junction box or controller will enable an unauthorized modification, tamper protection should be provided.

5. *System Requirements*

a. *Independent Equipment.* When many alarmed areas are protected by one monitor station, secure room zones must be clearly distinguishable from the other zones to facilitate a priority response. All sensors shall be installed within the protected area.

b. *Access and/or Secure Switch and PCU:* No capability should exist to allow changing the access status of the IDS from a location outside the protected area. All PCUs must be located inside the secure area and should be located near the entrance. Assigned personnel should initiate all changes in access and secure status. Operation of the PCU may be restricted by use of a device or procedure that verifies authorized use. In the secure mode, any unauthorized entry into the space shall cause an alarm to be transmitted to the monitor station.

c. *Motion Detection Protection:* Secure areas that reasonably afford access to the container or where classified data is stored should be protected with motion detection sensors; e.g., ultrasonic and passive infrared. Use of dual technology is authorized when one technology transmits an alarm condition independent from the other technology. A failed detector shall cause an immediate and continuous alarm condition.

d. *Protection of Perimeter Doors:* Each perimeter door shall be protected by a balanced magnetic switch (BMS) that meets the standards of UL 634.

e. *Windows:* All readily accessible windows (within 18 feet of ground level) shall be protected by an IDS, either independently or by the motion detection sensors in the space.

f. *IDS Requirements for Continuous Operations Facilities:* A continuous operations facility may not require an IDS. This type of secure area should be equipped with an alerting system if the occupants cannot observe all potential entrances into the room. Duress devices may also be required.

g. *False and/or Nuisance Alarm:* Any alarm signal transmitted in the absence of detected intrusion or identified as a nuisance alarm is a false alarm. A nuisance alarm is the activation of an alarm sensor by some influence for which the sensor was designed but which is not related to an intrusion attempt. All alarms shall be investigated and the results documented. The maintenance program for the IDS should ensure that incidents of false alarms should not exceed 1 in a period of 30 days per zone.

6. *Personnel*

a. *IDS Installation and Maintenance Personnel:* Alarm installation and maintenance should be accomplished by U.S. citizens who have been subjected to a trustworthiness determination in accordance with 32 CFR part 154.

b. *Monitor Station Staffing:* The monitor station should be supervised continuously by U.S. citizens who have been subjected to a trustworthiness determination in accordance with 32 CFR part 154.

Appendix H to Part 159a—Priority for Replacement

Priorities range from 1 to 4, with 1 being the highest and 4 the lowest.

LOCK REPLACEMENT PRIORITIES IN THE UNITED STATES AND ITS TERRITORIES

Item	TS/SAP	TS	S/SAP	S–C
Vault Doors	1	1	3	4
Containers (A)[1]	3	4	4	4
Containers (B)[2]	1	1	1	2
Crypto	1	1	2	2

LOCK REPLACEMENT PRIORITIES OUTSIDE THE UNITED STATES AND ITS TERRITORIES

Item	TS/SAP	TS	S/SAP	S–C
Vault Doors	1	1	2	2
Containers (A)[1]	2	2	3	3
Containers (B)[2]	1	1	1	2
Crypto	1	1	2	2
High Risk Areas	1	1	1	1

[1] A—Located in a controlled environment where the Department of Defense has the authority to prevent unauthorized disclosure of classified information. The Government may control or deny access to the space, post guards, require identification, challenge presence, inspect packages, program elevators, or take other reasonable measures necessary to deny unauthorized access.

[2] B—Located in an uncontrolled area without perimeter security measures.

Appendix I to Part 159a—Access Controls

1. *Access Controls:* The perimeter entrance should be under visual control at all times during working hours to preclude entry by unauthorized personnel. This may be accomplished by several methods (e.g., employee work station, guard, and CCTV). Regardless of the method utilized, an access control system shall be used on the entrance. Uncleared persons are to be escorted within the facility by a cleared person who is familiar with the security procedures at the facility.

a. *Automated Entry Control Systems:* An automated entry control system may be used to control admittance during working hours instead of visual control, if it meets the criteria stated below.

The automated entry control system must identify an individual authenticate that person's authority to enter the area through the use of an identification (ID) badge or card, and number or by personal identity verification. Exist should also be recorded.

(1) *ID Badges or Key Cards.* The ID badge or key card must use embedded sensors, integrated circuits, magnetic stripes or other means of encoding data that identifies the facility and the individual to whom the card is issued.

(2) *Personal Identity Verification.* Personel identity verification (biometrics device) identifies the individual requesting access by some unique personal characteristic, such as:

(a) *Fingerprinting*

(b) *Hand Geometry*

(c) *Handwriting*

(d) *Retina*

(e) *Voice recognition.* A biometrics device may be required for access to most sensitive information.

2. In conjunction with subparagraph 1.a(2)(a), above, a personal identification number (PIN) may be required. The PIN must be separately entered into the system by each individual using a keypad device and shall consist of four or more digits, randomly selected, with no known or logical association with the individual. The PIN must be changed when it is believed to have been compromised or subjected to compromise.

3. Authentication of the individual's authorization to enter the area must be accomplished within the system by the inputs from the ID badge and/or card or the personal identity verification device or the keypad with an electronic data base of individuals authorized into the area. A procedure must be established for removal of the individual's authorization to enter the area upon reassignment, transfer or termination, or when the individual's access is suspended, revoked, or downgraded to a level lower than required.

4. Protection must be established and continuously maintained for all devices and/