CHAPTER 6

SAFEGUARDING

Section 1

Control Measures

6-100 General

a. Components shall have a system of control measures that ensure that access to classified information is limited to authorized persons. The control measures shall be appropriate to the environment in which the access occurs and 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.

b. Foreign government information shall be controlled and safeguarded as described in Section 6 of this Chapter.

6-101 Working Papers

Working papers are documents and material accumulated or created in the preparation of finished documents and material. Working papers containing classified information shall be:

a. Dated when created;

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

c. Protected in accordance with the assigned classification:

d. Conspicuously marked “Working Paper” on the first page of the document in letters larger than the text.

e. Destroyed when no longer needed; and

f. Accounted for, controlled, and marked in the manner prescribed for a finished document of the same classification when retained more than 180 days from date of origin or released by the originator outside the activity.

Section 2

Access

6-200 Policy

Except as otherwise provided in subsection 6-201, below, no person may have access to classified information unless that person has been determined to be trustworthy and access is essential to the accomplishment of a lawful and authorized Government purpose. DoD Regulation 5200.2-R contains detailed guidance concerning personnel security investigation, adjudication and clearance. The final responsibility for determining whether an individual’s official duties require possession of or access to any element or item of classified information, and whether the individual has been granted the appropriate security clearance by proper authority, rests with the individual who has authorized possession, knowledge, or control of the information and not on the prospective recipient.

6-201 Access by Persons Outside the Executive Branch

Classified information may be made available to individuals or agencies outside the Executive Branch provided that such information is necessary for performance of a function from which the Government will derive a benefit or advantage, and that such release is not prohibited by the originating department or agency. Heads of DoD Components shall designate appropriate officials to determine, before the release of classified information, the propriety of such action in the interest of national

security and assurance of the recipient's trustworthiness and need-to-know.

a. Congress. Access to classified information or material by Congress, its committees, members, and staff representatives shall be in accordance with DoD Directive 5400.4. Any DoD employee testifying before a Congressional committee in executive session in relation to a classified matter shall obtain the assurance of the committee that individuals present have a security clearance commensurate with the highest classification of information that maybe discussed. Members of Congress by virtue of their elected positions, are not investigated or cleared by die Department of Defense.

b. Government Printing Office (GPO). Documents and material of all classification maybe . processed by the GPO, which protects the information in accordance with the DoD/GPO Security Agreement of February 20, 1981.

c. Representatives of the General Accounting Office (GAO). Representatives of the GAO maybe granted access to classified information originated by and in the possession of the Department of Defense when such information is relevant to the performance of the statutory responsibilities of that office, as set forth in DoD Directive 7650.1. Certifications of security clearances, and the basis therefor, shall be accomplished pursuant to arrangements between GAO and the DoD Component concerned. Personal recognition or presentation of official GAO credential cards are acceptable for identification purposes.

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

(1) Makes a written determination 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 trustworthy pursuant to paragraph 6-200, above, and DoD 5200.2-R;

(2) Limits such access to specific categories of information over which the DoD Component has classification jurisdiction and to any other category of information for which the researcher obtains the written consent of a DoD Component or non-DoD department or agency that has classification jurisdiction over information contained in or revealed by documents within the scope of the proposed historical research;

(3) Maintains custody of the classified material at a DoD installation or activity *or* authorizes access to documents in the custody of the National Archives and Records Administration;

(4) Obtains the researcher's agreement to safeguard the information and to submit any notes and manuscript for review by all DoD Components or non-DoD departments or agencies with classification jurisdiction for a determination that no classified information is contained therein by execution of a statement entitled, "Conditions Governing Access to Official Records for Historical Research Purposes"; and

(5) Issues an authorization for access valid for not more than 2 years from the date of issuance that may be renewed under regulations of the issuing DoD Component.

