ENCLOSURE 3

STORAGE AND DESTRUCTION

1. GENERAL REQUIREMENTS

a. Classified information shall be secured under conditions adequate to deter and detect access by unauthorized persons. The requirements specified in this Volume represent acceptable security standards. DoDD 5210.56 (Reference (ai)) specifies DoD policy concerning the use of force for the protection of classified information. Do not store weapons or items such as funds, jewels, precious metals, or drugs in the same container used to safeguard classified information. Holdings of classified material should be reduced to the minimum required to accomplish the mission.

b. GSA establishes and publishes minimum standards, specifications, and supply schedules for containers, vault doors, modular vaults, alarm systems, and associated security devices suitable for storing and protecting classified information. DoDI 3224.03 (Reference (aj)) describes requirements for acquiring physical security equipment for use within the Department of Defense.

c. The DNI establishes security requirements for sensitive compartmented information facilities (SCIFs). These are issued by Reference (i) within the Department of Defense.

d. The DoD Lock Program is designated as the DoD technical authority for locking and storage systems used for the protection of classified information. For technical support, call the DoD Lock Program Technical Support Hotline at 1-800-290-7607 or DSN 551-1212 or review the website at https://locks.navfac.navy.mil, for more information.

e. Volume 4 of this Manual specifies storage and destruction requirements for controlled unclassified information.

2. LOCK SPECIFICATIONS.

Except as provided elsewhere in this Volume, combination locks on vault doors, secure rooms, and security containers protecting classified information shall conform to Federal Specification FF-L-2740 (hereafter referred to as “FF-L-2740”)(Reference (ak)).

3. STORAGE OF CLASSIFIED INFORMATION BY LEVEL OF CLASSIFICATION.

Store classified information not under the personal control and observation of an authorized person, in a locked security container, vault, room, or area, as specified in this section.

a. Top Secret. Top Secret information shall be stored:

(1) In a GSA-approved security container with one of the following supplementary

controls:

(a) An employee cleared to at least the Secret level shall inspect the security container once every 2 hours.

(b) The location that houses the security container is protected by an intrusion detection system (IDS) meeting the requirements of the Appendix to this enclosure with personnel responding to the alarm arriving within 15 minutes of the alarm annunciation.

(2) In a GSA-approved security container equipped with a lock meeting FF-L-2740, provided the container is located within an area that has been determined to have security-in-depth (see Glossary for definition);

(3) In an open storage area (also called a secure room) constructed according to the Appendix to this enclosure and equipped with an IDS with the personnel responding to an alarm within 15 minutes of the alarm annunciation if the area has been determined to have security-in-depth, or within 5 minutes of alarm annunciation if it has not;

(4) In a vault, or GSA-approved modular vault, meeting the requirements of Federal Standard (FED-STD) 832 (Reference (al)) as specified in the Appendix to this enclosure; or

(5) Under field conditions during military operations, using such storage devices or security control measures as a military commander deems adequate to prevent unauthorized access. Military commanders should employ risk management methodologies when determining appropriate safeguards.

b. Secret. Secret information shall be stored by one of the following methods:

(1) In the same manner as prescribed for Top Secret information;

(2) In a GSA-approved security container or vault built to FED-STD 832 specifications, without supplementary controls;

(3) In an open storage area meeting the requirements of the Appendix to this enclosure, provided the senior agency official determines in writing that security-in-depth exists, and one of the following supplemental controls is utilized:

(a) An employee cleared to at least the Secret level shall inspect the open storage area once every 4 hours.

(b) An IDS meeting the requirements of the Appendix to this enclosure with the personnel responding to the alarm arriving within 30 minutes of the alarm annunciation.

(4) In a secure room that was approved for the storage of Secret information by the DoD Component prior to October 1, 1995, provided the DoD Component reassesses the requirement for the secure room and makes plans to bring the room up to the standards of subparagraphs

3.b.(1) through 3.b.(3) of this section by October 1, 2013 and provided the area has been determined to have security-in-depth.

c. Confidential. Confidential information shall be stored in the same manner as prescribed for Top Secret or Secret information except that supplemental controls are not required.

