APPENDIX G
PHYSICAL SECURITY STANDARDS

A. Vault and Secure Room Construction Standards

1. Vault

a. Floor and Walls. Eight inches of concrete reinforced to meet current standards. Walls are to extend to the underside of the roof slab above.

b. Roof. Monolithic reinforced-concrete slab of thickness to be determined by structural requirements, but not less than the floors and walls.

c. Ceiling. The roof or ceiling must be reinforced concrete of a thickness to be determined by structural requirements, but not less than the floors and walls

d. Vault door and frame unit should conform to Federal Specification AA-D-2757 Class 8 vault door, or Federal Specification AA-D-600 Class 5 vault door.

2. Secure Room

a. The walls, floor, and roof construction of secure rooms must be of permanent construction materials; i.e., plaster. gypsum wallboard, metal panels, hard-board, wood. plywood, or other materials offering resistance to, and evidence of unauthorized entry into the area. Walls shall be extended to the true ceiling and attached with permanent construction materials, with mesh or 18 gauge expanded steel screen.

b. Ceiling. The ceiling shall be constructed of plaster, gypsum, wallboard material, hardware or any other acceptable material.

c. Doors. The access door to the room shall be substantially constructed of wood or metal. The hinge pins of outswing doors shall be peened, brazed, or spot welded to prevent removal. Door should be equipped with a built-in GSA-approved combination lock meeting Federal Specification FF-L-2740.

d. Windows. Windows that are less than 18 feet above the ground measured from the bottom of the window, or are easily accessible by means of objects directly beneath the windows. shall be constructed from or covered with materials that will provide protection from forced entry. The protection provided to the windows need be no stronger than the strength of the contiguous walls.

e. Openings. Utility openings such as ducts and vents should be kept at less than man-passable (96 square inches) opening. Openings larger than 96 square inches will be hardened in accordance with Military Handbook 1013/1 A.

B. Intrusion Detection System (IDS) Standards

1. An IDS must detect an unauthorized penetration in the secured area. An IDS complements other physical security measures and consists of the following:

a. Intrusion Detection Equipment (IDE)

b. Security forces

c. Operating procedures

2. System Functions

a. IDS components operate as a system with the following four distinct phases:

(1) Detection

(2) Communications

(3) Assessment

(4). Response

b. These elements are equally important, and none can be eliminated if an IDS is to provide an acceptable degree of protection.

(1) Detection: The detection phase begins as soon as a detector or sensor reacts to stimuli it is designed to detect The sensor alarm condition is then transmitted over cabling located within the protected area to the Premise Control Unit (PCU) The PCU may service many sensors. The PCU and the sensors it serves comprise a “zone” at the monitor station. This shall be used as the definition of an alarmed zone for purposes of this Regulation.

(2) Reporting: The PCU receives signals from all sensors in a protected area and incorporates these signals into a communication scheme. Another signal is added to the communication for supervision to prevent compromise of the communication scheme. This tampering or injection of false information by an intruder. The supervised signal is sent by the PCU through the transmission link to the monitor station. Inside the monitor station either a dedicated panel or central processor monitors information from the PCU signals. When an alarms occur, an annunciator generates an audible and visible alert to security personnel. Alarms result normally from intrusion, tampering, component failure, or system power failure.

(3) Assessment The assessment period is the first phase that requires human interaction. When alarm conditions occur, the operator assesses the situation and dispatches the response force.

(4) Response: The response phase begins as soon as the operator assesses an alarm condition. A response force must immediately respond to all alarms. The response phase must also determine the precise nature of the alarm and take all measures necessary to safeguard the secure area.

3 Threat, Vulnerability and Acceptability

a. As determined by the commander all areas that reasonably afford access to the container, or where classified data is stored should be protected by IDS unless continually occupied. Prior to the installation of an IDS, commanders shall consider the threat, vulnerabilities, in-depth security measures and shall perform a risk analysis.

b. Acceptability of Equipment: All IDE must be UL-listed, (or equivalent) and approved by the DoD Component or government contractor. Government installed, maintained, or furnished systems are acceptable.