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

(1) Makes a written determination 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 trustworthy pursuant to subsection 7-100, below;

(2) Limits such access to specific categories of information over which that DoD Component has classification jurisdiction and to any other category of information for which the former appointee obtains the written consent of a DoD Component or non-DoD department or agency that has classification jurisdiction over information contained in or revealed by documents within the scope of the proposed access;

(3) Retains custody of the classified material at a DoD installation or activity or authorizes access to documents in the custody of the National Archives and Records Administration: and

(4) Obtains the former presidential appointee's agreement to safeguard the information and to submit any notes and manuscript for review by all DoD Component or non-DoD departments or agencies with classification jurisdiction for a determination that no classified information is contained therein.

f. Judicial proceedings. DoD Directive 5405.2 governs the release of classified information in litigation.

g. Other Situations. When necessary in the interests of national security, heads of DoD Components, or their senior agency official, may authorize access by persons outside the Federal Government, other than those enumerated above, to classified information upon determining that the recipient is trustworthy for the purpose of accomplishing a national security objective; and that the recipient can and will safeguard the information from unauthorized disclosure.

6-202 Visits

Heads of 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 will include verification of the identity, personnel security clearance, access (if appropriate), and need-to-know for all visitors.

Section 3

Safeguarding

6-300 General Policy

Everyone who has been granted access to classified information is responsible for providing protection to information and material in their possession or control. that contains such information. Classified information must be protected at all times either by storage in an approved device or facility or having it under the personal observation and control of an authorized individual. Everyone who works with classified information is personally responsible for taking proper precautions to ensure that unauthorized persons do not gain access to it.

6-301 Care During Working Hours

a. Classified material removed from storage shall be kept under constant surveillance of authorized persons. Classified document cover sheets (Standard Forms 703, 704 and 705) will be placed on classified documents not in secure storage.

b. Preliminary drafts, carbon sheets, plates, stencils, stenographic notes, worksheets, typewriter and printer ribbons, floppy disks, and other items containing classified information shall be either destroyed immediate] y after they have served their purpose or protected as required for the level of classified information they contain.

6-302 End-of-Day Security Checks

Heads of activities that processor store classified information shall establish a system of security checks at the close of each working day to ensure that the area is secure' Standard Form 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 the storage of classified material; Standard Form 702, "Security Container Check Sheet," shall be used to record such actions. In addition, Standard Forms 701 and 702 shall be annotated to reflect after-hours, weekend, and holiday activity.

6-303 Emergency Planning

a. Plans shall be developed for the protection, removal, or destruction of classified material in case of fire, natural disaster, civil disturbance, terrorist activities, or enemy action, to minimize the risk of its compromise. The level of detail and amount of testing and rehearsal of these plans should be determined by an assessment of the risk of hostile action, natural disaster, or terrorist activity that might place the information in jeopardy.

b. Planning for the emergency protection (including emergency destruction under no-notice conditions) of classified COMSEC material shall be developed in accordance with requirements of National Telecommunications Information Systems Security Instruction (NTISSI) 4004.

c. When preparing emergency plans, consideration should be given to:

(1) Reduction of the amount of classified material on hand;

(2) Storage of less frequently used classified material at more secure locations; and

(3) Transfer of as much retained classified information to microforms or to removable automated information systems media as possible, thereby reducing its bulk.

6-304 Telephone Conversations

Classified information shall be discussed in telephone conversations only over secure communications circuits approved for transmission of information at the specific level of classification. When discussing classified information on the telephone, the ability of others in the area to overhear what is being said must be considered.

6-305 **Removal of Classified Storage Equipment**

Storage containers that may have been used to store classified information shall be inspected by properly cleared personnel before removal from protected areas or unauthorized persons are allowed access to them. The inspection should ensure that no classified information remains within the equipment.

6-306 **Residential Storage Arrangement**

a. Only the Secretary of Defense, the Secretaries of the Military Departments, the Combatant Commanders and the Senior Agency Official of the DoD Component may authorize removal of Top Secret information from designated working areas in off-duty hours for work at home.

b. Heads of DoD Components or their designees may authorize removal of Secret and Confidential information from designated working areas in off-duty hours for work at home. Authority to approve such removal shall not be delegated below the major command or equivalent level.

c. A GSA-approved security container shall be furnished for residential storage. Written procedures shall be developed to provide for appropriate protection of the information, to include a record of the information that is authorized for removal.

