Department of Defense

MANUAL

NUMBER 5200.01, Volume 3
February 24, 2012

USD(I)

SUBJECT: DoD Information Security Program: Protection of Classified Information

References: See Enclosure 1

1. PURPOSE

a. Manual. This Manual is composed of several volumes, each containing its own purpose. The purpose of the overall Manual, as authorized by DoD Directive (DoDD) 5143.01 (Reference (a)) and DoD Instruction (DoDI) 5200.01 (Reference (b)), is to reissue DoD 5200.1-R (Reference (c)) as a DoD Manual to implement policy, assign responsibilities, and provide procedures for the designation, marking, protection, and dissemination of controlled unclassified information (CUI) and classified information, including information categorized as collateral, sensitive compartmented information (SCI), and Special Access Program (SAP). This guidance is developed in accordance with Reference (b), Executive Order (E.O.) 13526, E.O. 13556, and part 2001 of title 32, Code of Federal Regulations (CFR) (References (d), (e), and (f)). This combined guidance is known as the DoD Information Security Program.

b. Volume. This Volume:

(1) Provides guidance for safeguarding, storage, destruction, transmission, and transportation of classified information.

(2) Identifies security education and training requirements and processes for handling of security violations and compromise of classified information.

(3) Addresses information technology (IT) issues of which the security manager must be aware.

(4) Incorporates and cancels Assistant Secretary of Defense for Command, Control, Communications, and Intelligence Memorandums (References (g) and (h)).

2. APPLICABILITY. This Volume:

a. Applies to OSD, the Military Departments, the Office of the Chairman of the Joint Chiefs of Staff and the Joint Staff, the Combatant Commands, the Office of the Inspector General of the Department of Defense, the Defense Agencies, the DoD Field Activities, and all other organizational entities within the Department of Defense (hereinafter referred to collectively as the "DoD Components").

b. Does not alter existing authorities and responsibilities of the Director of National Intelligence (DNI) or of the heads of elements of the Intelligence Community pursuant to policies issued by the DNI. Consistent with Reference (b), SCI shall be safeguarded in accordance with the policies and procedures issued by the DNI, as implemented by DoD 5105.21-M-1 (Reference (i)) and other applicable guidance.

3. DEFINITIONS. See Glossary.

4. POLICY. It is DoD policy, in accordance with Reference (b), to:

a. Identify and protect national security information and CUI in accordance with national-level policy issuances.

b. Promote information sharing, facilitate judicious use of resources, and simplify management through implementation of uniform and standardized processes.

c. Employ, maintain and enforce standards for safeguarding, storing, destroying, transmitting, and transporting classified information.

d. Actively promote and implement security education and training throughout the Department of Defense.

e. Mitigate the adverse effects of unauthorized access to classified information by investigating and acting upon reports of security violations and compromises of classified information.

5. RESPONSIBILITIES. See Enclosure 2 of Volume 1.

6. PROCEDURES. See Enclosures 2 through 7.

7. INFORMATION COLLECTION REQUIREMENTS. All inspections, investigations, notifications, and audits required by this Volume are exempt from licensing according to paragraphs C4.4.1, C4.4.2, C4.4.7 and C4.4.8 of DoD 8910.1-M (Reference (j)).

8. RELEASABILITY. UNLIMITED. This Volume is approved for public release and is available on the Internet from the DoD Issuances Website at http://www.dtic.mil/whs/directives.

9. EFFECTIVE DATE. This Volume is effective upon its publication to the DoD Issuances Website.

Michael G. Vickers
Under Secretary of Defense
for Intelligence

Enclosures

1. References
2. Safeguarding
3. Storage and Destruction
4. Transmission and Transportation
5. Security Education and Training
6. Security Incidents Involving Classified Information
7. IT Issues for the Security Manager

Glossary

ENCLOSURE 2

SAFEGUARDING

1. CONTROL MEASURES. DoD Components shall have a system of control measures that ensure access to classified information is limited to authorized persons. The control measures shall be appropriate to the environment in which access occurs and to the nature and volume of the information. The system shall include technical, physical, and personnel control measures. Administrative control measures, which may include records of internal distribution, access, generation, inventory, reproduction, and disposition, shall be required when technical, physical, and personnel control measures are insufficient to deter and detect access by unauthorized persons. Except as otherwise specified, requests for waivers to the provisions of this Volume shall be submitted in accordance with section 16 of Enclosure 3 of Volume 1.

2. PERSONAL RESPONSIBILITY FOR SAFEGUARDING. Everyone who works with classified information is personally responsible for taking proper precautions to ensure that unauthorized persons do not gain access to classified information. Everyone granted access to classified information is personally responsible for protecting the classified information they know, possess, or control and for complying with the pre-publication security review processes specified in DoDD 5230.09 (Reference (k)). Classified information shall be protected at all times either by storing it as this Volume prescribes or by having it under the personal observation and control of an authorized individual.

3. ACCESS TO CLASSIFIED INFORMATION. Except as provided in sections 5 and 6 of this enclosure and in accordance with section 11 of Enclosure 3 of Volume 1, no person may have access to classified information unless that person has a security clearance in accordance with DoD 5200.2-R (Reference (l)) and has signed a Standard Form (SF) 312, "Classified Information Non-Disclosure Agreement" (NDA), and access is essential to the accomplishment of a lawful and authorized Government function (i.e., has a need to know).

4. DETERMINING NEED FOR ACCESS. The individual with authorized possession, knowledge, or control of the information has the final responsibility for determining whether a prospective recipient's official duties requires them to possess or have access to any element or item of classified information, and whether that prospective recipient has been granted the appropriate security clearance by proper authority.