4. RISK ASSESSMENT. When considering the storage alternatives specified in section 3, a risk assessment shall be performed to facilitate a security-in-depth determination and to aid identification and selection of supplemental controls that may need to be implemented. The analysis should, at a minimum, consider local threats, both known and anticipated, and vulnerabilities; the existing security environment and controls; the ease of access to containers or other areas where classified data is stored; the criticality, sensitivity, and value of the information stored; and cost verses benefits of potential countermeasures. The risk assessment shall be used to determine whether installation of an IDS is warranted or whether other supplemental controls are sufficient.

5. U.S. CLASSIFIED INFORMATION LOCATED IN FOREIGN COUNTRIES. Except for classified information that has been authorized for release to a foreign government or international organization in accordance with Reference (z), and is under that government's or organization's security control, U.S. classified material may be retained and stored in a foreign country only when necessary to satisfy specific U.S. Government requirements. The Heads of the DoD Components shall prescribe requirements for protecting this information, paying particular attention to ensuring proper enforcement of controls on release of U.S. classified information to foreign entities. Compliance with the provisions of this enclosure is required. U.S. classified material in foreign countries shall be stored at a:

a. U.S. military installation, or a location where the United States enjoys extraterritorial status, such as an embassy or consulate.

b. U.S. Government activity located in a building used exclusively by U.S. Government tenants, provided the building is under continuous (i.e., 24/7) control by U.S. Government personnel.

c. U.S. Government activity located in a building not used exclusively by U.S. Government tenants which is under host government control, provided that the classified material is stored in GSA-approved security containers which are further secured in a locked room or area to which only U.S. personnel have access and the room or area is under continuous (i.e., 24/7) control by U.S. Government personnel.

d. U.S. Government activity located in a building not used exclusively by U.S. Government tenants nor under host-government control, provided the classified material is stored in GSA-approved security containers and is placed under continuous (i.e., 24/7) control by U.S. Government personnel.

6. SPECIALIZED STORAGE

a. Military Platforms

(1) The Heads of the DoD Components shall, consistent with this Volume, delineate the appropriate security measures required to protect classified information stored in security containers on military platforms (e.g., aircraft, militarized or tactical vehicle) and for classified munitions items.

(2) GSA-approved field safes and special size one- and two-drawer security containers approved by the GSA may be used for storage of classified information in the field and in military platforms. These containers shall use locks conforming to FF-L-2740 or Federal Specification FF-L-2937 (Reference (am)), as required by Federal Specification AA-F-358 (Reference (an)). Special size containers shall be securely fastened to the platform; field safes shall be under sufficient control and surveillance when in use to prevent unauthorized access or loss.

b. IT Equipment. GSA-approved information processing system cabinets are available for protection of operational IT equipment. The cabinets can be used for storage of network equipment (such as routers, switches, and crypto devices), servers, power control units, and laptops and can be configured for rack mounting with interior fans for heat management and cable connections for exterior data transmission and power.

c. Map and Plan File Cabinets. GSA-approved map and plan file cabinets are available for storing odd-sized items such as computer media, maps, charts, and classified equipment.

d. Modular Vaults. GSA-approved modular vaults meeting Federal Specification AA-V-2737 (Reference (ao)) may be used to store classified information as an alternative to vault requirements described in the Appendix to this enclosure.

e. Bulky Material. Storage areas for bulky material containing Secret or Confidential information may have access openings (e.g., roof hatches, vents) secured by GSA-approved changeable combination padlocks meeting Federal Specification FF-P-110 (Reference (ap)). Other security measures are required, in accordance with paragraphs 3.b. and 3.c. of this enclosure.

(1) When special circumstances exist, the Heads of the DoD Components may authorize the use of key operated locks for storing bulky material containing Secret and Confidential information. The authorization shall be documented with an explanation of the special circumstances that warrant deviation from other established standards. Whenever using such locks, administrative procedures for the control and accounting of keys and locks shall be established. The level of protection provided to such keys shall be equivalent to that afforded the classified information the padlock protects.

(2) Section 1386 of title 18, United States Code (U.S.C.) (Reference (aq)), makes

unauthorized possession of keys, key-blanks, keyways, or locks that any part of the Department of Defense adopts for protecting conventional arms, ammunition, or explosives, special weapons, and classified equipment, a criminal offense punishable by fine or imprisonment for up to 10 years, or both.