6-307 **Classified Meetings and Conferences**

a. Meetings and conferences that involve classified information present special vulnerabilities to unauthorized disclosure. Heads of the DoD Components shall establish specific requirements for protection of classified information at Component conferences, seminars, exhibits, symposia, conventions, training courses, or other such gatherings during which classified information is disseminated. This does not apply to in-house gatherings, routine gatherings of U.S. Government officials, 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 government contract, program, or project. Requirements developed shall, as a minimum, include a determination that:

(1) The meeting will serve a specific U.S. Government purpose;

(2) The use of other appropriate channels for dissemination of classified information or material are insufficient;

(3) The meeting location will be under the security control of a U.S. Government agency or a U.S. contractor with an appropriate facility security clearance:

(4) Adequate security procedures have been developed and will be implemented to minimize risk to the classified information involved;

(5) Classified sessions shall be segregated from unclassified sessions whenever possible; and

(6) Access to the meeting or conference, or *specific* sessions thereof, at which classified information will be discussed or disseminated, will be limited to persons who possess an appropriate security clearance and need-to-know.

(7) Any participation by foreign nationals or foreign representatives complies with the requirements of DoD Instruction 5230,20 and DoD Directive 5230. 11; e.g., assurance is obtained, in writing, from the responsible U.S. Government foreign disclosure office(s) that the information to be presented has been cleared for foreign disclosure.

(8) Announcement of the classified meeting shall be unclassified and limited to a general description of topics expected to be presented, names of speakers, logistical information, and administrative and security instructions.

(9) Non-government organizations may assist in organizing and provide administrative support for a classified meeting, but all security requirements remain the specific responsibility of the DoD Component sponsoring the meeting.

(10) Procedures must ensure that classified documents, recordings, audiovisual material, notes, and other materials created, distributed, or used during the meeting are controlled, safeguarded, and transported as required by other provisions of this Regulation. Note taking or electronic recording 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.

b. Special requirements apply to meetings, conferences, seminars, and activities other than those described in subparagraph 6-307 a., above, at which classified information is to be presented and discussed as follows:

(1) Meetings must be approved by the head of the DoD Component, a person serving at the level of Deputy Assistant Secretary or above within OSD, the Director of the Joint Staff, the Directors of the Defense Agencies, or the Senior Agency Officials appointed within the Military Departments in accordance with Section 5.6(c) of E.O. 12958.

(2) A DoD official is appointed by the DoD *Component sponsoring the meeting, to serve as* security manager for the meeting and physical security of the actual site of the classified meeting is established and maintained by U.S. Government personnel. Other U.S. Government organizations or cleared DoD contractors with appropriate facility security clearances may assist with implementation of security requirements under the direction of the appointed security manager.

6-308 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 pursuant to DoD Directive 5230.11, and is under the security control of that government or organization, U.S. classified material may be retained in foreign countries only when necessary to satisfy specific U.S. Government requirements. Heads of the DoD Components will prescribe requirements for protection *of* this information, with particular attention to ensuring proper enforcement of controls on release of U.S. classified information to foreign entities. U.S. classified material in foreign countries shall be stored as described in paragraphs a. through d. below. The provisions of Section 4, below, also apply.

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

b. At a U.S. Government activity located in a building used exclusively by U.S. Government tenants, provided the building is under 24-hour control by U.S. Government personnel.

c. At a 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 security containers approved by the GSA and is placed under 24-hour control by U.S. Government personnel.

d. At a U.S. Government activity located in a building not used exclusively by U.S. Government tenants but which is under host government control, provided 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.

6-309 Information Processing Equipment

The Department of Defense has a variety of non-COMSEC-approved equipment *that is used to process* classified information. This includes copiers, facsimile machines, AIS equipment and peripherals, electronic typewriters, word processing systems, and others. Activities must 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 must prescribe the appropriate safeguards to:

a. Prevent unauthorized access to that information.

b. Replace and destroy equipment parts as classified material when the information cannot be removed from them. Alternatively, the equipment may be designated as classified and appropriately protected at the retained information's classification level.

c. Ensure that equipment is inspected by appropriately cleared and technically knowledgeable personnel before the equipment is removed from protected areas.

Section 4

Storage

6-400 General **Policy**

Classified information shall be secured under conditions adequate to prevent access by unauthorized persons. The requirements specified in this Regulation represent acceptable security standards. DoD policy concerning the use of force for the protection of classified information is specified in DoD Directive 5210.56. Weapons or sensitive items such as funds, jewels, precious metals or drugs shall not be stored in the same container used to safeguard classified information. Security requirements for Sensitive Compartmented Information Facilities (SCIFs) are established by the Director of Central Intelligence. Current holdings of classified material shall be reduced to the minimum required for mission accomplishment.