4. Transmission and Annunciation

a. Transmission Line Security: When the transmission line leaves the facility and traverses an uncontrolled area, Class I or Class II line supervision shall be used.

(1) Class I: Class I line security is the achieved through the use of DES or an algorithm based on the cipher feedback or cipher block chaining mode of encryption. Certification by NIST or another independent testing laboratory is required.

(2) Class 11: Class II line supervision refers to systems in which the transmission is based on pseudo random generated tones or digital encoding using an interrogation and response scheme throughout the entire communication, or UL Class AA line supervision. The signal shall not repeat itself within a minimum 6 month period. Class II security shall be impervious to compromise using resistance, voltage, current, or signal substitution techniques.

b. Internal Cabling: The cabling between the sensors and the PCU should be dedicated to IDE and must comply with national and local code standards.

c. Entry Control Systems: If an entry control system is integrated into an IDS, reports from the automated entry control system should be subordinate in priority to reports from intrusion alarms.

d. Maintenance Mode: When an alarm zone is placed in the maintenance mode, condition shall be signaled automatically to the monitor station. The signal must appear as an alarm, or maintenance message at the monitor station and the IDS shall not be securable while in the maintenance mode. The alarm or message must be continually visible at the monitor-station throughout the period of maintenance. A standard operating procedure must be established to address appropriate actions when maintenance access is indicated at the panel. All maintenance periods shall be archived in the system. A self-test feature shall be limited to one second per occurrence.

e. Annunciation of Shunting or Masking Condition: Shunting or masking of any internal zone or sensor must be appropriately logged or recorded in archive. A shunted or masked internal zone or sensor must be displayed as such at the monitor station throughout the period the condition exists whenever there is a survey of zones or sensors.

f . Indications of alarm status shall be revealed at the monitoring station and optionally within the confines of the secure area.

g. Power Supplies: Primary power for all IDE shall be commercial AC or DC power. In the event of commercial power failure at the protected area or monitor station, the equipment shall change power sources without causing an alarm indication.

(1) Emergency Power: Emergency power shall consist of a protected independent backup power source that provides a minimum of 4 hours operating power battery and/or generator power. When batteries are used for emergency power, they shall be maintained at full charge by automatic charging circuits. The

manufacturer's periodic maintenance schedule shall be followed and results documented.

(2) Power Source and Failure Indication: An illuminated indication shall exist at the PCU of the power source in use (AC or DC). Equipment at the monitor station shall indicate a failure in power source, a change in power source, and the location of the failure or change.

h. Component Tamper Protection: IDE components located inside or outside the secure area should be evaluated for a tamper protection requirement. If access to a 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 independently 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. Installation, Maintenance and Monitoring

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 DoD 5200.2-R.

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 DoD 5200.2-R.

C. Priorities for Replacement of Locks

[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)*	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)	2	2	3	3
Containers (B)	1	1	1	2
Crypto	1	1	2	2
High Risk Areas	1	1	1	1

[1] 1. Located in a controlled environment where the Department of Defense has the authority to prevent unauthorized disclosure of classified informaiton. The Government may control or deny access to the space, post guards, require identificaiton, challenge presence, inspect packages, program elevators, or take other reasonable measures necessary to deny unauthorized access.
[2] 2. Located in an uncontrolled area without perimeter security measures.

D. Access Controls

1. Access Controls

The perimeter entrance should be under visual control at all times during working hours to prevent entry by unauthorized personnel. This may be accomplished by several methods (e.g., employee work station, guard CCTV). Regardless of the method used. 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 AECS criteria stated in subparagraphs 1a., and 2., below.

The automated entry control system must identify an individual and authenticate the person's authority to enter the area through the use of an identification (ID) badge or card.

