CHAPTER 5.

SAFEGUARDING CLASSIFIED INFORMATION

SECTION 1. GENERAL SAFEGUARDING REQUIREMENTS

5-100. General. Employees shall be responsible for safeguarding classified information in their custody or under their control. Individuals are responsible for safeguarding classified information entrusted to them. The extent of protection afforded classified information shall be sufficient to reasonably foreclose the possibility of its loss or compromise.

5-101. Safeguarding Oral Discussions. Employees shall ensure that all cleared employees are aware of the prohibition against discussing classified information over unsecured telephones, in public conveyances or places, or in any other manner that permits interception by unauthorized persons.

5-102. End of Day Security Checks.

a. Employees that store classified material shall establish a system of security checks at the close of each working day to ensure that all classified material and security repositories have been appropriately secured.

b. Employees that operate multiple work shifts shall perform the security checks at the end of the last working shift in which classified material had been removed from storage for use. The checks are not required during continuous 24-hour operations.

5-103. Perimeter Controls. Employees authorized to store classified material shall establish and maintain a system to deter and detect unauthorized introduction or removal of classified material from their facility. The objective is to discourage the introduction or removal of classified material without proper authority. If the unauthorized introduction or removal of classified material can be reasonably foreclosed through technical means, which are encouraged, no further controls are necessary. Employees who have a legitimate need to remove or transport classified material should be provided appropriate authorization media for passing through designated entry/exit points. The fact that persons who enter or depart the facility are subject to an inspection of their personal effects shall be conspicuously posted at all pertinent entries and exits.

a. All persons who enter or exit the facility shall be subject to an inspection of their personal effects, except under circumstances where the possibility of access to classified material is remote. Inspections shall be limited to buildings or areas where classified work is being performed. Inspections are not required of wallets, change purses, clothing, cosmetic cases, or other objects of an unusually personal nature.

b. The extent, frequency and location of inspections shall be accomplished in a manner consistent with contractual obligations and operational efficiency. Inspections may be done using any appropriate random sampling technique. Employees are encouraged to seek legal advice during the formulation of implementing procedures and to surface significant problems to the CSA.

5-104. Emergency Procedures. Employees shall develop procedures for safeguarding classified material in emergency situations. The procedures shall be as simple and practical as possible and should be adaptable to any type of emergency that may reasonably arise. Contractors shall promptly report to the CSA, any emergency situation which renders the facility incapable of safeguarding classified material.

SECTION 2. CONTROL AND ACCOUNTABILITY

5-200. General. Employees shall establish an information management system and control the classified information in their possession.

5-201. Policy. The document accountability system for SECRET material is eliminated as a security protection measure, except for highly sensitive program information and where special conditions exist as approved by the GCA. Employees shall ensure that classified in their custody is used or retained only in furtherance of a lawful and authorized U.S. Government purpose. The U.S. Government reserves the right to retrieve its classified material or to cause appropriate disposition of the material by the employee. The information management system employed by the employee shall be capable of facilitating such retrieval and disposition in a reasonable period of time.

5-202. External Receipt and Dispatch Records. Employees shall maintain a record that reflects (i) the date of the material, (ii) the date of receipt or dispatch, (iii) the classification, (iv) an unclassified description of the material, and (v) the identify of the activity from which the material was received or to which the material was dispatched. Receipt and dispatch records shall be retained for 2 years.

5-203. Accountability for TOP SECRET.

a. TOP SECRET control officials shall be designated to receive, transmit, and maintain access and accountability records for TOP SECRET information. An inventory shall be conducted annually unless written relief is granted by the GCA.

b. The transmittal of TOP SECRET information shall be covered by a continuous receipt system both within and outside the facility.

c. Each item of TOP SECRET material shall be numbered in series. The copy number shall be placed on TOP SECRET documents and on all associated transaction documents.

5-204. Receiving Classified Material. All classified material shall be delivered directly to designated personnel. When U.S. Registered Mail, U.S. Express Mail, U.S. Certified Mail, or classified material delivered by messenger is not received directly by designated personnel, procedures shall be established to ensure that the material is received by authorized persons for prompt delivery or notice to authorized personnel. The material shall be examined for evidence of tampering and the classified contents shall be checked against the receipt. Discrepancies in the contents of a package, or absence of a receipt for TOP SECRET and SECRET material, shall be reported promptly to the sender. If the shipment is in order, the receipt shall be signed and returned to the sender. If a receipt is included with CONFIDENTIAL material, it shall be signed and returned to the sender.