5. EMERGENCY AUTHORITY. In emergencies in which there is an imminent threat to life or in defense of the homeland, the Heads of the DoD Components may authorize the disclosure of classified information, including information normally requiring the originator's prior authorization, to an individual or individuals who are otherwise not routinely eligible for access. The disclosing authority shall:

a. Limit the amount of classified information disclosed to the absolute minimum to achieve the purpose.

b. Limit the number of individuals who receive classified information.

c. Transmit the classified information through approved Federal government channels by the most secure and expeditious method consistent with this Volume, or by other means deemed necessary when time is of the essence.

d. Provide instructions about what specific information is classified and how it should be safeguarded. Information disclosed shall not be deemed declassified as of result of such disclosure or subsequent use by a recipient. Physical custody of classified information must remain with an authorized Federal government entity in all but the most extraordinary circumstances.

e. Provide appropriate briefings to the recipients on their responsibilities not to disclose the information to unauthorized individuals and obtain a signed SF 312.

f. Notify the agency or DoD Component originating of the information and the Deputy Under Secretary of Defense for Intelligence, and Security (DUSD(I&S)) within 72 hours of the disclosure of classified information, or at the earliest opportunity that the emergency permits but no later than 30 days after the release, by providing:

(1) A description of the disclosed information.

(2) Identification of individuals to whom the information was disclosed.

(3) How the information was disclosed and transmitted.

(4) Reason for the emergency release.

(5) How the information is being safeguarded.

(6) A description of the briefings provided.

(7) A copy of the signed SF(s) 312.

6. ACCESS BY INDIVIDUALS OUTSIDE THE EXECUTIVE BRANCH. Classified information may be made available to individuals or agencies outside the Executive Branch, as provided in this section, if such information is necessary for performance of a lawful and authorized function, and such release is not prohibited by the originating department or agency. The Heads of DoD Components shall designate officials to ensure the recipient's eligibility for access, prior to the release of classified information. (See Volume 1, Enclosure 3, section 11 for requirements for access by individuals inside the Executive Branch.)

a. Congress. DoDI 5400.04 (Reference (m)) provides rules for access to classified information or material by Congress, its committees, members, and staff representatives. Members of Congress, by virtue of their elected position, are not investigated or cleared by the Department of Defense.

b. Government Printing Office (GPO). Collateral documents and material of all classifications may be processed by the GPO, which protects the information according to a DoD/GPO Security Agreement (Reference (n)).

c. Representatives of the Government Accountability Office (GAO). DoDI 7650.01 (Reference (o)) sets forth rules for granting GAO representatives access to classified information that the Department of Defense originates and possesses when such information is relevant to the performance of the statutory responsibilities of that organization. Certifications of security clearances and the basis therefore, shall be accomplished under arrangements between the GAO and the relevant DoD Component. Personal recognition or presentation of official GAO credential cards are acceptable for identification purposes, but not for access to classified information.

d. Historical Researchers. Persons outside the Executive Branch who are engaged in historical research projects may be authorized access to classified information provided that the DoD Component Head or senior agency official with classification jurisdiction over the information:

(1) Determines, in writing, that such access is clearly consistent with the interests of national security in view of the intended use of the material to which access is granted by certifying that the requester has been found to be eligible for access pursuant to Reference (l) and section 3 of this enclosure.

(2) Limits access to specific categories of information over which the DoD Component has classification jurisdiction or for which the researcher has the written consent of the DoD Component or non-DoD agency with classification jurisdiction. The information contained within or revealed by the specified categories must be within the scope of the research.

(3) Maintains custody of the classified material at a DoD installation or activity or authorizes access to documents held by the National Archives and Records Administration (NARA).

(4) Obtains the requester's agreement to safeguard the information and to submit any notes and manuscripts intended for public release for review by all DoD Components or non-DoD departments or agencies with classification jurisdiction to determine whether classified information is contained therein. The agreement shall be documented by execution of a statement substantially similar to that in Figure 1.

Figure 1. Conditions Governing Access to Official Records by Historical Researchers

To Whom It May Concern:

I understand that the classified information to which I have requested access for historical research purposes is concerned with the national defense or foreign relations of the United States. Unauthorized disclosure could reasonably be expected to cause damage, serious damage, or exceptionally grave damage to the national security depending on whether the information is classified Confidential, Secret, or Top Secret, respectively. If granted access, I therefore agree to the following conditions governing access to the [insert Component or activity] files:

1. I will abide by any rules and restrictions issued in your letter of authorization, including those of other Agencies whose information is interfiled with that of the [insert Component or activity].

2. I agree to safeguard the classified information to which I gain possession or knowledge in a manner consistent with Part 4 of Executive Order 13526, "Classified National Security Information," and the applicable provisions of the DoD regulations concerning safeguarding classified information, including Volumes 1, 2, and 3 of DoD Manual 5200.01, "DoD Information Security Program."

3. I agree not to reveal to any person or Agency any classified information obtained because of this access except as authorized in the terms of your authorization letter or a follow-on letter. I further agree that I shall not use the information for purposes other than those set forth in my request for access.

4. I agree to submit my research notes for review to determine if classified information is contained in them before their removal from the specific area assigned to me for research. I further agree to submit my manuscript(s) for a security review before its publication or presentation. In each of these reviews, I agree to comply with any decision of the reviewing official in the interests of the security of the United States, including the retention or deletion of any classified parts of such notes and manuscript whenever the Federal Agency concerned deems such retention or deletion necessary.

5. I understand that failure to abide by the conditions in this statement shall constitute sufficient cause for canceling my access to classified information and for denying me any future access and may subject me to criminal provisions of Federal Law as referred to in Item 6.

6. I have been informed that provisions of title 18 of the United States Code impose criminal penalties, under certain circumstances, for the unauthorized disclosure, loss, copying, or destruction of defense information.

THIS STATEMENT IS MADE TO THE UNITED STATES GOVERNMENT TO ENABLE IT TO EXERCISE ITS RESPONSIBILITY FOR THE PROTECTION OF INFORMATION AFFECTING THE NATIONAL SECURITY. I UNDERSTAND THAT ANY MATERIAL FALSE STATEMENT THAT I MAKE KNOWINGLY AND WILFULLY SHALL SUBJECT ME TO THE PENALTIES OF TITLE 18, U.S. CODE, SECTION 1001.

