

5 FAH-4 H-200 RECORDS ORGANIZATION

5 FAH-4 H-210 DEPARTMENT OFFICES, FIELD OFFICES, AND POSTS

(CT:RMH-8; 8-13-2008)
(Office of Origin: A/ISS/IPS)

5 FAH-4 H-211 GENERAL

(CT:RMH-8; 8-13-2008)

- a. *As mandated by the Federal Records Act and reflected in 5 FAM 400, the Department must create and preserve records containing adequate and proper documentation of the organization, functions, policies, decisions, procedures, and essential transactions or operations of the Department and posts, and records necessary to protect the legal and financial rights of the U.S. Government and of persons directly affected by the Department's activities.* To ensure the *appropriate* preservation of records, each bureau, office, and post must organize and maintain documentary materials that it produces or receives in accordance with the standards and procedures contained in this handbook and appropriate volumes of the Foreign Affairs Manual and associated handbooks relating to information and security management and policy and procedures. *See 5 FAM 415 and 5 FAH-4 H-113 for definitions of relevant terms used in 5 FAH-4 H-200, including what documentary materials qualify as official "Federal records" also known as "records").*
- b. Unless otherwise specified, these procedures apply to all Department of State domestic offices, including field offices and all Foreign Service posts, missions, special interest sections, international organizations, and other operations such as the Financial Service Centers (FSC). Other agencies at posts abroad must follow their own records management procedures.

5 FAH-4 H-212 RECORDS CREATION - GENERAL METHODS AND PROCEDURES

(CT:RMH-8; 8-13-2008)

The following methods and procedures for the creation of *documentary materials* are to be followed by all offices and posts on a continuing basis:

- (1) Survey of office/post procedures: All existing and proposed office/post procedures are to be subject to continuing examination for their effect on recordkeeping. Wherever possible, such procedures are to be revised, consolidated, or eliminated to prevent the creation of unnecessary records;
- (2) Elimination of duplicate files: Every bureau, office, and post will take positive action to prevent the establishment of, or to eliminate, duplicate files not required for current operating purposes. Proliferation of individual office working files can be controlled through careful planning at the division or branch level and by maximum use of the Department's Central Foreign Policy File;
- (3) Limitation on the number of copies: The number of copies of communications and other documents reproduced and distributed is to be limited to those required on a need-to-know basis. To the extent feasible, control is to be exercised to prevent the reproduction of unnecessary copies. As a general rule, information copies are not to be filed with official records but rather maintained in a chronological, post, or other temporary file which is retained for only a *relatively* short period of time.

5 FAH-4 H-213 SEPARATION BY SECURITY CLASSIFICATION, CHANNEL, AND CAPTION

(CT:RMH-8; 8-13-2008)

Offices and posts must follow pertinent procedures in *5 FAM*, 12 FAM, and associated security handbooks to determine how best to file and adequately protect classified and Sensitive But Unclassified (SBU) material.

5 FAH-4 H-213.1 General

(CT:RMH-8; 8-13-2008)

The following procedures apply to Department offices and posts (see 5 FAH-

4 H-213.2 for additional procedures applicable to Department offices and 5 FAH-4 H-213.3 for those applicable to posts):

- (1) Documents bearing the special distribution captions NO DISTRIBUTION (NODIS) or EXCLUSIVE DISTRIBUTION (EXDIS) shall be treated as NOFORN. These documents must be given the physical protection prescribed by their classification. See 12 FAM 539 for additional guidance;
- (2) Documents bearing the captions STATE DISTRIBUTION ONLY (STADIS), and bearing no other captions, may be filed with unrestricted material of the same security classification, but with access limited to need to know. STADIS materials, which may also be captioned EXDIS, must be given physical security appropriate to their classification; *and*
- (3) All NODIS and EXDIS documents (i.e., telegrams, memoranda and letters) are automatically decapTIONed after five years unless exempted by *the Secretariat Staff (S/ES-S)*. The storage of decapTIONed but still classified documents should afford a level of protection appropriate to their classification.