7. PROCURING NEW STORAGE EQUIPMENT. New security storage equipment shall be procured from those items listed on the GSA Federal Supply Schedule. When GSA-approved security containers or vault doors with locks meeting FF-L-2740 are placed in service or when existing mechanical locks are replaced with locks meeting FF-L-2740, the custodian or security manager shall record the lock serial number on an SF 700, "Security Container Information." For procurement or technical support, call the DoD Lock Program as specified in paragraph 1.d of this enclosure.

8. SECURITY CONTAINER LABELS. GSA-approved security containers must have a label stating "General Services Administration Approved Security Container," affixed to the front of the container, usually on the control or the top drawer.

a. If the label is missing or if the container's integrity is in question, the container shall be inspected by a GSA certified inspector. Information on obtaining inspections and recertification of containers can be found on the DoD Lock Program Website (https://locks.navfac.navy.mil) or by calling the DoD Lock Program at (800) 290-7607 or DSN 551-1212.

b. When the container is being sent to the Defense Reutilization and Marketing Office, the GSA label shall be removed.

9. EXTERNAL MARKINGS ON CONTAINERS. There shall be no external mark revealing the level of classified information authorized to be or actually stored in a given container or vault, or indicating the priority assigned to the container for emergency evacuation and destruction. This does not preclude placing a mark or symbol (e.g., a bar code) on the container for other purposes (e.g., identification and/or inventory purposes) or from applying decals or stickers the DNI requires for containers and equipment used to store or process intelligence information. If a GSA container or vault door recertification is required, such labels and markings must be removed, but may be reapplied as needed after recertification.

10. SECURITY CONTAINER INFORMATION. Maintain a record for each container, or vault or secure room door, used for storing classified information. SF 700 with all information blocks completed, shall be used for this purpose. Update the form each time the security container combination is changed.

a. Part 1 of SF 700 is not classified, but contains personally identifiable information (PII) that shall be protected by sealing Part 1 in an opaque envelope (not provided as part of the SF 700) conspicuously marked "Security Container Information" and stored in accordance with SF

700 instructions. If the information must be accessed during non-duty hours and a new opaque envelope is not available to replace the opened one, the original envelope should be temporarily resealed, to the extent possible, until Part 1 can be placed in a new envelope the next working day.

b. Part 2 of SF 700, when completed, is classified at the highest level of classification authorized for storage in the security container. It shall be sealed and stored in accordance with SF 700 instructions. The classification authority block shall state "Derived From: 32 CFR 2001.80(d)(3))," with declassification upon change of combination.

11. COMBINATIONS TO CONTAINERS, VAULTS AND SECURE ROOMS

a. Protecting and Storing Combinations. In accordance with section 2001.45(a)(1) of Reference (f), the combination shall be classified at the same level as the highest classification of the material authorized for storage in the container.

(1) Use SF 700 Part 2, as specified in section 10 of this enclosure, to record the combination and other required data.

(2) If another record of the combination is made, the record shall be marked as required by Volume 2 of this Manual.

(3) Only a minimum number of authorized persons shall have knowledge of combinations to authorized storage containers, including vaults and secure rooms.

(4) Security containers, vaults, secure rooms and other authorized storage containers shall be kept locked when not under the direct supervision of an authorized person entrusted with the contents.

(5) A record of the names of persons having knowledge of the combination shall be maintained.

b. Changing Combinations. Only individuals with the responsibility and an appropriate security clearance shall change combinations to security containers, vaults and secure rooms used for storing classified information. Combinations shall be changed:

(1) When the container, vault, or secure room door is placed in service.

(2) Whenever an individual knowing the combination to the container or vault door no longer requires access, unless other sufficient controls exist to prevent that individual's access to the lock.

(3) When compromise of the combination is suspected.

(4) When the container, vault, or secure room door is taken out of service or is no longer

used to store classified information, at which time built-in combination locks shall be reset to the standard combination 50-25-50, and combination padlocks shall be reset to the standard combination 10-20-30.

12. ENTRANCES TO OPEN STORAGE AREAS FOR CLASSIFIED INFORMATION

a. When areas storing classified information are occupied by authorized individual(s), the entrances shall either be:

(1) Under visual control at all times to detect entry by unauthorized persons; or

(2) Equipped with an automated entry control system to limit access (see section 3 of the Appendix to this enclosure).

b. Secure rooms or other areas storing classified information shall be secured when the area is not occupied by authorized individual(s) or under continual visual control.

c. The Appendix to this enclosure provides standards for access control devices. Electrically actuated locks (e.g., magnetic strip card locks) do not, by themselves, meet the required standards for protecting classified information and shall not be used as a substitute for the locks prescribed in section 2 of this enclosure.