Signature:

Witness's Signature:

Date:

(5) Authorizes access, in writing, for no more than 2 years from the date of issuance. The DoD Component may renew access for 2-year periods in accordance with DoD Component-issued regulations.

e. Presidential or Vice Presidential Appointees and Designees. Persons who previously occupied senior policy-making positions to which they were appointed or designated by the President or Vice President may not remove classified information upon departure from office, as all such material shall remain under the U.S. Government's security control. Such persons may be authorized access to classified information they originated, reviewed, signed, received, or that was addressed to them while serving as an appointee or designee, provided that the DoD Component Head or senior agency official with classification jurisdiction for such information:

(1) Determines, in writing, that such access is clearly consistent with the interests of national security in view of the intended use of the material to which access is granted and by certifying that the requester has been found to be eligible for access pursuant to section 3 of this enclosure.

(2) Limits access to items that the person originated, reviewed, signed, or received while serving as a Presidential or Vice Presidential appointee or designee.

(3) Retains custody of the classified material at a DoD installation or activity or authorizes access to documents in the custody of the NARA.

(4) Obtains the requestor's agreement (SF 312) to safeguard the information and to submit any notes and manuscript for pre-publication review by all DoD Components and non-DoD departments or agencies with classification jurisdiction to determine that no classified information is contained therein.

f. Use of Classified Information in Litigation. DoDD 5405.2 (Reference (p)) governs the use of classified information in litigation.

g. Special Cases. When necessary in the interests of national security, the Heads of the DoD Components or their senior agency official may authorize access to classified information by persons outside the Federal government, other than those enumerated in section 5 of this enclosure and paragraphs 6.a through 6.f of this section. Prior to authorizing access, such official must determine that the recipient is reliable, loyal, and trustworthy for the purpose of accomplishing a national security objective; meets the requirements of section 3 of this enclosure; and can and will safeguard the information from unauthorized disclosure. The national security objective shall be stated in the authorization, which shall be in writing. This authority may not be further delegated.

7. VISITS. The Heads of the DoD Components shall establish procedures to accommodate visits to their Component facilities involving access to, or disclosure of, classified information. As a minimum, these procedures shall include verifying the identity, personnel security clearance, access (if appropriate), and need to know for all visitors.

a. Visit requests shall be processed and security clearance and access level verified using the Joint Personnel Adjudication System (JPAS) for DoD civilian, military, and contractor personnel whose access level and affiliation are reflected in JPAS. Fax, telephone, or other appropriate method shall be used for those personnel whose access level and affiliation are not reflected in JPAS.

b. Visits by foreign nationals to DoD Components and facilities, except for activities or events that are open to the public, shall be handled in accordance with DoDD 5230.20 (Reference (q)) and documented in the Foreign Visits System Confirmation Module.

8. PROTECTION WHEN REMOVED FROM STORAGE. An authorized person shall keep classified material removed from storage under constant surveillance. Classified document cover sheets (SF 703, "Top Secret (Cover sheet);" SF 704, "Secret (Cover sheet);" or SF 705 "Confidential (Cover sheet)") shall be placed on classified documents not in secure storage. The cover sheets show, by color and other immediately recognizable format or legend, the applicable classification level.

9. END OF DAY SECURITY CHECKS. The heads of activities that process or store classified information shall establish a system of security checks at the close of each duty and/or business day to ensure that any area where classified information is used or stored is secure. SF 701, "Activity Security Checklist," shall be used to record such checks. An integral part of the security check system shall be the securing of all vaults, secure rooms, and containers used for storing classified material. SF 702, "Security Container Check Sheet," shall be used to record such actions. SFs 701 and 702 shall be retained and disposed of as required by Component records management schedules.

10. EMERGENCY PLANS. Plans shall be developed to protect, remove, or destroy classified material in case of fire, natural disaster, civil disturbance, terrorist activities, or enemy action, to minimize the risk of compromise, and for the recovery of classified information, if necessary, following such events. The level of detail and the amount of testing and rehearsal of these plans shall be determined by assessing the risk of hostile action, foreign intelligence threats, natural disaster, or terrorist activity that may place the information in jeopardy.

a. Use the requirements of Committee on National Security Systems (CNSS) Instruction 4004 (Reference (r)) when developing plans for the emergency protection (including emergency destruction under no-notice conditions) of classified communications security (COMSEC) material.

b. When preparing emergency plans, consider:

(1) Reducing the amount of classified material on hand.

(2) Storing less frequently used classified material at other secure locations.

(3) Creating regular back up copies of information in electronic formats for off-site storage.

(4) Transferring as much retained classified information to removable electronic media as possible, thereby reducing its bulk.

11. USE OF SECURE COMMUNICATIONS. In accordance with the requirements of Enclosure 4, classified information shall be transmitted only over secure communications circuits approved for transmission of information at the specified level of classification. This includes communication by telephone, facsimile, e-mail and other forms of electronic communications (e.g., messages, websites). See Volume 2 of this Manual for guidance on required markings.

12. REMOVAL OF CLASSIFIED INFORMATION FOR WORK AT HOME. When it is mission critical for individuals to remove classified information and materials (e.g., IT equipment and associated storage media) for work at home, specific security measures and approvals are required. Security measures appropriate for the level of classification must be in place to provide adequate protection and security-in-depth and to prevent access by unauthorized persons. Compliance with section 12 of Enclosure 4 of this Volume is also required.

a. Top Secret. Only the Secretary of Defense, the Secretaries of the Military Departments, the Chairman of the Joint Chiefs of Staff, the Combatant Commanders, or the senior agency officials appointed pursuant to section 5.4(d) of Reference (d) may authorize the removal of Top Secret information from designated working areas for work at home. Such officials may also authorize removal of information for work at home for any lower level of classification.

b. Secret and Confidential. The Heads of the DoD Components may authorize removal of Secret and Confidential information from designated working areas for work at home. This authority shall not be delegated below the major command or equivalent level.

c. Residential Storage Equipment. A General Services Administration (GSA)-approved security container shall be furnished for residential storage of classified information. Written procedures shall be developed to provide for appropriate protection of the information, including a record of the classified information that has been authorized for removal for work at home.

d. Classified IT Systems. See section 7 of Enclosure 7 of this Volume when classified IT equipment will be used. All residential classified network connections must be certified and accredited in accordance with DoDI 8510.01 (Reference (s)) requirements.

e. Foreign Country Restriction. Work at home may be authorized in foreign countries only when the residence is in a specific location where the United States enjoys extraterritorial status (e.g., on the embassy, chancery, or consulate compound) or on a U.S. military installation.