5 FAH-4 H-213.2 Department Offices

(CT:RMH-8; 8-13-2008)

- a. Action documents and telegrams captioned NODIS and EXDIS are maintained by the Executive Secretariat only. When captioned material is no longer needed, bureaus should destroy their copy(ies).
- b. Special channel messages are distributed from the communications center only to the action bureau. Bureaus having their own channel *are* to establish procedures and guidelines for the security of these messages, how these messages are filed, maintained, and who has access to them. While not all messages will be classified, most contain sensitive information.

5 FAH-4 H-213.3 Posts

(CT:RMH-8; 8-13-2008)

- a. For critical and high threat posts, the segregation of classified and unclassified materials is required to allow for rapid destruction of classified materials.

- b. All other posts can separate or commingle classified and unclassified records based upon ease of destruction in an emergency. Over and above the availability and capability of destruction equipment, probably the most significant factor in separating classified from unclassified is the physical volume of classified records involved.
- c. The following procedures are to be used to process **TOP SECRET** traffic on the **TERP V** systems (TOP SECRET material can only be maintained in paper form. These messages will not be stored on any hard drives, floppies, or other media once *they have* been received and processed):
 - (1) Upon receipt of TOP SECRET traffic, the operator makes sure it is processed and a hard copy is printed;
 - (2) Once the telegram has been printed and stored, the operator retrieves the message and enters the "EDIT" mode. (**NOTE:** The time required for a telegram to be stored will vary on how active the TERP V system is at the time);
 - (3) After entering the edit mode, use the "F6" (Line Delete) key to delete the text of the message, leaving only the header and end of message (EOM) functions. (**NOTE:** If the telegram is more than one section, each section will have to be retrieved and the text deleted);
 - (4) Once all of the text has been deleted, save the remainder of the message using the "FLO" (Save Changes) key. The TERP V system will save the file in the same area on the SCSI drive as it was originally stored; and
 - (5) Exit the Retrieve function and continue with normal processing.
- d. Documents bearing the special distribution captions NO DISTRIBUTION (NODIS) or EXCLUSIVE DISTRIBUTION (EXDIS) are maintained in the Information Program Center (IPC) and kept separate from other documents.
- e. Unclassified and SBU records may be maintained together if all persons having access to those files have been authorized (i.e., have an established need to know, and if security conditions at post warrant such access).
- f. NAROP captioned documents are kept by the action office and afforded physical protection appropriate to their security classification.
- g. Action copies of AGREEMENT, DIRGEN, DISSENT, and ROGER channel messages are not kept in the action office, but in the IPC. Sections may

file dummy copies in their chronological files for sake of continuity.

- h. *The Medical Director (MED)* and *the Bureau of Diplomatic Security (DS)* channel messages are maintained by the action office, with a dummy copy included in the IPC.
- j. All other channel captioned messages are kept in the action office, with a copy included in the IPC.
- k. Certain categories of unclassified files may contain sensitive information, and are stored and handled as if they were classified.
- l. The responsible official at post applies the Terminal Equipment Replacement Program (TERP) "store inhibit" function to those authorized channel caption telegrams that require a dummy copy in the IPC post chronological file and storage of the action copy in the Post Communications Center (PCC). These telegrams are deleted or archived off Classified Information Handling System (CIHS) media once processing is completed.