(1) ID Badges or Kev 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. Personal identity verification (Biometrics Devices) identifies the individual requesting access by some unique personal characteristic, such as:

(a) Fingerprinting

(b) Hand Geometry

(c) Handwriting

(d) Retina scans

(e) Voice recognition.

A biometrics device may be required for access to the most sensitive information.

2. In conjunction with subparagraph 1.a.(1), 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 inputs from the ID badge/card, the personal identity verification device, or the keypad with an electronic database of individuals authorized to enter 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 the required access level

4. Protection must be established and maintained for all devices or equipment which constitute the entry control system. The level of protection may vary depending upon the type of device or equipment being protected.

a. Location where authorization data and personal identification or verification data is input, stored, or recorded must be protected.

b. Card readers, keypads, communication or interface devices located outside the entrance to a controlled area shall have tamper resistant enclosures and be securely fastened to the wall or other permanent structure. Control panels located within a controlled area shall require only a minimal degree of physical security protection sufficient to preclude unauthorized access to the mechanism

c. Keypad devices shall be designed or installed in such a manner that an unauthorized person in the immediate vicinity cannot observe the selection of input numbers.

d. Systems that use transmission lines to , carry access authorizations, personal identification data, or verification data between devices or equipment located outside the controlled area shall have line supervision.

e. Electric strikes used in access control systems shall be heavy duty, industrial grade.

5. Access to records and information concerning encoded ID data and PINs shall be restricted. Access to identification or authorizing data, operating system software or any identifying data associated with the entry control system shall be limited to the fewest number of personnel as possible. Such data or software shall be kept secure when unattended.

6. Records shall be maintained reflecting active assignment of ID badge/card, PIN, level of access, and similar system-related records. Records concerning personnel removed from the system shall be retained

for 90 days. Records of entries shall be retained for at least 90 days or until investigations of system violations and incidents have been investigated, resolved and recorded.

7. Personnel entering or leaving an area shall be required to secure the entrance or exit point. Authorized personnel who permit another individual to enter the area are responsible for confirmation of need to know and access. The Heads of DoD Components may approve the use of standardized AECS which meet the following criteria:

a. For a Level 1 key card system, the AECS must provide a .95 probability of granting access to an authorized user providing the proper identifying information within three attempts. In addition, the system must ensure an unauthorized user is granted access with less than 0.05 probability after three attempts to gain entry.

b. For a Level 2 key card and PIN system, the AECS must provide a 0.97 probability of granting access to an authorized user providing the proper identifying information within three attempts. In addition, the system must ensure an unauthorized user is granted access with less than 0.010 probability after three attempts to gain entry have been made.

c. For a Level 3 key card and PIN and biometrics identifier system, the AECS must provide a 0.97 probability of granting access to an unauthorized user providing the proper identifying information within three attempts. In addition, the system must ensure an unauthorized user is granted access with less than 0.005 probability after three attempts to gain entry have been made,

8. Electric, Mechanical. or Electromechanical Access Control Devices. Electric, mechanical, or electromechanical devices which meet the criteria stated below may be used to control admittance to secure areas during duty hours if the entrance is under visual control. These devices are also acceptable to control access to compartmented areas within a secure area. Access control devices must be installed in the following manner:

a. The electronic control panel containing the mechanical mechanism by which the combination is set is to be located inside the area. The control panel (located within the area) will require only minimal degree of physical security designed to preclude unauthorized access to the mechanism.

b. The control panel shall be installed in such a manner, or have a shielding device mounted, so that an unauthorized person in the immediate vicinity cannot observe the setting or changing of the combination.

c. The selection and setting of the combination shall be accomplished by an individual cleared at the same level as the highest classified information controlled within.

d. Electrical components, wiring included, or mechanical links (cables, rods and so on) should be accessible only from inside the area, or, if they traverse an uncontrolled area they should be secured within protecting covering to preclude surreptitious manipulation of components.