13. WORKING PAPERS. Working papers are documents (e.g., notes, drafts, prototypes) or materials (e.g., printer ribbons, photographic plates), regardless of the media, created during development and preparation of a finished product. Working papers and materials are not intended or expected to be disseminated. Working papers and materials containing classified information shall be:

a. Dated when created.

b. Marked with the highest classification of any information contained therein.

c. Safeguarded as required for the assigned classification.

d. Conspicuously marked "Working Paper" on the cover and/or first page of the document or material (or comparable location for special types of media) in letters larger than existing text.

e. Destroyed in accordance with chapter 33 of title 44, U.S.C. (Reference (t)) as implemented by DoDD 5015.2 (Reference (u)) and appropriate DoD Component implementing directives and records schedules when no longer needed.

f. Marked and controlled the same way as this Manual requires for finished products of the same classification when retained more than 180 days from date of origin (30 days for SAPs), filed permanently, e-mailed within or outside the originating activity, or released outside the originating activity, except as provided in paragraph 13.g. of this section.

g. Shared between action officers, either physically or electronically, without controlling them as permanent documents only when:

(1) The working materials are shared informally (e.g., collaborative documents or coordinating drafts) in the development process.

(2) Transfer or transmission of the material is via secure means and, if electronic, by means other than e-mail.

(3) All copies held by other than the originator are marked and controlled as required for finished products when retained more than 180 days of origin (30 days for SAPs). Consult with the originator for correct markings.

14. EQUIPMENT USED FOR PROCESSING CLASSIFIED INFORMATION. The Department of Defense has a variety of non-COMSEC-approved equipment that is used to process classified information. This includes copiers, facsimile machines, computers and other IT equipment and peripherals, display systems, and electronic typewriters. Activities shall identify those features, parts, or functions of equipment used to process classified information that may retain all or part of the information. Activity security procedures shall prescribe the appropriate safeguards to:

a. Prevent unauthorized access to that information, including by repair or maintenance personnel.

b. Ensure that repair procedures do not result in unauthorized dissemination of or access to classified information. Where equipment cannot be properly sanitized or appropriately knowledgeable escort provided, cleared maintenance technicians shall be used. Electronic repair or diagnostic equipment shall be maintained as classified material by the DoD Component if there is the potential for classified data transmission from the equipment being serviced. Use of remote diagnostic or repair capabilities shall be specifically approved and authorized in writing by the activity security manager; if the equipment retains or stores any classified information appropriate physical and logical protection must be provided on the remote end and secure communications are required.

c. Replace and destroy equipment parts in the appropriate manner when classified information cannot be removed. Removable disk drives, memory chips and boards, and other electronic components of copiers, fax machines, etc. may be sanitized or destroyed in the same manner as used for comparable computer equipment. Alternatively, the equipment shall be designated as classified and be retained and protected accordingly.

d. Ensure that appropriately knowledgeable, cleared personnel inspect equipment and associated media used to process classified information before the equipment is removed from protected areas to ensure there is no retained classified information. Classification markings and labels shall be removed from sanitized equipment and media after inspection, prior to removal from protected areas.

e. Ensure computers and other equipment used to process classified information or to transmit classified information across a network are certified and accredited in accordance with Reference (s) as required by DoDD 8500.01E (Reference (v)). Measures to protect against compromising emanations shall be implemented in accordance with DoDD C-5200.19 (Reference (w)).

15. REPRODUCTION OF CLASSIFIED MATERIAL. Paper copies, electronic files, and other material containing classified information shall be reproduced only when necessary for accomplishing the organization's mission or for complying with applicable statutes or Directives. Use of technology that prevents, discourages, or detects unauthorized reproduction of classified information is encouraged.

a. Unless restricted by the originating agency, Top Secret, Secret, and Confidential information may be reproduced, including by e-mailing, scanning, and copying, to the extent operational needs require.

b. The DoD Components shall establish procedures that facilitate oversight and control of the reproduction of classified information and the use of equipment for such reproduction, including controls that ensure:

(1) Reproduction is kept to a minimum consistent with mission requirements.

(2) Personnel reproducing classified information are knowledgeable of the procedures for classified reproduction and aware of the risks involved with the specific reproduction equipment being used and the appropriate countermeasures they are required to take.

(3) Reproduction limitations originators place on documents and special controls applicable to special categories of information are fully and carefully observed.

(4) Reproduced material is placed under the same accountability and control requirements as applied to the original material. Extracts of documents will be marked according to content and may be treated as working papers if appropriate.

(5) Reproduced material is conspicuously identified as classified at the applicable level and copies of classified material are reviewed after the reproduction process to ensure that the required markings exist.

(6) Waste products generated during reproduction are protected and destroyed as required.

(7) Classified material is reproduced only on approved and, when applicable, properly accredited systems. Section 14 of this enclosure provides additional guidance.

(8) Foreign government information (FGI) is reproduced and controlled pursuant to guidance and authority granted by the originating government.