5 FAH-4 H-213.3-1 Continuous Actions

(CT:RMH-8; 8-13-2008)

- a. The Information Management or Information Program Officer sees that the following actions are taken on a regular basis for the security of information at posts.
 - (1) Keep classified, substantive files to a minimum through periodic review;
 - (2) Accelerate retirement of front office, political, and economic program files;
 - (3) Distribute information copies as "read and destroy" and limit distribution to those who "need-to-know;" and
 - (4) Identify and mark SBU documents and include in the post destruction planning.
- b. Examples of SBU documents include (See 12 FAM for definition of sensitive but unclassified):
 - (1) Blank passports;
 - (2) Consular stamps and seals;

- (3) Biographic or investigative files (including those of other agencies such as DEA, INS, Customs, Legatt, etc.);
- (4) Security investigative files and indices;
- (5) Visa and passport/citizenship fraud files;
- (6) Visa refusal files (categories I and II);
- (7) Immigrant visa control cards (FS-499) (OF-224-B) and immigrant visa petitions with supporting material in visa A-Z files;
- (8) Personnel folders, including those of foreign national employees;
- (9) Leave records;
- (10) Employee medical records;
- (11) Business, commercial, and *public affairs (and former USIS) contact(s) files*; and
- (12) Budget and fiscal (B&F) records, such as representational vouchers, lists of contract employees, and other files showing contacts.

5 FAH-4 H-213.3-2 Planning

(CT:RMH-8; 8-13-2008)

Prior to the establishment, or as a periodic review procedure, of an official file system, the post's security officer and the post's information management or information program officer *must*:

- (1) Verify that the present physical and procedural security is satisfactory as it applies to existing file systems;
- (2) In areas of political instability, review emergency destruction procedures and equipment to *ensure* that all requirements are being met; and
- (3) Brief offices on security of files and *ensure* that the files destruction procedures are covered in the emergency evacuation procedures.

5 FAH-4 H-214 BLOCKING

(CT:RMH-8; 8-13-2008)

- a. *Blocking files facilitates the application of retirement and disposition instructions. When blocking files:*
- (1) *Maintain all official files in one year blocks, based on the calendar year, except where the fiscal year is more appropriate; and*
 - (2) *Organize case files in an "active" or "inactive" mode, or incorporate them into basic program files, as appropriate, using the correct TAGS.*
 - (3) *See 5 FAH-4 H-218 for procedures on nonpaper records.*
- b. *Any exceptions to these requirements, based on small volume or other considerations, require the approval of the Programs and Policy Division (A/ISS/IPS/PP).*

5 FAH-4 H-215 TYPES OF DOCUMENTARY MATERIALS

(CT:RMH-8; 8-13-2008)

"Documentary materials" is a collective term for both "Federal record" and nonrecord materials and encompasses all media on which information is recorded. The Department's documentary materials are filed as:

- (1) Central files;
- (2) Chronological files;
- (3) Program files;
- (4) Reference materials;
- (5) Working files; and
- (6) Personal papers.

5 FAH-4 H-215.1 Central Files

5 FAH-4 H-215.1-1 Department Offices

(CT:RMH-8; 8-13-2008)

- a. There are several major central files in the Department, *including:*

- (1) *The Central Foreign Policy File, for which the automated interface is the SAS (State Archiving System);*
- (2) Personnel Records;
- (3) Financial Records; and
- (4) Other operational records, *such as those noted in 5 FAM 414.6.*

These files reflect the official documentation of an organization's activities in specific areas or missions. These files can be *in electronic* or paper *form*. The offices responsible for these files, such as *the Bureau of Human Resources (HR)* and *the Office of Information Programs and Services (A/ISS/IPS)*, establish the guidelines and procedures for maintenance, retirement, transfer, and retrieval. For specific guidance on these *central* files, contact the responsible offices.

- b. **Decision to Centralize.** The decision to centralize files depends on the type of information and the needs of the bureau or organization to effectively meet its mission. *Additional* factors to be considered in deciding whether or not to centralize include:
 - (1) Size and location of the organizational elements within a bureau;
 - (2) Degree of physical protection needed;
 - (3) Adequacy of space and filing facilities;
 - (4) Adequacy of human resources to manage the files; and,
 - (5) Training and experience in maintaining files.
- c. **File management:** Each program, bureau, or office that maintains a major central file must assign a responsible person to manage the operations of the file, ensure the integrity of the data, and assist in access to, filing, and disposition of data. The responsible person must have received training in the basic practices and principles of records management and maintain active contact with A/ISS/IPS.
- d. **File contents and arrangement:** *If a central file is authorized, it must contain all materials within its scope that are "records" as defined in 5 FAM 415.1 and 5 FAH-4 H-113, such that the documentation is complete and accurate to the extent required to cover the scope of the issues described above in 5 FAH-4 H-211.* Division of records between a central file and an operating unit's subject/program or working files can lead to duplication and lack of central integrity of information, as well as inhibiting effective retrieval. Offices must see that procedures exist that

explain to all personnel the operations of the central file.