13. INSPECTION OF STORAGE CONTAINERS PRIOR TO REMOVAL, REPAIR, ETC. Cleared personnel shall inspect storage containers that may have been used to store classified information before removing them from protected areas or allowing unauthorized persons access to them to ensure no classified material remains within.

14. NEUTRALIZATION AND REPAIR PROCEDURES. The procedures described in FED-STD 809 (Reference (ar)) shall be followed for neutralization and repair of security containers and vault doors. Reference (ar) can be found on the DoD Lock Program Website, https://locks.navfac.navy.mil.

a. Neutralization and repair of a security container or door to a vault approved for storage of classified information shall be accomplished only by appropriately cleared or continuously escorted personnel specifically trained in the methods specified by Reference (ar).

b. Neutralization or repair by, or using, methods and procedures other than described in Reference (ar) is considered a violation of the security container's or vault door's security integrity and the GSA label shall be removed. Thereafter, the containers or doors may not be used to protect classified information.

15. STORAGE OF FGI. To the extent practical, FGI shall be stored separately from other

information to facilitate its control. To avoid additional costs, separate storage may be accomplished by methods such as using separate drawers in the same container as other information or, for small amounts, the use of separate file folders in the same drawer.

16. RETENTION OF CLASSIFIED INFORMATION. Classified documents and other material shall be retained within DoD organizations only if they are required for effective and efficient operation of the organization or if law or regulation requires their retention. Documents no longer required for operational purposes shall be disposed of according to the provisions of chapter 33 of Reference (t) and appropriate implementing directives and records schedules, and in accordance with sections 17 and 18 of this enclosure.

17. DESTRUCTION OF CLASSIFIED INFORMATION. Classified documents and material identified for destruction shall be destroyed completely, to prevent anyone from reconstructing the classified information, according to procedures and methods the DoD Component Head prescribes. Methods and equipment used to routinely destroy classified information include burning, crosscut shredding, wet pulping, mutilation, chemical decomposition or pulverizing. Methods used for clearing, sanitization or destruction of classified IT equipment and media include overwriting, degaussing, sanding, and physical destruction of components or media.

a. Documents and other material identified for destruction shall continue to be protected as appropriate for their classification until actually destroyed.

b. Each activity with classified holdings shall establish at least 1 day each year when specific attention and effort is focused on disposing of unneeded classified material ("clean-out day").

c. Guidance on standards, processes, and procedures for the destruction of COMSEC and other classified material can be found in Reference (r). NATO material shall be destroyed in accordance with Reference (ac). FGI shall be destroyed in the same manner as U.S. classified information of the equivalent level, except where otherwise required by international treaty or agreement. Also see Enclosure 2, subparagraphs 17.b.(7)(a) through (d) for guidance on recording FGI destruction.

d. Effective January 1, 2011, only equipment listed on an evaluated products list (EPL) issued by NSA may be used to destroy classified information using any method covered by an EPL. EPLs currently exist for paper shredders, punched tape destruction devices, optical media destruction devices (for compact discs (CDs) and digital video discs (DVDs)), degaussers (for magnetic media sanitization), and disintegrators (for paper and punched tape material). The EPLs may be obtained by calling (410) 854-6358 or at http://www.nsa.gov/ia/guidance/media_destruction_guidance/index.shtml.

(1) Equipment approved for use prior to January 1, 2011, and not found on the appropriate EPL may be used for destruction of classified information until December 31, 2016.

(2) Unless determined otherwise by NSA, whenever an EPL is revised, equipment

removed from the EPL may be utilized for destruction of classified information for up to 6 years from the date of its removal from the EPL.

(3) In all cases, if any such previously approved equipment needs to be replaced or otherwise requires a rebuild or replacement of a critical assembly (e.g., shredder blade assembly), the unit must be replaced with one listed on the appropriate EPL.

e. Classified IT storage media (e.g., hard drives) cannot be declassified by overwriting. Sanitization (which may destroy the usefulness of the media) or physical destruction is required for disposal. See also section 6 of Enclosure 7 of this Volume.

