VAC
	1A @ 70 VAC
Operating Temperature	0 to 40 degrees C F (32 to 140 degrees)

2.9 EXTERIOR DETECTION DEVICES (SENSORS): - NOT USED

2.10 INTERIOR DETECTION DEVICES (SENSORS)

- A. The IDS shall consist of interior, exterior, and other detection devices that are capable of:
1. Locating intrusions at individually protected asset areas or at an individual portal;
 2. Locating intrusions within a specific area of coverage;
 3. Locating failures or tampering of individual sensors or components.
- B. Provide and adjust for devices so that coverage is maximized in the space or area it is installed in. For large rooms where multiple devices are required, ensure device coverage is overlapping.
- C. Detection sensitivity shall be set up to ensure maximum coverage of the secure area is obtained while at the same time limiting excessive false alarms due to the environment and impact of small animals. All detection devices shall be anti-masking with exception of video motion detection.
- D. Dual sensor technology shall be used when possible. Sensor technology shall not be of the same type that is easily defeated by a single method. This will reduce the amount of false alarms.
- E. Interior Environmental Conditions: Systems shall be able to operate in environmentally protected interior areas and shall meet operational performance requirements for the following ambient conditions:
1. If components are installed in unheated areas they shall be able to operate in temperatures as low as -17 C (0 F);
 2. Interior Sensor Environmental Characteristics:

Temperatures	0 to 50 C (32F to 120 F)
--------------	--------------------------

Pressure	Sea Level to 4573m (15,000 ft.) above sea level
Humidity	5% - 95%
Fungus	Components of non-fungus nutrient materials
Acoustical Noise	Suitable for high noise environments above 100db

F. Balanced Magnetic Switches (BMS)

1. BMS switches shall be surface or recessed mounted according to manufacturer's instructions. Recessed mounted is the preferred method to reduce tampering or defeating of the system. Switches shall activate when a disturbance in the balanced magnetic field occurs.
2. Switches shall have a minimum of two (2) encapsulated reed switches.
3. Contractor shall provide each BMS with a current protective device, rated to limit current to 80% of the switch capacity.
4. Surface Mounted BMS: For exterior application, components shall be housed in weatherproof enclosures.
5. BMS 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.
6. BMS Technical Characteristics:

Maximum current	.25 amperes
Maximum voltage	30 VDC
Maximum power	3.0 W (without internal terminating resistors). 1.0 W (with internal terminating resistors).
Components	Three (3) pre-adjusted reed switches Three (3) pre-adjusted magnets
Output contacts	Transfer type SPDT
Contact rating	0.5 amperes, 28 VDC
Switch mechanism	Internally adjustable $\frac{1}{4}$ - $\frac{1}{2}$ in. (6-13 mm)
Wiring	Two (2) wires #22 American Wire Gauge (AWG), three (3) or 11 foot attached cable
Activation lifetime	1,000,000 activations
Enclosure	Nonferrous materials
Tamper alarm	Cover opened 3 mm (1/8 in.) and

activation	inaccessible until actuated
------------	-----------------------------

G. Passive Infrared Motion Sensors (PIR)

1. These sensors shall detect an intruder presence by monitoring the level of infrared energy emitted by objects within a protected zone and meet ANSI PIR-01 Passive Infrared Motion Detector Standards Features for Enhancing False Alarm Immunity. An alarm shall be initiated when motion and temperature changes within set patterns are detected as follows.
2. The detector shall provide multiple detection zones distributed at a variety of angles and distance.
3. Sensors shall be passive in nature; no transmitted energy shall be required for detection.
4. Sensors shall be sensitive to infrared energy emitted at wavelengths corresponding to human body and other objects at ambient temperatures.
5. Sensors shall not alarm in response to general area thermal variations and shall be immune to radio frequency interference.
6. Sensors shall not be susceptible to changes in temperature due to an air conditioner being turned on or off.
7. Sensors shall be housed in a tamper-alarmed enclosure.
8. Sensor detectors shall include motion analyzer processing, adjustable lens, and walk test LED's visible from any angle.
9. Sensors 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.
10. Sensor detectors shall include a motion monitoring verification circuit that will signal trouble or alarm if the detector fails to detect motion for an extended period.
11. PIR Technical Characteristics:

Power	Six (6) - 12 VDC 25 mA continuous current draw 38 mA peaks
Alarm Velocity	1500 mm (Five (5) ft.) at a velocity of 30 mm (0.1 ft.) per second, and one (1) step per second, assuming 150 mm (6 in.) per step. Also, faster than 30 mm (1 foot) per second, up to 3000 mm (10 feet) per second