5-205. Generation of Classified Material.

a. A record of TOP SECRET material produced by the employee shall be made when the material is: (i) completed as a finished document; (ii) retained for more than 30 days after creation, regardless of the stage of development; and (iii) transmitted outside the facility.

b. Classified working papers, such as, notes and rough drafts generated by the contractor in the preparation of a finished document shall be: (i) dated when created; (ii) marked with its overall classification, and with the annotation "WORKING PAPERS," and (iii) destroyed when no longer needed.

SECTION 3. STORAGE AND STORAGE EQUIPMENT

5-300. General. This Section describes the uniform requirements for the physical protection of classified material in the custody of contractors. When these requirements are not appropriate for protecting specific types or forms of classified material, compensatory provisions shall be developed and approved by the CSA. Nothing in this Manual shall be construed to contradict or inhibit compliance with the law or building codes. Cognizant security officials shall work to meet appropriate security needs according to the intent of this Manual and at acceptable cost.

5-301. General Services Administration (GSA) Storage Equipment. GSA establishes and publishes uniform standards, specifications, and supply schedules for security containers, vault door and frame units, and key-operated and combination padlocks suitable for the storage and protection of classified information. Manufacturers, and prices of storage equipment approved by the GSA, are listed in the Federal Supply Schedule (FSS) catalog (FSC GROUP 71-Part III). Copies of specifications and schedules may be obtained from any regional office of the GSA.

5-302. TOP SECRET Storage. TOP SECRET material shall be stored in a GSA-approved security container, an approved vault or an approved Closed Area. Supplemental protection is required.

5-303. SECRET Storage. SECRET material shall be stored in the same manner as TOP SECRET material and as follows without supplemental protection:

a. A safe, steel file cabinet, or safe-type steel file container which has an automatic unit locking mechanism. All such receptacles will be accorded supplemental protection during non-working hours.

b. Any steel file cabinet which has four sides and a top and bottom (all permanently attached by welding, rivets or peened bolts so the contents cannot be removed without leaving visible evidence of entry) and is secured by a rigid metal lock bar and an approved key operated or combination padlock. The keepers of the rigid metal lock bar shall be secured to the cabinet by welding, rivets, or bolts, so they cannot be removed and replaced without leaving evidence of the entry. The drawers of the container shall be held securely, so their contents cannot be removed without forcing open the drawer. This type cabinet will be accorded supplemental protection during non-working hours.

5-304. CONFIDENTIAL Storage. CONFIDENTIAL material shall be stored in the same manner as TOP SECRET or SECRET material except that no supplemental protection is required.

5-305. Restricted Areas. When it is necessary to control access to classified material in an open area during working hours, a Restricted Area may be established. A Restricted Area will normally become necessary when it is impractical or impossible to protect classified material because of its size, quantity or other unusual characteristic. The Restricted Area shall have a clearly defined

perimeter, but physical barriers are not required. Personnel within the area shall be responsible for challenging all persons who may lack appropriate access authority. All classified material will be secured in approved repositories during non-working hours.

5-306. Closed Areas. Due to the size and nature of the classified material, or operational necessity, it may be necessary to construct Closed Areas for storage because GSA-approved containers or vaults are unsuitable or impractical. Closed Areas must be approved by the CSA and be constructed in accordance with Section 8 of this chapter. Access to Closed Areas must be controlled to preclude unauthorized access. This may be accomplished through the use of a cleared employee or by a supplanting access control device or system. Access shall be limited to authorized persons who have an appropriate security clearance and a need-to-know for the classified material/information within the area. Persona without the appropriate level of clearance and/or need to know shall be escorted at all times by an authorized person where inadvertent or unauthorized exposure to classified information cannot otherwise be effectively prevented. The Closed Area shall be accorded supplemental protection during non-working hours. During such hours, admittance to the area shall be controlled by locked entrances and exits secured by either an approved built-in combination lock or an approved combination or key-operated padlock. However, doors secured from the inside with a panic bolt (for example, actuated by a panic bar), a dead bolt, a rigid wood or metal bar, or other means approved by the CSA, will not require additional locking devices.

a. Open shelf or bin storage of classified documents in Closed Areas require CSA approval. Only areas protected by an approved intrusion detection system will qualify for such approval.

b. The CSA and the employee shall agree on the need to establish, and the extent of, Closed Areas prior to the award of the contract, when possible, or at such subsequent time as the need for such areas becomes apparent during performance on the contract.

