



Designation: D8218 – 20

Standard Guide for Intrusion Detection System (IDS)¹

This standard is issued under the fixed designation D8218; the number immediately following the designation indicates the year of original adoption or, in the case of revision, the year of last revision. A number in parentheses indicates the year of last reapproval. A superscript epsilon (ε) indicates an editorial change since the last revision or reapproval.

1. Scope

1.1 This guide covers the recommended intrusion detection system (IDS) for protecting resin cannabis, resin cannabis products, resin cannabis waste, currency, people, property, and assets.

1.2 *Units*—The values stated in inch-pound units are to be regarded as standard. The values given in parentheses are mathematical conversions to SI units that are provided for information only and are not considered standard.

1.3 *This standard does not purport to address all of the safety concerns, if any, associated with its use. It is the responsibility of the user of this standard to establish appropriate safety, health, and environmental practices and determine the applicability of regulatory limitations prior to use.*

1.4 *This international standard was developed in accordance with internationally recognized principles on standardization established in the Decision on Principles for the Development of International Standards, Guides and Recommendations issued by the World Trade Organization Technical Barriers to Trade (TBT) Committee.*

2. Terminology

2.1 Definitions of Terms Specific to This Standard:

2.1.1 *beam alarm, n*—electronic device that detects any interruption to the signal between a transmitter and receiver.

2.1.2 *contact alarm, n*—activated when the device is separated, such as opening.

2.1.3 *duress code, n*—code that, when entered, generates a silent alarm signal indicating that a person is being forced to turn off the alarm, also known as a holdup alarm.

2.1.4 *failure notification, n*—provides an audible, text, or visual notification of any failure in the systems.

2.1.5 *glass break, n*—audio sensor to pick up the actual frequency of broken glass.

2.1.6 *holdup alarm, n*—device activated to signal a robbery in progress, which shall generate a silent alarm.

2.1.7 *Internet protocol, IP, n*—data sent over the Internet or other network.

2.1.8 *intrusion detection system, IDS, n*—motion detection, door and window contact alarm, and glass-break sensor.

2.1.9 *motion detection, n*—passive infrared to survey the area and sounds an audible notification alarm when a person or object moves into the protected space.

2.1.10 *panic alarm, n*—keypad code, button, or device for use in a life-threatening or emergency situation that shall be manually activated in any emergency when security, police, or fire response is needed.

2.1.11 *perimeter alarm, n*—outdoor alarms including fence detection, underground cable, microwave and infrared sensors.

2.1.12 *two-factor authentication, n*—at least two of the following: an access control credential (for example, badge, FOB, wireless device), personal identification number (PIN), or biometric, or combinations thereof.

2.1.13 *uninterruptible power supply, UPS, n*—ensure continuous operation of the IDS using a surge protector with a built-in backup battery.

3. Significance and Use

3.1 The intrusion detection system (IDS) safeguards various areas considered critical to operations. Intrusion detection devices include but are not limited to, door or window contact alarms that are activated when the device is separated, such as opening; and motion detection technology that uses a passive infrared to survey the area and sounds an audible notification alarm when a person or object moves into the protected space. Also included are glass-break detectors that use an audio sensor to pick up the actual frequency of broken glass. If the glass-break detector “hears” broken glass, an alarm is activated. If any of the devices are triggered when the system is armed, an alert is sent to a 24-h monitoring area for notification.

4. Summary of Guide

4.1 The following intrusion detection system (IDS) technologies, equipment, capabilities, and procedures are industry best-practice-based.

¹ This guide is under the jurisdiction of ASTM Committee D37 on Cannabis and is the direct responsibility of Subcommittee D37.05 on Security and Transportation. Current edition approved Feb. 1, 2020. Published February 2020. DOI: 10.1520/D8218-20.

4.1.1 An on- or off-site monitoring station designed to manage and monitor all intrusion detection information, along with receiving and sending notifications of all alarm activations.

4.1.2 Using intrusion detection technology, select personnel with designated backups are able to monitor and assign appropriate access.

4.1.3 The IDS should have the following capabilities among others: motion detection, door and window contact alarms, glass-break sensors, and perimeter alarms.