Maximum detection range	10.6 m (35 ft.)
Frequency range- non activation or setup use	26 to 950 MHz using a 50 watt transmitter located 1 ft. from the unit or attached wiring
Infrared detection	1 1/2°C (3°F) different from the background temperature
Detection Pattern	180 degrees for volumetric units, non PIR 360
PIR 360°Detection Pattern	Programmable 60 detection zones including one directly below
Mounting	Ceiling and walls
Ceiling heights	2.4 m (Eight (8) ft.) - 5.4 m (18 ft)
Sensitivity adjustments	Three (3) levels

2.11 TAMPER ALARM SWITCHES

A. The following IDS sensors shall be used to monitor and detect potential tampering of sensors, control panels and enclosures.

1. Tamper Switches: All enclosures including cabinets, housings, boxes, raceways, and fittings with hinged doors or removable covers containing circuits and power supplies related to the IDS shall include corrosion-resistant tamper switches.
2. Tamper alarms shall be annunciated to be clearly distinguishable from IDS alarms.
3. Tamper switches will not be in a viewable from a direct line of sight perspective. The minimum amount of time the tamper switch becomes active and sends a signal after an enclosure is opened or panel removable is attempted, shall be one (1) second.
4. Tamper switches will initiate when enclosure doors or covers is removed as little as 6.35 mm (1/4 inch) from the closed position unless otherwise indicated. Tamper switches shall be:
 - a. Push/pull automatic reset type;
 - b. Inaccessible until switch is activated;
 - c. Spring-loaded and held in closed position by door or cover; and
 - d. Wired to break a circuit when door or cover is removed with each sensor annunciated individually at a central reporting processor.

5. Fail-Safe Mode: Shall provide the capability to detect and annunciate diminished functional capabilities and perform self-tests. Fail-safe alarms shall be annunciated to be clearly distinguishable from other types of alarms.

2.12 POWER SUPPLY

- A. A power supply shall only be utilized if the control panel is unable to support the load requirements of the IDS system.
- B. All power supplies shall be UL rated and able to adequately power two entry control devices on a continuous base without failure.
- C. Power supplies shall meet the following minimum technical characteristics:

INPUT POWER	110 VAC 60 HZ 2 amp
OUTPUT VOLTAGE	12 VDC Nominal (13.8 VDC) 24 VDC Nominal (27.6 VDC) Filtered and Regulated
BATTERY	Dependant on Output Voltage shall provide a minimum of 90 minutes, rechargeable
OUTPUT CURRENT	4 amp max. @ 13.8 VDC 3 amp max. @ 27.6 VDC
BATTERY FUSE SIZE	3.5 A @ 250 VAC
CHARGING CIRCUIT	Built-in standard

2.13 AUDIBLE AND VISUAL ALARM DEVICES

- A. Strobe: Xenon light complying with UL 1638, with a clear polycarbonate lens.
1. Light Output: 115 cd, minimum.
2. Flash Rate: 60 per minute.

2.14 SECURITY FASTENERS

- A. Security fasteners shall be operable only by tools produced for use on specific type of fastener by fastener manufacturer or other licensed fabricator. Drive system type, head style, material, and protective coating as required for assembly, installation, and strength.
- B. Drive System Types: Pinned Torx or pinned hex (Allen).
- C. Socket Flat Countersunk Head Fasteners:
1. Heat-treated alloy steel, ASTM F 835 (ASTM F 835M).
2. Stainless steel, ASTM F 879 (ASTM F 879M), Group 1 CW.
- D. Socket Button Head Fasteners:
1. Heat-treated alloy steel, ASTM F 835 (ASTM F 835M).

2. Stainless steel, ASTM F 879 (ASTM F 879M), Group 1 CW.
- E. Socket Head Cap Fasteners:
 1. Heat-treated alloy steel, ASTM A 574 (ASTM A 574M).
 2. Stainless steel, ASTM F 837 (ASTM F 837M), Group 1 CW.
- F. Protective Coatings for Heat-Treated Alloy Steel:
 1. Zinc chromate, ASTM F 1135, Grade 3 or 4; for exterior applications and interior applications where indicated.
 2. Zinc phosphate with oil, ASTM F 1137, Grade I, or black oxide.