5-307. Supplemental Protection.

a. Intrusion Detection Systems as described in Section 9 of this Chapter shall be used a supplemental protection for all storage containers, vaults and Closed Areas approved for storage of classified material following publication of this Manual.

b. Security guards approved as supplemental protection prior to publication of this Manual may continue to be utilized. When guards are authorized, the schedule of patrol is 2 hours for TOP SECRET material and 4 hours for SECRET material.

c. GSA-approved security containers and approved vaults secured with a locking mechanism meeting Federal Specification FF-L-2740, do not require supplemental protection when

the CSA has determined that the GSA-approved security container or approved vault are located in an area of the facility with security-in-depth.

5-308. Protection of Combinations to Security Containers, Cabinets, Vaults and Closed Areas. Only a minimum number of authorized persons shall have knowledge of combinations to authorized storage containers. Containers shall bear no external markings indicating the level of classified material authorized for storage.

a. A record of the names of persons having knowledge of the combination shall be maintained.

b. Security containers, vaults, cabinets, and other authorized storage containers shall be kept locked when not under the direct supervision of an authorized person entrusted with the contents.

c. The combination shall be safeguarded in accordance with the highest classification of the material authorized for storage in the container. Superseded combinations shall be destroyed.

d. If a record is made of a combination, the record shall be marked with the highest classification of material authorized for storage in the container.

5-309. Changing Combinations. Combinations shall be changed by a person authorized access to the contents of the container, or by the FSO or his or her designee. Combinations shall be changed as follows:

a. The initial use of an approved container or lock for the protection of classified material.

b. The termination of employment of any person having knowledge of the combination, or when the clearance granted to any such person has been suspended or revoked.

c. The compromise or suspected compromise of a container or its combination, or discovery of a container left unlocked and unattended.

d. At other times when considered necessary by the FSO or CSA.

5-310. Supervision of Keys and Padlocks. Use of key-operated padlocks are subject to the following requirements: (i) a key and lock custodian shall be appointed to ensure proper custody and handling of keys and locks used for protection of classified material; (ii) a key and lock control register shall be maintained to identify keys for each lock and their current location and custody; (iii) keys and locks shall be audited each month; (iv) keys shall be inventoried with each changed of custody; (v) keys shall not be removed from the premises; (vi) keys and spare locks shall be protected equivalent to the level of classified material involved; (vii) locks shall be changed or rotated at least

annually, and shall be replaced after loss or compromise of their operable keys; and (viii) making master keys is prohibited.

5-311. Repair of Approved Containers. Repairs, maintenance, or other actions that affect the physical integrity of a security container approved for storage of classified information shall be accomplished only by appropriately cleared or continuously escorted personnel specifically trained in approved methods of maintenance and repair of containers.

a. An approved security container is considered to have been restored to its original state of security integrity if all damaged or altered parts are replaced with manufacturer's replacement or identical cannibalized parts.

b. GSA-approved containers manufactured prior to October 19990, and often referred to as BLACK labeled containers, can be neutralized by drilling a hole adjacent to or through the dial ring of the container, thereby providing access into the locking mechanism to open the lock. Before replacement of the damaged locking mechanism, the drill hole will have to be repaired with a plug which can be (i) a tapered, hardened tool-steel pin, (ii) a steel dowel, (iii) a drill bit, or (iv) a steel ball bearing. The plug must be of a diameter slightly larger than the hole, and of such length that when driven into the hole there shall remain at each end a shallow recess not less than 1/8 inch or more than 3/16 inch deep to permit the acceptance of substantial welds. Additionally, the plug must be welded on both the inside and outside surfaces. The outside of the drawer/door must then be puttied,

sanded, and repainted in such a way that no visible evidence of the hole or its repair remains after replacement of the damaged parts with the new lock.