5 FAH-4 H-215.1-2 Posts

(CT:RMH-8; 8-13-2008)

- a. The establishment of central files at post is the exception to the rule (e.g., a very small post which houses all records in the *Information Program Center (IPC)*).
- b. **Contents and completeness:** *If a central file is authorized, it must contain all materials within its scope that are official "records" as defined in 5 FAM 415.1 and 5 FAH-4 H-113, such that the documentation of the post's business is complete and accurate to the extent required to cover the scope of the issues described above in 5 FAH-4 H-211. Refer to 5 FAH-4 H-215.3-2 for procedures when files are not centralized.*
- c. **File management:** The officer in charge of the post's IPC is designated as the post records officer. The officer must have experience and training in management of records. This person is responsible for:
 - (1) Maintaining the central file, providing for the integrity of the data, assisting in access to, filing, and disposition of data. This person must maintain active contact with A/ISS/IPS, coordinate on-site training in records management, and provide technical assistance to post personnel;
 - (2) Coordinating the annual disposal of records and retirement of records to the Department's Records Service Center;
 - (3) Working with post security to provide adequate enforcement of security over records;
 - (4) Reporting in even-numbered years the status of records in the Biennial Records Report. See 5 FAH-4 H-312.3.

5 FAH-4 H-215.2 Chronological Files

(CT:RMH-8; 8-13-2008)

- a. **Contents.** A chronological file (*or "chron file"*) typically consists of duplicate information copies of incoming and outgoing communications, *such as* telegrams, letters, or reports. Chronological files are a valuable tool for quick retrieval of current information. *Although chronological files do not often contain materials requiring long-term preservation, the contents of a chronological file nonetheless may qualify as Federal*

"records" as defined in 5 FAM 415.1 and 5 FAH-4 H-113, such that even their disposition in the short term might be regulated. The chronological files of Department principals are permanent records that may never be destroyed. See 5 FAM 400 and 5 FAH-4 H-300 for more information on disposition and destruction of Department records.

b. File Management:

- (1) Department offices: Chronological files are usually maintained by a designated person, such as an *office management specialist (OMS)*, who is responsible for their integrity, upkeep, security, and disposition. Chronological files may be kept in a centralized file or with office program files; and
- (2) Posts: Chronological files are usually maintained by a designated person, such as an *OMS* or information management officer, who is responsible for their integrity, upkeep, security, and disposition.

c. File arrangement: By their nature, chronological files are usually maintained by date order. The file may also be arranged in separate incoming and outgoing series, alphabetically by post, or by serial number.

d. Security: Chronological files *often* contain both unclassified and classified documents. Top Secret and special captioned documents are maintained separately (see 5 FAH-4 H-213).

5 FAH-4 H-215.3 Program Files

5 FAH-4 H-215.3-1 Department Offices

(CT:RMH-8; 8-13-2008)

a. Content: Program files consist of records relating directly to an organization or bureau's specific mission and *are typically* maintained *throughout various* offices within an organization. They are the official documentation of that organization's activities. *Collectively they must contain all materials within the organization's scope that are its official "records" as defined in 5 FAM 415.1 and 5 FAH-4 H-113, such that the documentation of the organization's activities is complete and accurate to the extent required to cover the scope of the issues described above in 5 FAH-4 H-211. For example,* information copies of documents that do not relate to the operations of an organization are to be destroyed, while those that do relate *and warrant preservation as "records"* are to be filed with appropriate program material. *To the extent record copies are not maintained elsewhere, material in an organization's chronological files*

and working files (described below) form part of its program files.