PART 3 - EXECUTION

3.1 INSTALLATION

- A. IDS installation shall be in accordance with Underwriters Laboratories (UL) 639 Standards for Intrusion Detection Units and UL 634 Standards for Connectors with Burglar Alarm Systems, and appropriate manufacture's installation manuals for each type of IDS.
- B. Components shall be configured with appropriate "service points" to pinpoint system trouble in less than 30 minutes.
- C. The Contractor shall install all system components including VA furnished equipment, and appurtenances in accordance with the manufacturer's instructions and shall furnish all necessary connectors, terminators, interconnections, services, and adjustments required for a complete and operable system.
- D. The IDS will be designed, engineered, installed, and tested to ensure all components are fully compatible as a system and can be integrated with all associated security subsystems, whether the system is a stand alone or designed as a computer network.
- E. The IDS shall be able to be integrated with other security subsystems. Integration with these security subsystems shall be achieved by computer programming and the direct hardwiring of the systems. Determination for methodology shall be outlined when the system(s) is/are being designed and engineered. For installation purposes, the IDS shall utilize an output module for integration with other security subsystems. The Contractor will ensure all connections are per the OEM and that any and all software upgrades required to integrate the systems are installed prior to system start-up.
- F. For programming purposes, the Contractor shall refer to the manufacturer's requirements and Contracting Officer instructions for correct system operations. This includes ensuring computers being

utilized for system integration meet or exceeds the minimum system requirements outlined in the IDS software packages.

- G. Lightning and power surges to the central alarm reporting and display unit shall be protected at both ends against excessive voltages. This requirement shall apply for circuits that are routed both in underground conduits and overhead runs.
- H. At a minimum, the Contractor shall install primary detection devices, such as three electrode gas-type surge arresters, and secondary protectors to reduce dangerous voltages to levels that will cause no damage. Fuses shall not be permitted as protection devices.
- I. The Contractor shall provide fail-safe gas tube type surge arresters on exposed IDS data circuits. In addition, transient protection shall protect against spikes up to 1000 volts peak voltage with a one-microsecond rise time and 100-microsecond decay time, without causing false alarms. The protective device shall be automatic and self-restoring. Also, circuits shall be designed or selected assuming a maximum of 25 ohms to ground.
- J. Product Delivery, Storage and Handling:
 - 1. Delivery: Deliver materials to the job site in OEM's original unopened containers, clearly labeled with the OEM's name, equipment model and serial identification numbers, and UL logo. The Contracting Officer may inventory the IDS equipment at the time of delivery and reject items that do not conform to this requirement.
 - 2. Storage and Handling: Store and protect equipment in a manner that will preclude damage as directed by the Contracting Officer.
- K. Cleaning and Adjustments:
 - 1. Cleaning: Subsequent to installation, clean each system component of dust, dirt, grease, or oil incurred during installation in accordance to manufacture instructions.
 - 2. 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 instructions.
- L. Tamper Switches
 - 1. Install tamper switches to initiate an alarm signal when a panel, box, or component housing door or cover is moved as little as 6.35

mm (1/4 inch) from the normally closed position unless otherwise specified.

2. 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.
3. Conceal tamper switch mounting hardware so that the location of the switch within the enclosure cannot be determined from the exterior.

M. Unique IDS Installation Components:

1. BMS Surface Mounted:

- a. Surface mounted BMS housing for the switch element shall have the capability to receive threaded conduit. Housing covers for surface mounted BMS, if made of cast aluminum, shall be secured by stainless steel screws. Magnet housing cover shall not be readily removable and BMS housings shall be protected from unauthorized access by a cover operated, corrosion-resistant tamper device.
- b. Conductors running from a door to alarm circuits shall be contained 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. Conductors and the armored cord shall experience no mechanical strain as the door is removed from fully open to closed position. Switch circuits shall initiate an alarm if a short circuit is applied to the door cord.
- c. For exterior application on double gates, both BMS elements must be mounted on the gate. Flexible armored cord constructed from corrosion-resistant metal shall be used to provide electrical connection.

2. BMS Recessed Mounted:

- a. 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.
- b. Door bolt locking mechanisms shall be fully engaged before the ball bearing door trip is activated. Also, circuit jumpers from the door shall be provided.

4. Passive Infrared Detectors: (PIR)

- a. The protective beam shall be focused in a straight line.
- b. Installed beam distance from transmitter to receiver shall not exceed 80% of the manufacturer's maximum recommended rating.
- c. Mirrors may be used to extend the beam or to establish a network of beams. Each mirror used shall not lower the rated maximum system range by more than 50%.
- d. Mirrors and photoelectric sources used in outdoor applications shall have self-heating capability to eliminate condensation and shall be housed in weatherproof enclosures.