c. GSA-approved containers manufactured after October 1990 and containers equipped with combination locks meeting Federal specification FF-L-2740 require a different method of repair. These containers, sometimes referred to as RED labeled containers, have a substantial increase in lock protection which makes the traditional method of drilling extremely difficult. The process for neutralizing a lockout involves cutting the lock bolts by sawing through the control drawerhead. The only authorized repair is replacement of the drawerhead and locking bolts.

d. Approved security containers that have been drilled or repaired in a manner other than as described above, shall not be considered to have been restored to their original integrity. The "Protection" label on the outside of the locking drawer's side and the **"General Services Administration Approved Security Container"** label on the face of the top drawer shall be removed.

e. A container repaired using other methods than those described above shall not be used for storage of Top Secret material, but may be used for storage of Secret material with the approval of the CSA and for storage of Confidential material with the approval of the FSO.

f. A list shall be maintained by the FSO of all approved containers which have sustained significant damage. Each container listed shall be identified by giving its location and a description

of the damage. There shall also be on file a signed and dated certification, provided by the repairer, setting forth the method of repair used.

5-312. Supplanting Access Control Systems or Devices. Automated access control systems and electric, mechanical or electromechanical devices which meet the criteria stated in paragraphs 5-313 and 5-314 below may be used to supplant authorized employees or guards to control admittance to Closed and Restricted Areas during working hours. Approval of the FSO is required before effecting the installation of a supplanting access control device to meet a requirement of this Manual.

5-313. Automated Access Control Systems. The automated access control system must be capable of identifying the individual entering the area and authenticating that person's authority to enter the area.

a. Manufacturers of automated access control equipment or devices must assure in writing that their system will meet the following standards before FSO's may favorably consider such systems for protection of classified information:

(1) Chances of an unauthorized individual gaining access through normal operation of the equipment are no more than one in ten thousand.

(2) Chances of an authorized individual being rejected for access through normal operation of the equipment are no more than one in one thousand.

b. Identification of individuals entering the area can be obtained by an identification (ID) badge or card, or by personal identity.

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

(2) Personal identity verification identifies the individual requesting access by some unique personal characteristic, such as, (i) fingerprint, (ii) hand geometry, (iii) handwriting, (iv) retina, or (v) voice recognition.

c. In conjunction with an ID badge/card or personal identity verification, a personal identification number (PIN) is required. The PIN must be separately entered into the system by each individual using a keypad device. The PIN shall consist of four or more digits, randomly selected with no known or logical association with the individual. The PIN must be changed when it is believed to have been compromised or subjected to compromise.

d. Authentication of the individual's authorization to enter the area must be accomplished within the system by comparing the inputs from the ID badge/card or the personal identity verification device and the keypad with an electronic database of individuals authorized into the area. A

procedure must be established for removal of the individual's authorization to enter the area upon reassignment, transfer or termination, or when the individual's personnel clearance is suspended or revoked.

e. Locations where access transactions are, or can be displayed, and where authorization data, card encoded data and personal identification or verification data is input, stored, displayed, or recorded must be protected.

f. Control panels, card readers, keypads, communication or interface devices located outside the entrance to a Closed Area shall have tamper resistant enclosures, be securely fastened to a wall or other structure, be protected by a tamper alarm or secured with an approved combination padlock. Control panels located within a Closed Area shall require only a minimal degree of physical security protection sufficient to preclude unauthorized access to the mechanism. Where areas containing TOP SECRET information are involved, tamper alarm protection is mandatory.

g. Systems that utilize transmission lines to carry access authorization, personal identification, or verification data between devices/equipment located outside the Closed Area shall receive circuit protection equal to or greater than that specified as Grade A by UL.

h. Access to records and information concerning encoded ID data and PINs shall be restricted to individuals cleared at the same level as the highest classified information contained

within the specific area or areas in which ID data or PINs are utilized. Access to identification or authorization data, operating system software or any identifying data associated with the access control system shall be limited to the least number of personnel possible. Such data or software shall be kept secured when unattended.

i. Records reflecting active assignments of ID badges/cards, PINs levels of access, personnel clearances, and similar system related records shall be maintained. Records concerning personnel removed from the system shall be retained for 90 days.

j. Personnel entering or leaving an area shall be required to immediately secure the entrance or exit point. Authorized personnel who permit another individual entrance into the area are responsible for confirming the individual's clearance and need-to-know. During shift changes and emergency situations, if the door remains open, admittance shall be controlled by an authorized employee or guard stationed to supervise the entrance to the area.