18. TECHNICAL GUIDANCE ON DESTRUCTION METHODS. Contact the National Security Agency/Central Security Service (NSA/CSS) System and Network Analysis Center at (410) 854-6358 or via e-mail at SNAC@radium.ncsc.mil, to obtain technical guidance concerning appropriate methods, equipment, and standards for destroying classified electronic media, IT equipment, electronic components, and other similar or associated materials.

a. Crosscut Shredders. Only crosscut shredders listed on the "NSA/CSS Evaluated Products List for High Security Crosscut Paper Shredders" (Reference (as)) may be used to destroy classified material by shredding.

(1) The EPL is updated on an as-needed basis as new models are successfully evaluated. Users are encouraged to contact shredders manufacturers and/or distributors for assistance in selecting unit(s) best suited to their requirements. Vendors and/or distributors can provide guidance on whether a specific model not listed meets the specifications in Reference (as) (e.g., for shred size) and, as applicable, a copy of the NSA/CSS letter confirming that the model will be included on the EPL at its next update.

(2) Crosscut shredders currently in use and not on the EPL that were at the time of acquisition on a NSA/CSS evaluated approved products list as being capable of maintaining a shred size of 1/2 inch by 1/32 inch (variance of 1/64 inch) may be used until December 31, 2016 in accordance with paragraph 17.d of this enclosure, EXCEPT for destruction of COMSEC materials. However, any such crosscut shredders requiring replacement of the unit and/or rebuild of the shredder blades assembly MUST BE REPLACED by a crosscut shredder on the latest NSA/CSS EPL. When COMSEC material is destroyed by shredding, ONLY crosscut shredders listed in Reference (as) at the time of acquisition shall be used.

(a) Pending replacement, the Heads of DoD Components shall ensure that procedures are in place to manage the risk posed by crosscut shredders not on the approved NSA/CSS list. At a minimum, the volume and content of each activity's classified material destruction flow shall be assessed and a process established to optimize the use of high security crosscut paper shredders (i.e., with top secret collateral material being the highest collateral priority) to take full advantage of the added security value of those shredders.

(b) The bag of shred must be "stirred" to ensure that the content is mixed up.

(c) Shredding of unclassified material along with the classified material is encouraged.

b. Pulverizers and Disintegrators. Pulverizers and disintegrators must have a 3/32 inch or smaller security screen. Consult the "NSA/CSS Evaluated Products List for High Security Disintegrators" (Reference (at)) for additional details and guidance.

c. Pulping. Pulping (wet process) devices with a 1/4 inch or smaller security screen may be used to destroy classified water-soluble material.

19. DESTRUCTION PROCEDURES

a. The Heads of the DoD Component shall establish procedures to ensure that all classified information intended for destruction is destroyed by authorized means and appropriately cleared personnel.

b. Classified information that cannot be destroyed shall be reevaluated and, when appropriate, downgraded, declassified, or retired to a designated record center.

c. Classified information shall be controlled in a manner designed to minimize the possibility of unauthorized removal and/or access. A burn bag may be used to store classified information awaiting destruction at a central destruction facility. Seal and safeguard each burn bag per this Volume until actually destroyed.

d. Records of destruction are not required, except as noted in paragraph 17.c of this enclosure and, for destruction of classified FGI, in Enclosure 2, subparagraphs 17.b.(7)(a) through (d).

Appendix
Physical Security Standards

APPENDIX TO ENCLOSURE 3

PHYSICAL SECURITY STANDARDS

1. VAULT AND SECURE ROOM CONSTRUCTION STANDARDS

a. Vaults. Vaults shall be constructed to meet Reference (al) as follows:

(1) Class A (concrete poured-in-place).

(2) Class B (GSA-approved modular vault meeting Reference (ao) specifications).

(3) Class C (steel-lined vault) is NOT authorized for protection of classified information.

b. Open Storage Area (Secure Room). This section provides the minimum construction standards for open storage areas.

(1) Walls, Floor, and Roof. Walls, floor, and roof shall be of permanent construction materials; i.e., plaster, gypsum wallboard, metal panels, hardboard, wood, plywood, or other materials offering resistance to and evidence of unauthorized entry into the area. Walls shall be extended from the true floor to the true ceiling and attached with permanent construction materials, mesh, or 18 gauge expanded steel screen.