- b. **File management:** Each program, bureau, or office that maintains program files must assign a person to be responsible for managing the operations of the files, ensure the integrity of the data, assist in access, filing, and disposition of data. The responsible person must receive training in the basic practices and principles of records management and maintain a liaison with A/ISS/IPS.
- c. **File arrangement:** Program records are filed according to their general informational, or subject content. They can be arranged *by* subject, chronologically, or by case.

5 FAH-4 H-215.3-2 Posts

(CT:RMH-8; 8-13-2008)

- a. The following procedures *apply to posts that do not centrally maintain all their major files:*
 - (1) Program files consist of records relating directly to post mission and are maintained in each section of the post. They are the official documentation of post activities. *Collectively they must contain all materials that are the post's official "records" as defined in 5 FAM 415.1 and 5 FAH-4 H-113, such that the documentation of the post's activities is complete and accurate to the extent required to cover the scope of the issues described above in 5 FAH-4 H-211; and*
 - (2) Program files kept in sections usually consist of: administrative, consular, political, security, commercial, economic, *and* personnel files. *(Other agencies at posts abroad follow their own records management procedures, and may similarly keep their records in a decentralized manner.)* Posts may decide to centrally locate only those records that are security sensitive.
- b. **File Management.** Each section that maintains program files must assign a responsible person to manage the operations of the files, ensure the integrity of the data, assist in access to, filing, and disposition of data. The responsible person must have received training from the post IPC *or A/ISS/IPS* in general records management policies and procedures and maintain active contact with *the post IPC. Records managers at post must assist in fulfilling the records management duties* outlined in 5 FAH-4 H-215.1-2, paragraph c, File Management. The post information management or information program officer remains the primary single contact with the Department regarding records. Additionally, the

responsible person must assist in periodic reporting of record holdings (see 5 FAH-4 H-312.3).

5 FAH-4 H-215.4 Reference Material

(CT:RMH-8; 8-13-2008)

Reference materials consist of magazines, books, and other types of publications, visuals, etc., that provide background information pertinent to an organization's mission *and do not meet the definition of "records" in 5 FAM 415.1 and 5 FAH-4 H-113. For example, reference materials include: extra copies of documents kept solely for convenience of reference; stocks of publications such as annual reports, brochures, handbooks, posters, and maps; and library or museum materials intended solely for reference or exhibit. Reference materials are kept for as long as they provide information of value to an organization, but are not to be retired with official files.*

5 FAH-4 H-215.5 Working Files

(CT:RMH-8; 8-13-2008)

a. **General:** Working files are *defined in 5 FAM 415.1. They are to be kept to an absolute minimum consistent with operating needs and the record-making duties described in 5 FAM and 5 FAH-4. Because material in working files may constitute "records" as defined in 5 FAM 415.1 and 5 FAH-4 H-113, employees must screen out any nontransitory record material for incorporation in the appropriate program file and destroy the remainder of the working file when projects or assignments are completed. As noted in 5 FAM 415.1, working papers would constitute records when they:*

- (1) Are circulated to other employees for approval, comment, action, recommendation, or follow-up, or to communicate with Department personnel about Department business; and*
- (2) Contain information such as substantive annotations or comments that adds to a proper understanding of the Department's formulation and execution of policies, decisions, actions or responsibilities.*

For examples of nonrecord material from working files, see 5 FAH-4 H-216. Some materials within working files might be appropriate for incorporation with reference materials, listed above in 5 FAH-4 H-215.4. If there are no centralized office files, the officer's working files become the program files of the office.