16. CLASSIFIED MEETINGS AND CONFERENCES. Meetings and conferences involving classified information present special vulnerabilities to unauthorized disclosure. The Heads of the DoD Components shall establish specific requirements for protecting classified information at DoD Component-sponsored meetings and conferences, to include seminars, exhibits, symposia, conventions, training classes, workshops, or other such gatherings, during which classified information is disseminated.

a. DoD Component approval processes shall ensure that the following requirements are met:

(1) The meeting or conference serves a specified U.S. Government purpose.

(2) Use of other approved methods or channels for disseminating classified information or material are insufficient or impractical.

(3) The meeting or conference, or classified sessions thereof, takes place only at an appropriately cleared U.S. Government facility or a U.S. contractor facility that has an appropriate facility security clearance and, as required, secure storage capability, unless an exception is approved, in writing, in advance by the DoD Component Head or senior agency

official. Such exception authority shall not be delegated below the senior agency official. Requests for exceptions to permit use of facilities other than appropriately cleared U.S. Government or U.S. contractor facilities shall be submitted to the DoD Component Head or senior agency official in accordance with Component procedures. The request shall include a security plan that describes how the requirements of paragraphs 16.b and 16.d of this section shall be met.

(a) If classified meetings or conferences occur at a cleared U.S. contractor location, the contractor shall comply with all applicable portions of DoD 5220.22-M (Reference (x)) and parts 120 through 130 of title 22, CFR (Reference (y)) (also known as "The International Traffic in Arms Regulations"). DoD approval for the conduct of the meeting does not constitute authorization for presentation of export-controlled information when foreign nationals attend.

(b) The conduct of classified meetings or conferences at foreign installations and contractor sites is often subject to the rules and regulations of the host country, thus presenting additional security risks. Prior to approval of the conduct of such meetings, the DoD Component shall obtain assurances, in writing, that the responsible foreign government will agree to use security measures and controls that are at least as stringent as those required by this Manual. The provisions of paragraph 16.d. also shall be satisfied. To this end, assistance can be provided by the Director, International Security Programs, Defense Technology Security Administration, Office of the Under Secretary of Defense for Policy (OUSD(P)).

(c) Routine day-to-day meetings and gatherings of DoD officials shall be conducted only at an appropriately cleared U.S. Government or contractor facility. Exceptions shall not be granted for routine meetings.

(d) The provisions of this section do not apply to operational meetings conducted in combat situations, classes conducted by DoD schools, or gatherings of personnel of a DoD Component and foreign government representatives or U.S. and/or foreign contractor representatives on a matter related to a specific U.S. Government contract, program, or project.

(4) Classified sessions are segregated from unclassified sessions.

(5) Access to the meeting or conference, or specific sessions thereof, where classified information may be discussed or disseminated is limited to persons who possess an appropriate security clearance and need to know.

(6) Any participation by foreign nationals or foreign representatives complies with requirements of Reference (q) and DoDD 5230.11 (Reference (z)) (e.g., the responsible U.S. Government foreign disclosure office(s) assures, in writing, that the information to be presented has been approved for disclosure to the represented foreign countries).

(7) Announcement of the meeting or conference is unclassified and limited to a general description of topics expected to be presented, names of speakers, logistical information, and administrative and security instructions.

(8) Procedures shall ensure that classified information, documents, recordings, audiovisual material, information systems, notes, and other materials created, distributed, or used during the meeting are controlled, safeguarded, and transported as provisions of this Manual require. Recording or taking notes, including notes on classified electronic devices, during classified sessions shall be permitted only when it is determined that such action is necessary to fulfill the U.S. Government purpose for the meeting.

(9) Information systems used during the meeting or conference to support creation or presentation of classified information shall meet all applicable requirements for processing classified information, including as appropriate considerations of technical security countermeasures (TSCM). Unclassified laptop computers, handheld information technologies (e.g., personal electronic devices (PEDs)), and other similar devices shall not be used for note taking during classified sessions. Use of classified computers and other electronic devices shall be permitted only when needed to meet the intent of the meeting or conference and appropriate protection and TSCM requirements have been met.

b. The DoD activity sponsoring a classified meeting or conference shall assign an official to serve as security manager for the meeting and be responsible for ensuring that, at a minimum, the following security provisions are met:

(1) Attendees are briefed on safeguarding procedures.

(2) Entry is controlled so that only authorized personnel gain entry to the area. Particular caution shall be taken to ensure that any individual who is not authorized to attend the classified session(s) is denied entry thereto.

(3) The perimeter is controlled to ensure unauthorized personnel cannot overhear classified discussions or introduce devices that would result in the compromise of classified information.

(4) Escorts are provided for uncleared personnel who are providing services to the meeting or conference (e.g., setting up food or cleaning) when classified presentations and/or discussions are not in session.

(5) Use of cell phones, PEDs, 2-way pagers, and other electronic devices that transmit is prohibited.

(6) Classified notes and handouts are safeguarded in accordance with Enclosure 3.

(7) Classified information is disclosed to foreign nationals only in accordance with the provisions of Reference (z).

(8) An inspection of the room(s) is conducted at the conclusion of the meeting or conference (or at the end of each day of a multi-day event) to ensure all classified materials are properly stored.

c. Appropriately cleared U.S. Government contractor personnel may provide administrative support and assist in organizing a classified meeting or conference, but the DoD Component sponsoring the gathering remains responsible for all security requirements.

d. Facilities other than appropriately cleared U.S. Government or U.S. contractor facilities proposed for use for classified meetings and conferences shall:

(1) Not be open to the public and access shall be controlled by the U.S. Government or cleared contractor through a 100 percent identification card check at the perimeter point. For a military installation or comparably protected Federal government compound, this can be at the perimeter fence of the installation or compound.

(2) Have the room(s) where the classified sessions are to be held located away from public areas so that access to the room(s), walls, and ceiling(s) can be completely controlled during the classified sessions.

(3) Provide authorized means to secure classified information in accordance with Enclosure 3.

(4) Meet the DoD antiterrorism standards specified by DoDI 2000.16 (Reference (aa)).