5-314. Electric, Mechanical, or Electromechanical Devices. Provided the classified material within the Closed Area is no higher than SECRET, electronic, mechanical, or electromechanical devices which meet the criteria stated in this paragraph may be used to supplant authorized employees or guards to control admittance to Closed Areas during working hours. Devices may be used that operate by either a push-button combination which activates the locking device or by a control card

used in conjunction with a push-button combination, thereby excluding any system that operates solely by the use of a control card.

a. The electronic control panel containing the mechanical mechanism by which the combination is set may be located inside or outside the Closed Area. When located outside the Closed Area, the control panel shall be securely fastened or attached to the perimeter barrier of the area and secured by an approved combination padlock. If the control panel is located within the Closed Area, it shall require only a minimal degree of physical security designed to preclude unauthorized access to the mechanism.

b. The control panel shall be installed in a manner that precludes an unauthorized person in the immediate vicinity from observing the selection of the correct combination of the push buttons, or have a shielding device mounted.

c. The selection and setting of the combination shall be accomplished by an employee who is authorized to enter the area. The combination shall be changed as specified in paragraph 5-309. The combination shall be classified and safeguarded in accordance with the classification of the highest classified material within the Closed Area.

d. Electrical gear, wiring included, or mechanical links (cables, rods, etc.) shall be accessible only from inside the area, or shall be secured within a protective covering to preclude surreptitious manipulation of components.

e. Personnel entering or leaving the area shall be required to immediately lock the entrance or exit point. Authorized personnel who permit another individual entrance into the area are responsible for confirming the individual's personnel clearance and need-to-know. During shift changes and emergency situations, if the door remains open, admittance shall be controlled by an authorized employee or guard stationed to supervise the entrance to the area.

SECTION 6. REPRODUCTION

5-600. General. A classified reproduction control system shall be established that will ensure that the reproduction of classified material is held to the minimum consistent with contractual and operational requirements. Classified reproduction shall be accomplished by authorized employees knowledgeable of the procedures for classified reproduction. The employment of technology that prevents, discourages, or detects the unauthorized reproduction of classified documents is encouraged.

5-601. Limitations.

a. Top Secret documents may be reproduced as necessary in the preparation and delivery of a contract deliverable. Reproduction for any other purpose requires the consent of the GCA.

b. Unless restricted by the GCA, Secret and Confidential documents may be reproduced as follows:

(1) Performance of a prime contract or a subcontract in furtherance of a prime contract.

(2) Preparation of a solicited or unsolicited bid, quotation, or proposal to a U.S. Government agency or prospective subcontractor.

(3) Preparation of patent applications to be filed in the U.S. Patent Office.

c. Reproduced copies of classified documents shall be subject to the same protection as the original documents.

5-602. Marking Reproductions. All reproductions of classified material shall be conspicuously marked with the same classification markings and any special warning notices as the material being reproduced. Copies of classified material shall be reviewed after the reproduction process to ensure that these markings are visible.

5-603. Records. Employees shall maintain a record of the reproduction of all TOP SECRET material. The record shall be retained for two years.

SECTION 7. DISPOSITION AND RETENTION

5-700. General. Classified information no longer needed shall be processed for appropriate disposition. Classified information approved for destruction shall be destroyed in accordance with this Section. The method of destruction must preclude recognition or reconstruction of the classified information or material.

a. All classified material received or generated in the performance of a classified contract shall be returned on completion of the contract unless the material has been declassified, destroyed or retention of the material has been authorized. (See 5-702).

b. Contractors shall establish procedures for review of their classified holdings on a recurring basis to reduce these classified inventories to the minimum necessary for effective and efficient operations. Multiple copies, obsolete material, and classified waste shall be destroyed as soon as practical after it has served its purpose. Any appropriate downgrading and declassification actions shall be taken on a timely basis to reduce the volume and to lower the level of classified material being retained by the contractor.