6-401 **Standards for Storage Equipment**

GSA establishes and publishes minimum standards, specifications, and supply schedules for containers, vault doors, modular vaults, alarm systems, and associated security devices suitable for the storage and protection of classified information. DoD Directive 3224.3 describes acquisition requirements for physical security equipment used within the Department of Defense.

6-402 **Storage of Classified Information**

Classified information that is not under the personal control and observation of an authorized person is to be guarded or stored in a locked security container, vault, room, or area, as follows:

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

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

(a) The location that houses the security container shall be subject to continuous protection by cleared guard or duty personnel;

(b) Cleared guard or duty personnel shall inspect the security container once every two hours;

(c) An Intrusion Detection System (IDS) meeting the requirements of Appendix G with personnel responding to the alarm arriving within 15 minutes of the alarm annunciation; or

(d) Security-In-Depth when the GSA-approved container is equipped with a lock meeting Federal Specification FF-L-2740.

(2) Modular vault, vault, or a secure room constructed in accordance with Appendix G and equipped with an IDS with the personnel responding to the alarm within 15 minutes of the alarm annunciation if the area is covered by Security-In-Depth, or a 5 minute alarm response time if it is not. (Other rooms that were approved for the storage of Top Secret in the U.S. may continue to be used.)

(3) New purchases of combination locks for GSA-approved security containers, vault doors and secure rooms shall conform to Federal Specification FF-L-2740. Existing non-FF-L-2740 mechanical combination locks will not be repaired. If they should fail, they will be replaced with locks meeting FF-L-2740.

(4) Under field conditions during military operations, the commander may prescribe the measures deemed adequate to meet the storage standard contained in subparagraphs 6-402a. 1. and 2., above.

b. 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 without supplemental controls;

(3) In secure rooms that were approved for the storage of Secret information by the DoD Components prior to October 1, 1995; or

(4) Until October 1,2002, in a non-GSA - approved container having a built-in combination lock or in a non-GSA approved container secured with a rigid metal lockbar and a GSA-approved padlock with one of the following supplemental controls:

(a) The location that houses the container is subject to continuous protection by cleared guard or duty personnel;

(b) Cleared guard or duty personnel shall inspect the security container once every four hours; or

(c) An IDS with the personnel responding to the alarm arriving within 30 minutes of the alarm.

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

d. Specialized Security Equipment

(1) The Heads of the DoD Components shall, consistent with this Regulation, delineate the appropriate security measures required to protect classified information stored in containers on military platforms or for classified munitions items.

(2) GSA-approved field safes and special purpose one and two drawer light-weight security containers approved by the GSA are used primarily for storage of classified information in the field and in military platforms. Such containers shall be securely fastened to the structure or under sufficient surveillance to prevent their theft.

(3) GSA-approved map and plan files are available for storage of odd-sized items such as computer media, maps, charts, and classified equipment.

(4) GSA-approved modular vaults meeting Federal Specification AA-V-2737 may be used to store classified information as an alternative to vault requirements described in Appendix G.

e. Replacement of Combination Locks. The mission and location of the activity, the classification level and sensitivity of the information, and the overall security posture of the activity determines the priority for replacement of existing combination locks. All system components and supplemental security measures including electronic security systems (e.g., intrusion detection systems, automated entry control subsystems, and video assessment subsystems), and level of operations must be evaluated by the commander when determining the priority for replacement of security equipment. Appendix G, provides a matrix illustrating a prioritization scheme for the replacement of existing combination locks on GSA-approved security containers and vault doors. Priority 1 requires immediate replacement.

f. Storage areas for bulky material containing Secret or Confidential information may have access openings secured by GSA-approved changeable combination padlocks (Federal Specification FF-P- 110 series) or high security key-operated padlocks (Military Specification MIL-P-43607). Other security measures are required, in accordance with subsection 6-308, above.

(1) When special circumstances exist, Heads of DoD Components may authorize the use of key operated locks for the storage of Secret and Confidential information. Whenever such locks are used, administrative procedures for the control and accounting of keys and locks shall be established. The level of protection provided such keys shall be equivalent to that afforded the classified information being protected by the padlock.