(5) Be subject to TSCM surveys in accordance with DoDI 5240.05 (Reference (ab)). When addressing this requirement, TSCM security classification guidance MUST be consulted to ensure proper classification of meeting details when associated with the use of TSCM.

e. Not later than 90 days following the conclusion of a classified meeting or conference for which an exception was granted, the sponsoring activity shall provide an after-action report to the DUSD(I&S) through the approving DoD Component Head or senior agency official. The after-action report shall be a brief summary of any issues or threats encountered during the event and actions taken to address the situation.

17. SAFEGUARDING FGI

a. North Atlantic Treaty Organization (NATO) Information. NATO classified information shall be controlled and safeguarded according to United States Security Authority for NATO Instruction 1-07 (Reference (ac)).

b. Other FGI. See the Glossary for the definition of FGI.

(1) To avoid inadvertent compromise, classified FGI shall be stored in a manner that will avoid commingling with other material. For small volumes of material, separate files in the same vault, container, or drawer will suffice.

(2) FGI shall be re-marked if needed to ensure the protective requirements are clear. FGI may retain its original classification if it is in English. However, when the foreign

government marking is not in English, or when the foreign government marking requires a different degree of protection than the same U.S. classification designation, a U.S. marking that results in a degree of protection equivalent to that required by the foreign government shall be applied. See Appendix 1 to Enclosure 4 of Volume 2 of this Manual for comparable U.S. classification designations.

(3) U.S. documents containing FGI shall be marked as required by section 9 of Enclosure 4 of Volume 2 of this Manual. The foreign government document or authority on which derivative classification is based must be identified on the "Derived from:" line, in addition to the identification of any U.S. classification authority. A continuation sheet should be used for multiple sources, if necessary. A U.S. document containing FGI cannot be declassified or downgraded below the highest level of FGI contained in the document without the written permission of the foreign government or international organization that originated the information.

(4) Security clearances issued by the U.S. Government are valid for access to classified FGI of a comparable level.

(5) The transmission of FGI within the United States among U.S. Government agencies and U.S. contractors and between U.S. contractors with a need to know must be in accordance with this Manual and Reference (x).

(6) The international transfer of foreign government classified information must be by government officials through government-to-government channels, or channels agreed upon in writing by the originating and receiving governments (collectively "government-to-government transfer"). See Enclosure 4 and its Appendix for further guidance on transfer of classified information.

(7) The receiving DoD Components shall protect FGI to at least a degree equivalent to that required by the foreign government or international organization that provided the information. FGI shall be controlled and safeguarded in the same manner as prescribed for U.S. classified information, except as described below. The control and safeguarding requirements for FGI may be modified as permitted by a treaty or international agreement, or, for foreign governments with which there is no treaty or international agreement, through formal written agreement between the responsible national security authorities or designated security authorities of the originating and receiving governments (hereafter referred to collectively as designated security authorities (DSAs)). The Under Secretary of Defense for Policy (USD(P)) serves as the DSA.

(a) Control of Foreign Government Top Secret Information. Maintain records for 5 years of the receipt, internal distribution, destruction, annual inventory, access, reproduction, and transmittal of foreign government Top Secret information. Reproduction requires the consent of the originating government. Destruction shall be witnessed.

(b) Control of Foreign Government Secret Information. Maintain records for 3 years of the receipt, distribution, external dispatch, reproduction, and destruction of material

containing foreign government Secret information. Other records may be necessary if the originator requires. Secret FGI may be reproduced to meet mission requirements.

(c) Control of Foreign Government Confidential Information. Maintain records for 2 years for the receipt and external dispatch of Confidential FGI. Do not maintain other records for foreign government Confidential information unless required by the originating government. Confidential FGI may be reproduced to meet mission requirements.

(d) Foreign Government Restricted Information and Information Provided in Confidence. In order to ensure the protection of Restricted FGI or foreign government unclassified information provided in confidence, such information shall be classified in accordance with Reference (d) which states that unauthorized disclosure of FGI is presumed to cause damage to the national security. If the foreign protection requirement is lower than the protection required for U.S. Confidential information, the information shall be marked "CONFIDENTIAL-Modified Handling" as described in Volume 2, Enclosure 4, paragraph 4.c of this Manual and the following requirements shall also be met:

1. The information shall be provided only to those individuals who have an established need to know, and where access is required by official duties.

2. Individuals given access shall be notified of applicable handling instructions. This may be accomplished by a briefing, written instructions, or by applying specific handling requirements to an approved cover sheet.

3. Documents shall be stored to prevent unauthorized access (e.g., a locked desk or cabinet or a locked room to which access is controlled).

4. DoD Components and contractors performing on DoD contracts shall handle documents bearing the marking "UK RESTRICTED" as classified in accordance with subparagraph 17.b.(7)(d). The provision in the U.S./United Kingdom (UK) Security Implementing Arrangement (Reference (ad)) that allows documents marked "UK RESTRICTED" to be handled in a manner similar to For Official Use Only (FOUO) information applies ONLY to DoD contactors operating under COMMERCIAL contracts with the UK and, pursuant to the agreement, the UK must include in the applicable contract its requirements for the marking and handling of the information. The provision does NOT apply to, nor permit, such handling of UK RESTRICTED information by DoD Components or by contractors when performing on DoD contracts.

(8) FGI shall not be disclosed to nationals of third countries, including foreign nationals who are protected individuals or permanent resident aliens, or to any other third party, or used for other than the purpose for which the foreign government provided it without the originating government's written consent. Questions regarding releasability or disclosure should be directed to the U.S. originator, who will consult with the foreign government as required. Contractors will submit their requests through the contracting U.S. Government agency for U.S. contracts and the Defense Security Service for direct commercial contracts. Approval from the originating government does not eliminate the requirement for the contractor to obtain an export

authorization as required by other regulations or policies.