5-701. Disposition of Classified. Employees shall return or destroy classified material in accordance with the following schedule:

a. If a bid, proposal, or quote is not submitted or is withdrawn - within 180 days after the opening date of bids, proposals, or quotes.

b. If a bid, proposal, or quote is not accepted - within 180 days after notification that a bid, proposal, or quote has not been accepted.

c. If a successful bidder - within 2 years after final delivery of goods and services, or after completion or termination of the classified contract, whichever comes first.

d. If the classified material was not received under a specific contract, such as material obtained at classified meetings or from a secondary distribution center - with 1 year after receipt.

5-702. Retention of Classified Material. Contractors desiring to retain classified material received or generated under a contract may do so for a period of two (2) years after completion of the contract, provided the GCA does not advise to the contrary. If retention is required beyond the two-year period, the contractor must request and receive written retention authority from the GCA.

a. Contractors shall identify classified material for retention as follows:

(1) TOP SECRET material shall be identified in a list of specific documents unless the GCA authorizes identification by subject matter and approximate number of documents.

(2) SECRET AND CONFIDENTIAL material may be identified by general subject matter and the approximate number of documents.

b. Contractors shall include a statement of justification for retention based on the following:

(1) The material is necessary for the maintenance of the contractor's essential records.

(2) The material is patentable or proprietary data to which the contractor has title.

(3) The material will assist the contractor in independent research and development efforts.

(4) The material will benefit the U.S. Government in the performance of other prospective or existing Government agency contracts.

(5) The material is being retained in accordance with the "records retention clause" of the contract.

(6) The material has been authorized for retention for a specific period under the terms of the contract.

(7) The material will benefit the U.S. Government in the performance of another active contract and will be transferred to that contract (specify contract).

5-703. Termination of Security Agreement. Notwithstanding the provisions for retention outlined above, in the event that the facility clearance is terminated, the contractor shall return all classified material in its possession to the UA concerned, or dispose of such material in accordance with instructions from the CSA.

5-704. Destruction. Contractors shall destroy classified material in their possession as soon as possible after it has served the purpose for which it was, (i) released by the government, (ii) developed or prepared by the contractor, and (iii) retained after completion or termination of the contract.

5-705. Methods of Destruction. Classified material may be destroyed by burning, shredding, pulping, melting, mutilation, chemical decomposition, or pulverizing (for example, hammer mills, choppers, and hybridized disintegration equipment). Pulpers, pulverizers, or shredders may be used only for the destruction of paper products. Residue shall be inspected during each destruction to ensure that classified information cannot be reconstructed. Crosscut shredders shall be designed to

produce residue particle size not exceeding 1/32 inch in width (with a 1/64 inch tolerance) by ½ inch in length. Only paper-based products may be destroyed by pulping. High wet strength paper, paper mylar, durable-medium paper substitute, or similar water repellent type papers are not sufficiently destroyed by pulping; other methods such as disintegration, shredding, or burning shall be used to destroy these types of papers. Classified material in microform, that is, microfilm, microfiche, or similar high data density material may be destroyed by burning or chemical decomposition, or other methods as approved by the CSA.

a. Public destruction facilities may be used only with the approval of, and under conditions prescribed by, the CSA.

b. Classified material removed from a cleared facility for destruction shall be destroyed on the same day it is removed.

5-706. Witness to Destruction. Classified material shall be destroyed by appropriately cleared employees of the contractor. These individuals shall have a full understanding of their responsibilities. For destruction of TOP SECRET material, two persons are required. For destruction of SECRET and CONFIDENTIAL material, one person is required.

5-707. Destruction Records. Destruction records are required for TOP SECRET material. The records shall indicate the date of destruction, identify the material destroyed, and be signed by the

individuals designated to destroy and witness the destruction. Destruction officials shall be required to know, through their personal knowledge, that such material was destroyed. At the contractor's discretion, the destruction information required may be combined with other required control records. Destruction records shall be maintained by the contractor for 2 years.

5-708. Classified Waste. Classified waste shall be destroyed as soon as practical. This applies to all waste material containing classified information. Pending destruction, classified waste shall be safeguarded as required for the level of classified material involved. Receptacles utilized to accumulate classified waste shall be clearly identified as containing classified material.