(2) Section 1386 of title 18, United States Code, makes unauthorized possession of keys, keyblanks, keyways or locks adopted by any part of the Department of Defense for use in the protection of 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.

6-403 **Procurement of New Storage Equipment**

a. New security storage equipment shall be procured from those items listed on the GSA Federal Supply Schedule. Exceptions may be made by the heads of the DoD Components, with notification to the ASD(C^3I).

b. Nothing in this chapter shall be construed to modify existing Federal supply class management assignments made under DoD Directive 5030.47.

6-404 **Equipment Designations and Combinations**

a. 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 to 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) nor from applying decals or stickers required by the Director of Central Intelligence for containers and equipment used to store or process intelligence information.

b. Combinations to Containers and Vaults

(1) Combinations to security containers, vaults and secure rooms shall be changed only by individuals having that responsibility and an appropriate security clearance. Combinations shall be changed:

(a) When placed in use;

(b) Whenever an individual knowing the combination no longer requires access to it unless other sufficient controls exists to prevent access to the lock; or

(c) When the combination has been subject to possible compromise;

(d) When taken out of service. Built-in combination locks shall then be reset to the standard combination 50-25-50; combination padlocks shall be reset to the standard combination 10-20-30.

(2) The combination of a container, vault or secure room used for the storage of classified information shall be treated as information having a classification equal to the highest category of the classified information stored therein. Any written record of the combination shall be marked with the appropriate classification level.

(3) A record shall be maintained for each vault or secure room door, or container used for storage of classified information, showing location of the door or container, and the names, home addresses, and home telephone numbers of the individuals having knowledge of the combination who arwe to be contacted in the event that the vault, secure room, or container is found open and unattended.. Standard Form 700, "Security Container Information," shall be used for this purpose.

(4) Access to the combination of a vault, secure room or container used for the storage of classified information shall be granted only to those individuals who are authorized access to the classified information to be stored therein or for the purpose of changing combinations or the repair of vaults or security containers..

b. Entrances to secure rooms or areas should be under visual control at all times during duty hours to prevent entry by unauthorized personnel or equipped with electric, mechanical or electromechanical access control devices to limit access during duty hours. Appendix G provides standards for these access control devices; the use of automated systems described therein is encouraged. Electrically actuated locks (e.g., cypher and magnetic strip card locks) do not afford by themselves the required degree of protection for classified information and must not be used as a substitute for the locks prescribed in subsection 6-402, above.

6-405 **Repair of Damaged Security Containers**

Neutralization of lock-outs or repair of any damage that affects the integrity of a security container approved for storage of classified information shall be accomplished only by authorized persons who have been the subject of a trustworthiness determination in accordance with DoD 5200.2-R or are continuously escorted while so engaged.

a. With the exception of frames bent through application of extraordinary stress, a GSA-approved security container manufactured prior to October 1991 (identified by a silver GSA label with black lettering affixed to the exterior of the container) is considered to have been restored to its original state of security integrity if repaired in accordance with Appendix G.

(1) All damaged or altered parts, for example, the locking drawer, drawer head, or lock, are replaced; or

(2) Has been drilled immediately adjacent to or through the dial ring to neutralize a lock-out, a replacement lock meeting FF-L-2740 is used, and the drilled hole is repaired with a tapered, hardened tool-steel pin, or a steel dowel, drill bit, or bearing with a diameter slightly larger than the hole and of such length that when driven into the hole there shall remain at each end of the rod a shallow recess not less than 1/8 inch nor more than 3/16-inch deep to permit the acceptance of substantial welds, and the rod is welded both on the inside and outside surfaces. The outside of the drawer head must then be puttied, sanded, and repainted in such a way that no visible evidence of the hole or its repair remains on the outer surface.

b. In the interests of cost efficiency, the procedures identified in paragraph 6-405 .a.(2)., above, should not be used for GSA-approved security containers purchased after October 1991 (distinguished by a silver GSA label with red lettering affixed to the outside of the container control drawer) until it is first determined whether warranty protection still applies. To make this determination, it will be necessary to contact the manufacturer and provide the serial number and date of manufacture of the

container. If the container is under warranty, a lock-out will be neutralized using the procedures described in the Naval Facilities Engineering Service Center (NFESC) Technical Data Sheet (TDS) 2000-SHR.

c. Unapproved modification or repair of security containers and vault doors is considered a violation of the container's or door's integrity and the GSA label shall be removed. Thereafter, they may not be used to protect classified information except as otherwise authorized in this Regulation.