4.1.4 A duress code, when entered, generates a silent alarm signal indicating when a person is being forced to turn off the alarm. Also known as a holdup alarm, it can be activated to signal a robbery in progress, which will generate a silent alarm.

4.1.5 A panic alarm code, button, or device for use in a life-threatening or emergency situation that will be activated in any emergency when security, police, or fire response is needed and personnel cannot use any other form of communication to request assistance. A panic alarm will generate an audible security alarm signal in the facility and can also notify law enforcement.

4.1.6 A notification system for alarm activations, including audible alarms, telephone, cell phone, text message, and e-mail, can notify monitoring personnel, law enforcement, public safety, or emergency services agencies.

4.1.7 An electronic, mechanical, or another device capable of being programmed to send a prerecorded voice message, when activated over a telephone line, radio, or other communication system, can notify monitoring personnel, law enforcement, public safety, or emergency services agencies.

4.1.8 A failure notification system provides an audible, text, or visual notification of any failure in the systems. The failure notification system is sent by telephone, e-mail, or text message as an alert to monitoring personnel within 5 min of failure.

4.1.9 Access doors that are not solely controlled by an electronic access panel that prevents locks from becoming released during a power outage.

4.1.10 An alarm control panel installed in a secured room with limited access requires two-factor authentication for entry (at least two of the following): an access control credential (for example, badge, FOB, wireless device), personal identification number (PIN), or biometric.

4.1.11 The IDS will send alarm signals and upload/download via Internet protocol (IP) or hardwire connection, or both, specific zones of protection, graphic keypad support, and dual partitions or hardwire, or both. Options include a wireless device to operate the system remotely and receive alarm notifications immediately.

4.1.12 To bridge the short time period between power loss and switch to a generator system, an uninterruptible power supply (UPS) ensures continuous operation of the IDS.

5. Policies and Procedures

5.1 Policies and procedures specifying instructional requirements applicable to the IDS to protect resin cannabis and currency, such as roles and responsibilities for responding to an alarm, and notification protocols for alarm activation.

5.2 A complete index and guide to the hardware, software, devices, technical documentation, monitors, and controls should be available either in hardcopy or electronic form.

5.2.1 This guide should include a map of the alarm locations, direction of coverage, device numbers, and operating instructions for the intrusion detection equipment.

6. Maintenance Requirements

6.1 The IDS should be maintained in good working order at all times.

6.2 Conduct and document monthly maintenance inspections to ensure that any repairs, alterations, or upgrades are made for proper operation of the system.

6.3 Designated personnel oversee the functioning of the system and need to report immediately any malfunctioning or technical problems.

6.4 The system conducts a self-test when set and identifies attempted sabotage of the system.

6.5 All security equipment is inspected, tested, and documented at regular intervals, not to exceed 30 calendar days from the previous inspection, and tested to ensure the systems remain functional.

6.6 All maintenance records shall be maintained for a period of time in compliance with applicable regulatory standards.

7. Monitoring and Notification

7.1 If any of the IDS sensors are triggered when the alarm is armed, 24 h per day, seven days per week, monitoring station either on- or off-site, or both, should be notified. The monitoring station should have connectivity with all IDS alarm devices, including both a panic alarm, which will immediately sound an audible alarm notification, and a duress or holdup alarm, which will generate a silent alarm.

7.2 The IDS is monitored at all times by personnel who determine the appropriate steps to be taken in response to an attempted or actual unauthorized access or tampering with the system.

7.3 Monitoring personnel should record the date, time, and location of an IDS alarm activation as well as all measures taken in response including notifications, such as law enforcement, public safety, or emergency services agencies.

7.4 The IDS is capable of monitoring individuals and activities and coverage of all enclosed areas, unless prohibited by law, including all points of entrances to and exits from the facility.

7.5 IDS devices should be positioned in and around the property including, but not limited to, loading docks, transaction areas, storage rooms; vaults; offices; areas in which product is grown, processed, manufactured, stored, handled, inventoried, sold, delivered, transported, or destroyed; rooms with exterior windows, roof hatches or skylights; rooms that contain equipment, product, currency, drop boxes, safes, vaults, data, and proprietary records.