3.2 WIRING INSTALLATION

- A. Wiring Method: Install wiring in metal raceways according to Section 28 05 28.33 "CONDUITS AND BACKBOXES FOR ELECTRONIC SAFETY AND SECURITY." Conceal raceway except in unfinished spaces and as indicated. Minimum conduit size shall be 3/4 inch (20 mm). Control and data transmission wiring shall not share conduit with other building wiring systems.
- B. Wiring Method: Install wiring in raceways except in accessible indoor ceiling spaces and in interior hollow gypsum board partitions where cable may be used. Conceal raceways and wiring except in unfinished spaces and as indicated. Minimum conduit size shall be 3/4 inch (20 mm). Control and data transmission wiring shall not share conduit with other building wiring systems.
- C. Wiring Method: Cable, concealed in accessible ceilings, walls, and floors when possible.
- D. Wiring within Enclosures: Bundle, lace, and train conductors to terminal points. Use lacing bars and distribution spools. Separate power-limited and non-power-limited conductors as recommended in writing by manufacturer. Install conductors parallel with or at right angles to sides and back of enclosure. Connect conductors that are terminated, spliced, or interrupted in any enclosure associated with intrusion system to terminal blocks. Mark each terminal according to system's wiring diagrams. Make all connections with approved crimp-on terminal spade lugs, pressure-type terminal blocks, or plug connectors.
- E. Wires and Cables:
 - 1. Conductors: Size as recommended in writing by system manufacturer, unless otherwise indicated.

2. 120-V Power Wiring: Install according to Division 26 Section "LOW-VOLTAGE ELECTRICAL POWER CONDUCTORS AND CABLES," unless otherwise indicated.
3. Control and Signal Transmission Conductors: Install unshielded, twisted-pair cable, unless otherwise indicated or if manufacturer recommends shielded cable, according to Division 28 Section "CONDUCTORS AND CABLES FOR ELECTRONIC SAFETY AND SECURITY."
4. Computer and Data-Processing Cables: Install according to Division 28 Section "CONDUCTORS AND CABLES FOR ELECTRONIC SAFETY AND SECURITY."
5. Television Signal Transmission Cables: Install according to Division 28 Section "CONDUCTORS AND CABLES FOR ELECTRONIC SAFETY AND SECURITY."
- F. Splices, Taps, and Terminations: Make connections only on numbered terminal strips in junction, pull, and outlet boxes; terminal cabinets; and equipment enclosures.
- G. Install power supplies and other auxiliary components for detection devices at controllers, unless otherwise indicated or required by manufacturer. Do not install such items near devices they serve.
- H. Identify components with engraved, laminated-plastic or metal nameplate for central-station control unit and each terminal cabinet, mounted with corrosion-resistant screws.

3.3 GROUNDING

- A. Ground system components and conductor and cable shields to eliminate shock hazard and to minimize ground loops, common-mode returns, noise pickup, cross talk, and other impairments.
- B. Signal Ground Terminal: Locate at main equipment rack or cabinet. Isolate from power system and equipment grounding.
- C. Install grounding electrodes of type, size, location, and quantity indicated. Comply with installation requirements in Division 28 Section "GROUNDING AND BONDING FOR ELECTRONIC SAFETY AND SECURITY SYSTEMS."

3.4 STARTUP AND TESTING

- A. The Commissioning Agent will observe startup and contractor testing of selected equipment. Coordinate the startup and contractor testing schedules with the Contracting Officer's Representative (COR) and Commissioning Agent. Provide a minimum of 7 days prior notice.

3.5 COMMISSIONING

- A. Provide commissioning documentation in accordance with the requirements of Section 28 08 00 - COMMISSIONING OF ELECTRONIC SAFETY AND SECURITY SYSTEMS for all inspection, start up, and contractor testing required above and required by the System Readiness Checklist provided by the Commissioning Agent.
- B. Components provided under this section of the specification will be tested as part of a larger system. Refer to Section 28 08 00 - COMMISSIONING OF ELECTRONIC SAFETY AND SECURITY SYSTEMS and related sections for contractor responsibilities for system commissioning.

3.6 TESTS AND TRAINING

- A. All testing and training shall be compliant with the VA General Requirements, Section 01 00 00, GENERAL REQUIREMENTS.
- B. Provide services of manufacturer's technical representative for four hours to instruct VA personnel in operation and maintenance of units.
- C. Submit training plans and instructor qualifications in accordance with the requirements of Section 28 08 00 - COMMISSIONING OF ELECTRONIC SAFETY AND SECURITY SYSTEMS.

-----END-----