6-406 **Maintenance and Operating Inspections**

Heads of DoD Components shall establish procedures concerning repair and maintenance of classified material security containers and vaults. vaults.

Section 5

Reproduction of Classified Material

6-500 **Policy**

Documents and other material containing classified information shall be reproduced only when necessary for accomplishment of the organization's mission or for compliance with applicable statutes or directives. Since reproduction equipment and the reproduction process involve substantial risk, heads of the DoD Components shall establish and enforce procedures for reproduction of classified material that limit reproduction to that which is mission-essential and ensure that appropriate countermeasures are taken to negate or minimize risk.
The use of technology that prevents, discourages, or detects unauthorized reproduction of classified information is encouraged.

6-501 Approval for Reproduction

Unless restricted by the originating agency, Top Secret, Secret, and Confidential information may be reproduced to the extent required by operational needs. The DoD Components shall establish procedures that, as a minimum:

a. Ensure compliance with reproduction limitations placed on documents by originators and special controls applicable to Special Access Programs and other special categories of information;

b. Facilitate oversight and control of reproduction of classified material; and.

c. Ensure the expeditious processing of documents in connection with review for declassification.

6-502 **Control Procedures**

The DoD Components shall establish controls to ensure that

a. Reproduction is kept to a minimum consistent with mission requirements;

b. Classified material is not reproduced on equipment that poses unacceptable risks;

c. Personnel doing the reproduction are aware of the risks involved with the specific reproduction equipment and the appropriate countermeasures they are required to take;

d. Reproduced material is clearly identified as classified at the applicable level;

e. Reproduced material is placed under the same accountability and control requirements as apply to the original material; and

f. Waste products generated during reproduction are properly protected and disposed of.

Section 6

Foreign Government Information

6-600 **General**

NATO classified information shall be controlled and safeguarded in compliance with USSAN Instruction 1-69. Other foreign government information shall be controlled and safeguarded in the manner described in this Chapter for U.S. classified information, except as described below. The control and safeguarding requirements for foreign government information may be modified as required

or permitted by a treaty or international agreement, or, for other obligations that do not have the legal status of a treaty or international agreement (e.g., a contract), by the responsible national security authority of the originating government.

6-601 Foreign Government **Top Secret, Secret and Confidential Information**

a. Top Secret

Records shall be maintained 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. Records shall be maintained for five years.

b. Secret

Records shall be maintained of the receipt, distribution, external dispatch and destruction of material containing foreign government Secret information. Other records may be necessary if required by the originator. Secret foreign government information may be reproduced to meet mission requirements. reproduction shall be recorded. Records shall be maintained for three years.

c. Confidential

Records shall be maintained for the receipt and external dispatch of Confidential foreign government information. Other records need not be maintained for foreign government Confidential information unless required by the originating government. Records shall be maintained **for two** years.

6-602 Foreign Government Restricted Information and Information Provided in Confidence

In order to ensure the protection of other foreign government information provided in confidence (e.g., foreign government "Restricted," or foreign government unclassified information provided in confidence), such information must be classified under E.O. 12958. The receiving DoD Component shall provide a degree of protection to the foreign government information at least equivalent to that required by the foreign government or international organization that provided the information. If the foreign protection requirement is lower than the protection required for U.S. CONFIDENTIAL information, the information shall be marked as described in Section 7 of Chapter 5 of this Regulation and the following requirements shall be met:

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

b. 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.

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

6-603 **Third-Country Transfers**

The release or disclosure of foreign government information to any third-country requires the prior written consent of the originating government.

6-604 **Storage**

To the extent practical, foreign government information should 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.

Section 7

Disposition and Destruction of Classified Material

6-700 **Policy**

a. 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 their retention is required by law or regulation. Documents that are no longer required for operational purposes shall be disposed of in accordance with the provisions of the Federal Records Act (44 U.S.C. Chapters21, 31 and 33) and

appropriate implementing directives and records schedules. Material that has been identified for destruction shall continue to be protected, as appropriate, for its classification until it is actually destroyed. Destruction of classified documents and material shall be accomplished by means that eliminate risk of reconstruction of the classified information they contain.

b. Heads of the DoD Components shall ensure that management of retention of classified material is included in oversight and evaluation of program effectiveness. Each activity with classified holdings should establish at least one day each year when specific attention and effort is focused on disposition of unneeded classified material ("clean-out day").