18. ALTERNATIVE COMPENSATORY CONTROL MEASURES (ACCM). A Head of a DoD Component with original classification authority (OCA) may employ ACCM when he or she determines that the standard security measures detailed in this Manual are insufficient to enforce need to know for classified information and SCI or SAP protections are not warranted. The use of an unclassified nickname, obtained in accordance with Chairman of the Joint Chiefs of Staff Manual (CJCSM) 3150.29C (Reference (ae)), together with a list of persons authorized access, and a specific description of information subject to the enhanced ACCM controls, are the three requisite elements of an ACCM.

a. DoD Proponents for ACCM. The DoD staff proponent for ACCM management, oversight and Congressional reporting is the OUSD(P). The proponent for ACCM security policy is the Office of the Under Secretary of Defense for Intelligence (OUSD(I)). Given this sharing of ACCM responsibilities, staff elements in OUSD(P) and OUSD(I) shall implement mechanisms that ensure transparency of all ACCM actions.

b. ACCM Approval. A Head of a DoD Component may approve ACCM use for classified information over which they have cognizance. Prior to approving the establishment of an ACCM, the criticality, sensitivity, and value of the information; analysis of the threats both known and anticipated; vulnerability to exploitation; and a countermeasures cost benefits analysis shall be assessed.

c. Guidance on ACCM Use. Use of ACCM must be consistent with the following guidance:

(1) ACCM may be used to assist in enforcing need to know for classified DoD intelligence matters. The DoD Component Head establishing or terminating any such ACCM shall provide written notification within 30 days to the Director of Security, OUSD(I), and the Director, Special Programs, OUSD(P), who shall maintain this information as long as the ACCM is in use.

(2) ACCM may be used to assist in enforcing need to know for classified operations, sensitive support, and other non-intelligence activities. The DoD Component Head establishing or terminating any such ACCM shall provide written notification within 30 days to the Director, Special Programs, OUSD(P), for review. The Director, Special Programs, OUSD(P), shall maintain this information as long as the ACCM is in use.

(3) ACCM shall not be used for acquisition programs or activities progressing through the acquisition process.

(4) DoD Components shall obtain an unclassified nickname consistent with Reference (ae) and coordinate with OUSD(P) to preclude duplication of nicknames.

(5) A roster or listing of all persons accessed to the ACCM shall be maintained by the ACCM control officer (see subparagraph 18.f.(1)(c) of this section). The access roster will

differentiate between those persons actively accessed and those whose accesses are currently inactive.

(6) ACCM documents and materials shall be marked as specified in Enclosure 4 of Volume 2 of this Manual.

(7) Heads of DoD Components must establish and maintain a system that provides for recurrent inspection of the ACCM they have approved. This mechanism shall ensure compliance with the provisions of this Manual. Each ACCM shall be overseen and inspected on a recurrent basis by the ACCM sponsor or OUSD(P).

d. Prohibited Security Measures. The application of the following security measures with ACCM material is prohibited:

(1) Using personnel security investigative or adjudicative standards that are more stringent than those normally required for a comparable level of classified information to establish access eligibility to ACCM-protected information.

(2) Using code words as defined in Reference (ae).

(3) Using trigraphs, digraphs, or other abbreviations of the approved nickname.

(4) Using specialized non-disclosure agreements or any certificates of disclosure or non-disclosure for ACCM access.

(5) Using a billet structure or system to control the position or numbers of persons afforded ACCM access.

e. Prohibited Uses of ACCM. The following uses of ACCM are prohibited:

(1) Using ACCM for NATO or non-intelligence FGI. For NATO, exceptions to this limitation can be granted only by the Secretary of Defense. For non-intelligence FGI, exceptions to this limitation can be granted only by the USD(P). Request for exceptions shall be forwarded to the Director, International Security Programs, Defense Technology Security Administration, OUSD(P), for action. Such approvals must be documented and retained by the sponsor.

(2) Using ACCM to protect classified information in acquisition programs as defined in DoDD 5000.01 (Reference (af)).

(3) Using ACCM to protect technical or operational requirements of systems in the acquisition process. Systems in operational use are not viewed as being in the acquisition process. Components of operational systems are fielded end items, not items in the acquisition process, and improvements to fielded items are eligible for ACCM status if properly justified.

(4) Using ACCM to protect Restricted Data (RD), Formerly Restricted Data (FRD),

COMSEC, SCI, SAP, or Nuclear Command and Control Extremely Sensitive Information.

(5) Using ACCM to protect unclassified information.

(6) Using ACCM to preclude or impede congressional, OSD, or other appropriate oversight of programs, command functions, or operations.

(7) Using ACCM to justify funding to procure or maintain a separate ACCM communication system.

f. Documentation

(1) Use of ACCM must be approved in writing by the cognizant DoD Component Head. The correspondence establishing the ACCM shall be signed by the DoD Component Head and shall include the following information:

(a) Unclassified nickname assigned in accordance with Reference (ae).

(b) Designation of the ACCM sponsor. As a minimum, the sponsor shall be a general or flag officer, or senior executive equivalent, who has OCA at the level of or higher than the information protected by the ACCM.

(c) Designation of an ACCM control officer who shall be the organization's point of contact for all matters concerning the ACCM. Subsequent changes in designated personnel shall be provided, in writing, to the Special Programs Office, OUSD(P).

(d) Description of the essential information to be protected by the ACCM.

(e) Effective activation date and expected ACCM duration.

(f) Any planned participation by foreign partners.

(2) The ACCM sponsor shall develop and distribute a program security plan, security classification guide, and program participant briefing to all participating organizations prior to the activation of the ACCM. As a minimum, the briefing will address the specific information that is subject to ACCM security measures.