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

(3) Doors. Access doors shall be substantially constructed of wood or metal. For out-swing doors, hinge-side protection shall be provided by making hinge pins non-removable (e.g., spot welding) or by using hinges with interlocking leaves that prevent removal. Doors shall be equipped with a GSA-approved combination lock meeting FF-L-2740. Doors other than those secured with locks meeting FF-L-2740 shall be secured from the inside with deadbolt emergency egress hardware, a deadbolt, or a rigid wood or metal bar that extends across the width of the door.

(4) Windows

(a) 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 located 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. Secure rooms which are located within a controlled compound or equivalent may eliminate the requirement for forced entry protection if the windows are made inoperable either by permanently sealing them or equipping them on the inside with a locking mechanism and they are covered by an IDS (either independently or by motion detection sensors within the area).

(b) Windows, which might reasonably afford visual observation of classified activities within the facility shall be made opaque or equipped with blinds, drapes, or other coverings.

(5) Utility Openings. Utility openings such as ducts and vents shall be smaller than man-passable (96 square inches). An opening larger than 96 square inches (and over 6 inches in its smallest dimension) that enters or passes through an open storage area shall be hardened in accordance with Military Handbook 1013/1A (Reference (au)).

2. IDS STANDARDS

a. IDS Purpose. An IDS shall detect an unauthorized penetration into the secured area. An IDS shall be installed when results of a documented risk assessment determine its use as a supplemental control is warranted, in accordance with Enclosure 3, sections 3 and 4 of this Volume, and use is approved by the activity head. When used, all areas that reasonably afford access to the security container or areas where classified data is stored shall be protected by IDS unless continually occupied. An IDS complements other physical security measures and consists of:

(1) Intrusion detection equipment (IDE).

(2) Security forces.

(3) Operating procedures.

b. System Functions

(1) IDS components operate as a system with four distinct phases:

(a) Detection.

(b) Communications.

(c) Assessment.

(d) Response.

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

(a) Detection. During the detection phase, a detector or sensor senses and reacts to the 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 (i.e., an

alarmed zone).

(b) Communications. The PCU receives signals from all sensors in a protected area and incorporates these signals into a communication scheme. An additional signal is added to the communication for supervision to prevent compromise of the communication scheme (i.e., 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 alarm occurs, an annunciator generates an audible and visible alert to security personnel. Alarms result normally from intrusion, tampering, component failure, or system power failure.

(c) 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.

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

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

d. Transmission and Annunciation

(1) 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.

(a) Class I. Class I security is achieved through the use of Data Encryption Standard or an algorithm based on the cipher feedback or cipher block chaining mode of encryption. Certification by the National Institutes of Standards and Technology or another independent testing laboratory is required.

(b) Class II. 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.

(2) Internal Cabling. The cabling between the sensors and the PCU shall be dedicated to IDE and shall comply with national and local code standards.

(3) Entry and/or Access Control Systems. If an entry and/or access control system is integrated into an IDS, reports from the automated entry and/or access control system shall be subordinate in priority to reports from intrusion alarms.

(4) Maintenance Mode. When the alarm zone is placed in the maintenance mode, this condition shall be signaled automatically to the monitor station. The signal shall 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 shall be continually visible at the monitor station throughout the period of maintenance. A standard operating procedure shall 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.

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

(6) Indications of Alarm Status. Indications of alarm status shall be revealed at the monitoring station and optionally within the confines of the secure area.

(7) Power Supplies. Primary power for all IDE shall be commercial alternating or direct current (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.

(a) Emergency Power. Emergency power shall consist of a protected independent backup power source that provides a minimum of 8 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.

(b) 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.

(8) Component Tamper Protection. IDE components located inside or outside the secure area shall be evaluated for a tamper protection requirement. If access to a junction box or controller will enable an unauthorized modification, tamper protection shall be provided.

e. System Requirements

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

(2) Access and/or Secure Switch and PCU. No capability shall exist to allow changing the access status of the IDS from a location outside the protected area. All PCUs shall be located inside the secure area and should be located near the entrance. Assigned personnel shall initiate all changes in access and secure status. Operations 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.

(3) Motion Detection Protection. Secure areas that reasonably afford access to the security container or area where classified data is stored shall 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.

(4) Protection of Perimeter Doors. When an IDS is installed, each perimeter door shall be protected by a balanced magnetic switch that meets UL Standard 634 (Reference (av)).