6-701 **Methods and Standards**

a. Classified information identified for destruction shall be destroyed completely to preclude recognition or reconstruction of the classified information in accordance with procedures and methods prescribed by the Head of the DoD Component or their designee. Methods and equipment used to routinely destroy classified information include burning, cross-cut shredding, wet-pulping, mutilation, chemical decomposition or pulverizing.

b. Technical guidance concerning appropriate methods, equipment, and standards for the destruction of classified electronic media, processing equipment components, and the like may be obtained by contacting the Directorate for Information Systems Security, National Security Agency, Ft. Meade, MD 20755. Specifications concerning appropriate equipment and standards for destruction of other storage media may be obtained from the General Services Administration.

Section 8

Alternative or Compensatory Control Measures

6-800 **General**

a. This Chapter prescribes the minimum requirements that will normally be applied for the safeguarding of classified information. Senior Agency Officials may, through issuance of appropriate Component guidelines and, consistent with other provisions of this paragraph and subsection 6-801, below, approve the use of alternative or compensatory security controls to ensure that the protection afforded classified information is sufficient to reasonably deter and detect actual or possible compromise. Approval to use alternative or compensatory control measures shall be documented, to include identification of the actual controls employed, and furnished upon request to other agencies with whom classified information or secure facilities are shared. A copy of this documentation must also be provided to the ASD(C3I) or USD(P), as appropriate, for reporting to the Director, Information Security Oversight Office, consistent with paragraph 1-401 .a. of Chapter 1 of this Regulation.

b. Alternative or compensatory security control measures shall be employed only after consideration of risk management factors such as criticality, sensitivity, and value of the information; analysis of the threats both known and anticipated; vulnerability to exploitation; and countermeasures benefits versus cost.

c. Authority to use any of the following security controls that would extend program-wide and that are program-specific shall require the approval of a Component official with original classification authority. The following security controls may be applied to another DoD Component or another Executive Branch agency, only with the written agreement of that Component or agency. Moreover, the Component instituting use of any of the following controls shall maintain a centralized record that, as a minimum, reflects the control(s) used and the rationale for use. (The provisions of this subparagraph do not apply to the Single Integrated Operational Plan (SIOP).)

(I) Maintenance of lists or rosters of personnel to whom the classified information has been or may be provided.

(2) Using an unclassified nickname to identify classified information requiring the alternative or compensatory protection. (NOTE: Codewords shall not be used for this purpose. Other special terminology or special markings shall not be used except as prescribed for the handling of message traffic, or as authorized by this Regulation)

(3) Requiring that classified information be placed *in sealed envelopes marked only with the* nickname and stored in a manner to avoid commingling with other classified files.

(4) Requiring unique DoD Component oversight or inspection procedures.

d. Alternative or compensatory security controls may be applied to contractors only when specifically identified in the DD Form 254, "Department of Defense Contract Security Classification Specification.".

e. Alternative or compensatory security controls shall not be applied to Restricted Data.

f. Requests to use alternative or compensatory security controls for the safeguarding of NATO or foreign government information shall be submitted through channels to the Deputy to the Under Secretary of Defense (Policy) for Policy Support.

g. Alternative or compensatory security controls shall not preclude, nor unnecessarily impede, Congressional, Office of the Secretary of Defense, or other appropriate oversight of program or activity functions or operations

6-801 Special Access Controls

The following security control measures shall be used only in those instances where a program has been approved in accordance with Chapter 8 of this Regulation as a Special Access Program:

a. Personnel security investigative or adjudicative requirements more stringent than those normally required for a comparable level of classified information;

b. Specialized non-disclosure agreements or briefing *statements;*

c. Use of any special terminology; other than a nickname issued in accordance with established JCS procedures, or as prescribed for the handling of message traffic; or special markings, other than those authorized by this Regulation; to identify or control the dissemination of the information that has been determined to require enhanced security controls.

d. Exclusion of a classified contract from inspection by the Defense Investigative Service (use of a carve-out); or

e. A centralized billet system to control the *number of personnel authorized access.*