- b. **Content:** Working files usually consist of *material such as:*
- (1) Copies of communications and correspondence;
 - (2) Publications of the Department, other Federal agencies, *and other entities (e.g., foreign governments, international organizations, and private sector or non-governmental organizations);*
 - (3) Newspaper clippings;
 - (4) Reference materials *and background data; and*
 - (5) *Preliminary drafts, rough notes, and similar materials.*
- c. **File management:** Offices and posts may allow management of working files to be handled by individual employees. Offices, however, *should* establish written policies regarding managing the working files belonging to retiring or resigning personnel or upon an employee's departure *from the office.*

5 FAH-4 H-215.6 Personal Papers

(CT:RMH-8; 8-13-2008)

- a. **Content:** Personal papers *are* documentary materials of a private or non-public nature that have not been used in the transaction of Department of State business *and do not contain classified or otherwise sensitive information. They are papers of a personal nature that pertain only to an individual's private affairs or employment but are kept in the office of a Department employee in a bureau, office, or post. If material qualifies as a personal paper, it is not an official Department record—but whether some work-related materials qualify as personal papers can be a complex determination. If there is any doubt whether certain personal papers or files may also be Department records, they should be treated as records until the Records Officer can be consulted.* Personal papers include:
- (1) **Papers created or received before entering Government service:** These papers must not have been used subsequently in the transaction of Department business. Examples include work files from previous employment, political materials, and reference files;
 - (2) **Purely private papers brought into, created, or received in the office:** Examples include family and personal correspondence, documents relating solely to outside business interests or political

and professional activities, manuscripts and drafts for articles and books *written in a private capacity*, and volunteer and community service records. *To be personal papers*, these *materials* must not be related to or used in the transaction of Department business. Correspondence or e-mail received or sent *in an employee's capacity* as a Department official is not personal. *Nor are "official-informal" materials;*

- (3) **Personal copies of employment-related records:** Examples include personal copies of financial disclosure forms, travel vouchers, or health insurance forms and literature.
- (4) **Journals, *personal* notes, personal calendars and appointment schedules:** *Only* if they are for personal use and not prepared *or used* for, or communicated in *the course of*, transacting Department business. This is the most complex category of personal papers and often requires consultation with the Department Records Officer and the Office of the Legal Adviser. Whether these papers are personal or official depends upon an assessment of several factors including their creation, content, purpose, distribution, maintenance, use, disposition, and control.

b. File management:

- (1) Personal papers must be filed separately from *official files and clearly marked "Personal papers of _____ (insert employee's name)." Maintain personal e-mail or electronic documents in a separate folder clearly marked "Personal." There is no guarantee of privacy for personal materials maintained on a Department computer;*
- (2) If information about both private matters and Department business appears in a document, *any portion pertaining to the official activities of the Department and appropriate for preservation* is to be copied or extracted and incorporated into the *Department's official records*.

5 FAH-4 H-216 NONRECORD MATERIALS

(CT:RMH-8; 8-13-2008)

- a. **Content:** Nonrecord materials are Department-owned documentary materials that do not meet the legal definition of a record *in 5 FAM 415.1 and 5 FAH-4 H-113*. Non-record materials include:

- (1) *Reference material. See 5 FAH-4 H-215.4; and*
- (2) *Some materials in working files, as described in 5 FAM 415.1 and 5 FAH-4 H-215.5. Examples of such non-record material are: preliminary drafts that either were not circulated or do not contain information that adds to a proper understanding of the Department's formulation and execution of basic policies, decisions, actions, or responsibilities; information copies of correspondence, directives, forms, and other documents on which no administrative action is recorded or taken (e.g., many FYI e-mails); routing slips and transmittal sheets adding no information meriting preservation to that contained in the transmitted material; duplicate copies of documents maintained in the same file; and physical material lacking evidentiary value.*

b. File management:

- (1) *As a general rule, non-record documentary materials are to be kept only for convenience or reference purposes and are to be destroyed when no longer needed;*
- (2) *Preservation and disclosure of non-record materials is nevertheless sometimes required by law:*
 - (a) *Although the Department need not preserve non-record material under the laws pertaining to federal records management generally, no documentary material (whether record or nonrecord) may be destroyed if it is:*
 - (i) *Relevant to any ongoing or specifically foreseeable civil litigation or criminal prosecution;*
 - (ii) *Responsive to a pending Freedom of Information Act or Privacy Act request;*
 - (iii) *Responsive to a pending Congressional document request or subpoena; or*
 - (iv) *In other situations as may be instructed by the Office of the Legal Adviser;*
 - (b) *Mandated searches for material in Department files must be reasonably calculated to yield all extant responsive material in the Department's possession or control, "record" and "nonrecord" alike;*
- (3) *Departing officials may request Department authorization to*

remove copies of unclassified, nonrecord material as provided in 5 FAH-4 H-217.

5 FAH-4 H-217 REMOVAL OF PERSONAL PAPERS AND NON-RECORD MATERIAL

5 FAH-4 H-217.1 Responsibilities

(CT:RMH-8; 8-13-2008)

- a. The administrative section of each Department of State bureau, office, or post, is responsible for:
 - (1) Reminding all officials, about to leave the Department or a post, of the requirements for the removal of personal papers and nonrecord materials;
 - (2) Enforcing compliance with these procedures for the removal of documentary materials prior to execution of the Separation Statement (Form OF-109);
 - (3) Reviewing materials proposed for removal for all officials except Presidential appointees, located in Washington, DC, who were confirmed by the Senate; and
 - (4) Ensuring that departing officials receive a mandatory briefing and that all departing officials will execute a Form SF-312, Classified Information Nondisclosure Agreement certifying that they have not retained in their possession classified or administratively-controlled documents.
- b. The Department of State records officer (A/ISS/IPS), assisted by the Office of the Legal Adviser (*L*), the Executive Secretariat (*S/ES*), and DS, has oversight responsibility for the removal of documentary materials and provides overall guidance.
- c. Departing officials must ensure that all record material that they possess is incorporated in the Department's official files and that all file searches for which they have been tasked have been completed, such as those required to respond to FOIA, Congressional, or litigation-related document requests. *Fines, imprisonment, or both may be imposed for the willful and unlawful removal or destruction of records as stated in the U.S. Criminal Code (e.g., 18 U.S.C., section 2071).*

5 FAH-4 H-217.2 Removal Procedures

(CT:RMH-8; 8-13-2008)

- a. Classified information: All Department of State employees are responsible for relinquishing all classified and administratively controlled documents at separation, including copies of classified documents. The following guidance applies to the declassification and access to classified documents after departure:
- (1) An individual may request the declassification of specified documents, but the documents must not be removed until they have been declassified and their removal as nonrecord copies is authorized as required by these procedures;
 - (2) Department of State officials appointed by the President and confirmed by the Senate who wish, after their departure, to have access to classified documents they originated, reviewed or signed while serving as a Presidential appointee, may apply for such access in accordance with 22 CFR 171.25.
- b. Unclassified papers and materials:
- (1) The departing official or a staff member must prepare an inventory of personal papers and nonrecord materials proposed for removal. The inventory need not be a listing of documents, but rather a description of categories of documents (e.g., resumes, personal correspondence, documents related to financial disclosure, and copies of speeches”);
 - (2) When the inventory is completed, the departing official must request a review of the materials proposed for removal. In the Department, the records officer in cooperation with the *S/ES* or appropriate administrative office will conduct the review for Presidential appointees confirmed by the Senate. The administrative or executive office conducts the review for other Department officials and/or employees. At Foreign Service posts and domestic field offices, the administrative officer will conduct the review for all officials. Reviewing officials will consult with the Department’s records officer as necessary;
 - (3) The purpose of the review is to certify that the documentary materials proposed for removal may be removed without diminishing the official records of the Department; violating national security, privacy or other restrictions on disclosure; or exceeding normal administrative economies. This generally requires a hands-

on examination of the materials to verify the accuracy of the inventory;