(5) 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 within the space, whenever a secure room is located within a controlled compound or equivalent and forced entry protection of the windows is not provided (also see subparagraph 1.b.(4) of this Appendix).

(6) IDS Requirements for Continuous Operations Facilities. A continuous operation 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.

(7) False and/or Nuisance Alarm. Any alarm signal transmitted in the absence of detected intrusion that is not 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 shall ensure that incidents of false and/or nuisance alarms shall not exceed 1 in a period of 30 days per zone.

f. Installation, Maintenance and Monitoring

(1) IDS Installation and Maintenance Personnel. Alarm installation and maintenance shall be accomplished by U.S. citizens who have been subjected to a trustworthiness determination according to Reference (l).

(2) Monitor Station Staffing. The monitor station shall be supervised continuously by U.S. citizens who have been subjected to a trustworthiness determination according to Reference (l).

3. ACCESS CONTROLS

a. The perimeter entrance to a secure facility (i.e., vault or secure room) shall be under control at all times during working hours to prevent entry by unauthorized personnel. This may be achieved by visual control or through use of an automated entry control system (AECS) that complies with the requirements of subparagraph 3.a.(2) of this section. Uncleared persons are to

be escorted within the facility by a cleared person who is familiar with the security procedures of the facility. 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 confirming their need to know and access.

(1) Visual control may be accomplished by methods such as designated employees, guards, or continuously monitored closed circuit television.

(2) An AECS may be used if it meets the criteria stated in subparagraphs 3.a.(2)(a) and 3.a.(2)(b). The AECS shall identify an individual and authenticate the person's authority to enter the area through the use of an identification (ID) badge or card.

(a) The ID badge or key card shall 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.

(b) Biometrics verification identifies the individual requesting access by some unique personal characteristic and may be required for access to sensitive information. The Biometrics Identity Management Agency can provide further information regarding biometric technologies and capabilities. Personal characteristics that can be used for identity verification include:

1. Fingerprints.

2. Hand geometry.

3. Handwriting.

4. Iris scans.

5. Voice.

6. Facial recognition.

(3) In conjunction with subparagraph 3.a.(2)(a) of this section, a personal identification number (PIN) may be required. The PIN shall 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 shall be changed when it is believed to have been compromised or subjected to compromise.

(4) Authentication of the individual's authorization to enter the area shall be accomplished within the system by inputs from the ID badge and/or card, the personal identity verification device, or the keypad with an electronic database of individuals authorized to enter the area. A procedure shall be established for removing 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.

(5) Protection shall be established and maintained for all devices or equipment that constitutes 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 shall 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.

(6) Access to records and information concerning encoded identification 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.

(7) Records shall be maintained reflecting active assignment of identification badge and/or card, PIN, level of access, and similar system-related records. Records concerning personnel removed from the system shall be retained for at least 90 days. Records of entries shall be retained for at least 90 days or until investigations of system violations and incidents have been resolved and recorded. Such records shall be destroyed when no longer required in accordance with Reference (u) and DoD Component implementing directives and records schedules.

b. The Heads of DoD Components may approve the use of standardized AECS that meet the following criteria:

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

(2) For a Level 2 key card and PIN system, i.e., a key card bearing a magnetic stripe

used in conjunction with a PIN, the AECS shall 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.

(3) For a Level 3 key card, i.e., a key card bearing a magnetic stripe used in conjunction with a PIN and biometrics identifier system, the AECS shall provide a 0.97 probability of granting access to an authorized user providing the proper identifying information within three attempts. In addition, the system shall ensure an unauthorized user is granted access with less than 0.005 probability after three attempts to gain entry have been made.

c. Electrical, mechanical, or electromechanical access control devices meeting the criteria stated below, may be used to control access 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 shall be installed in the following manner:

(1) The electronic control panel containing the mechanism for setting the combination shall be located inside the area. The control panel shall require only a minimal degree of physical security designed to preclude unauthorized access to the mechanism.

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

(3) An individual cleared at the same level as the highest classified information controlled within the area shall select and set the combination.

(4) Electrical components, including wiring, or mechanical links (cables, rods, and so on) shall be accessible only from inside the area, or, if they traverse an uncontrolled area, they shall be secured within conduit to preclude surreptitious manipulation of components.