(3) The Special Programs Office, OUSD(P), shall maintain a central repository of records for all DoD ACCM.

g. Annual Reports of ACCM Use. Not later than December 15 of each year, the DoD Components shall provide a report to OUSD(P) on all ACCM usage during the previous year. The exact format for this report shall be provided annually by OUSD(P), however, the general data elements include: ACCM nickname; purpose and/or description of the ACCM program; expected duration; and ACCM sponsor and ACCM control officer(s).

h. Sharing ACCM-Protected Information. ACCM-protected information may be shared with other DoD Components and/or other Federal government departments and agencies only when the recipient organization agrees to abide by the ACCM security requirements stipulated in this enclosure.

i. Contractor Access to ACCM. DoD contractors may participate in ACCMs, or be directed to participate, only when such access and the associated security plan are identified in the DD Form 254, "Contract Security Classification Specification." Care must be taken to ensure identification of the security plan does not disclose ACCM-protected data.

j. Program Maintenance

(1) ACCM sponsors shall maintain an updated listing of primary and alternate ACCM control officers for each organization to which they have extended their program.

(2) Each organization's ACCM control officer shall maintain an updated ACCM access control list for their organization.

(3) Initial contact between organizations will be between each organization's ACCM control officers. ACCM control officers may authorize action officer to action officer contact once access control lists have been exchanged between organizations.

(4) Personnel requiring access to ACCM-protected information shall receive specialized training upon initial access to the program and annually thereafter. Training, as a minimum, shall address the procedures for access, control, transmission, storage, and marking. Individuals may be required to sign an acknowledgement of training should the security plan so specify.

(5) ACCM documentation (i.e., program security plan and security classification guide) must be updated a minimum of once every 5 years.

(6) ACCM sponsors shall provide the following information, through the DoD Component Head, to OUSD(P) concurrently with the ACCM annual report:

(a) A listing of primary and alternate ACCM control officers for each organization managing an ACCM.

(b) Any updated ACCM documentation or confirmation that program documentation has been reviewed and is current.

k. Safeguarding ACCM Information. The provisions of this Manual regarding the safeguarding of classified information are modified with respect to use of ACCM as follows:

(1) Top Secret, Secret, and Confidential cover sheets (i.e., SFs 703, 704, and 705, respectively) used to cover ACCM material shall be over stamped or marked with "ACCM" and the appropriate nickname. Cover sheets specifically designated by the DoD Components for use with ACCM must be approved by the Director of Security, OUSD(I), prior to use.

(2) ACCM material should be handled and stored based on the security classification of the information contained therein and in a manner that separates it from non-ACCM classified information. Separate GSA approved storage containers are not required so long as everyone with access to container is also approved for access to the ACCM material stored within, but the measures used (e.g., segregated files, separate folders, drawers labeled for ACCM) shall prevent the commingling of ACCM material with other classified documents.

(3) ACCM information shall be transmitted in the same manner as other classified information at the same classification level with the following exceptions:

(a) ACCM information packaged for transmission shall have the inner envelope marked with the appropriate classification, the caveat "ACCM," and the assigned nickname, and shall be addressed to the attention of an individual authorized access to the ACCM information.

(b) The ACCM nickname shall be used in the text of message traffic and on cover sheets accompanying secure facsimile transmissions to assist in alerting the recipient that the transmission involves ACCM-protected information. Senders shall ensure that an authorized recipient is awaiting the transmission when sending via secure facsimile. When using the Defense Message System (DMS), the material must also be marked as "SPECAT" (Special Category) in accordance with the requirements and procedures in CJCSM 5720.01B (Reference (ag)). Due to limits in DMS processing, only one ACCM nickname should be used in a DMS message.

(c) Automated information systems or electronic files containing ACCM protected information shall be configured with appropriate discretionary access controls to ensure that access is restricted to individuals with authorized access.

(d) Secret Internet Protocol Router Network (SIPRNET) or other secure transmission methods authorized for processing information at the required level of classification may be used to transmit ACCM information. Each such transmission must be marked with the caveat "ACCM" and the authorized nickname in accordance with the marking guidance in Volume 2 and transmitted only to those authorized access to the ACCM information.

(e) The method of transmission selected for ACCM information, whether in hardcopy or electronic form, shall be consistent with the security classification assigned. Designation of information as requiring ACCM protection does not, in and of itself, require the transmission of the information by methods usually reserved for a higher level of classified information.

l. Security Incidents. Compromise of ACCM program information can present an immediate and real threat to national security and those personnel involved in mission execution. Anyone finding ACCM material out of proper control shall take actions to safeguard the material and shall immediately notify the local ACCM control officer, if known, or the local security manager.

(1) All reporting, inquiry, investigation, and damage assessment will be conducted per the guidelines contained in Enclosure 6 of this Volume. Any reports containing ACCM information shall be handled in accordance with the requirements of this Manual as modified by this section.

(2) Section 13 of Enclosure 6 of this Volume states the actions to take if unauthorized personnel are inadvertently afforded access to ACCM information. Inadvertent disclosure forms, commonly used with compartmented information, are not authorized for use with ACCM information.

(3) Because ACCM program information is not SCI or SAP, reasonable risk management procedures should be followed when ACCM program information is incorrectly placed on non-approved electronic processing systems or electronically transmitted to non-authorized personnel and/or systems. Deleting the file or material from all affected systems is normally a sufficient action unless the material in question is classified at a higher level of classification than that for which the system is accredited.

(4) The ACCM sponsor should be notified when the local inquiry and investigation is completed. Resolution will be in accordance with current guidance contained in Enclosure 6 of this Volume and must consider the guidance contained in the ACCM program security plan. Responsibility for the damage assessment remains with the ACCM sponsor. Any additional action will be as directed by the ACCM sponsor and the local security manager.

m. ACCM Termination. ACCM shall be terminated by the establishing DoD Component when ACCM security measures are no longer required. Notification of ACCM termination must be submitted, in writing, as required by paragraphs 18.c.(1) and 18.c.(2) of this enclosure.

n. Transitioning an ACCM to a SAP. If, at any point in time, the DoD Component Head determines that information protected by ACCM requires further protection as a SAP, authorization to establish a DoD SAP must be requested in accordance with DoD Directive 5205.07 (Reference (ah)).

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.