- (4) Once the reviewing official is satisfied that documentary materials proposed for removal comply with Federal law and regulations the reviewing official completes Form DS-1904, Authorization for the Removal of Personal Papers and Non-Record Materials, and forwards the form and the inventory to the Department of State records officer.
- c. Nonrecord materials may be removed only when authorized by the Department and only to the extent that their removal does not:
- (1) Diminish the official records of the Department;
 - (2) Violate confidentiality required by national security, privacy or other restrictions on disclosure (e.g., commercial or financial information, personnel files or investigative records);
 - (3) Exceed normal administrative economies (a charge for excessive copies is within the discretion of the Department).
- d. The Department's records officer or administrative officer reviews the inventory, examines the materials further if necessary, and certifies the materials for removal by signing Form DS-1904, Authorization for the Removal of Personal Papers and Non-Record Materials. A copy of Form DS-1904 and the inventory are given to the departing official and a copy is retained in the reviewing office.

5 FAH-4 H-218 NONPAPER RECORDS

(CT:RMH-8; 8-13-2008)

- a. *Documentary material can constitute a record as defined in 5 FAM 415.1 and 5 FAH-4 H-113 regardless whether it exists in paper form.* Many records of both temporary and long-term value are stored in electronic media, *such as* floppy (flexible) disks, hard disks, optical disks, CD-ROM, thumb drives, and audio, video or magnetic tapes. These records can be duplicates of paper records or can be major information systems. Electronic records, *like any Department records*, can cover a variety of subjects from purely administrative matters to foreign policy. They can be created, *for example*, as word processing documents, spreadsheets, or on databases. *5 FAM 400 provides guidance on electronic records management, including management of e-mail.*

- b. *Given ongoing developments in electronic record-keeping practices and requirements, it is critical that bureaus, offices, and posts coordinate closely with A/ISS/IPS on issues of electronic records management. In addition to ensuring the Department's compliance with all relevant obligations, A/ISS/IPS can provide offices upon request with copies of relevant guidance contained in OMB Circular A-130, Chapter 36 of the Code of Federal Regulations (especially the requirements of 36 C.F.R. Part 1234), and various regulatory bulletins from the General Services Administration and National Archives and Records Administration. GSA's publication: "Applying Technology to Records Systems—A Media Guideline" (KML-93-1-R) also contains information on electronic records.*

5 FAH-4 H-218.1 File Management

(CT:RMH-8; 8-13-2008)

- a. Department offices and posts usually allow management of electronic files to be handled by system managers. Offices and posts, however, are to establish written *policies in coordination with A/ISS/IPS* regarding the disposition and review of these files to see that unique records are properly preserved.
- b. Electronic files are usually accessible by date or through an index or key words for retrieval:
- (1) Department offices *must* establish procedures for the retention of on-line or off-line storage of electronic records in conjunction with A/ISS/IPS;
 - (2) Posts *must* establish procedures for the retention of on-line or off-line storage of electronic records and coordinate with the post information management or information program officer and post systems manager (if any), *who in turn must coordinate with A/ISS/IPS.*

5 FAH-4 H-218.2 Security

(CT:RMH-8; 8-13-2008)

- a. Special precaution is given to the security of electronic records. Because of the ability to compact large volumes of records onto small media, if compromised, more data can be exposed than in a paper file. Such laws and regulations as the Computer Fraud and Abuse Act of 1986, Computer Security Act of 1987, OMB Circular A-130, and *22 C.F.R. Part 1234* address guidelines and procedures that are used by records managers

and systems administrators in protecting electronic records.

- b. Additional guidance, pertinent to the Department, can be obtained from the *Office of Security Technology (DS/C/ST)*.

5 FAH-4 H-218.3 Selection and Maintenance of Electronic Records Storage Media

(CT:RMH-8; 8-13-2008)

- a. Based upon guidance contained in *22 C.F.R. Part 1234*, administrators of electronic record systems *must* select appropriate media and systems for storing Department records throughout their life cycle, which meet the following requirements:
- (1) Permit easy retrieval in a timely fashion;
 - (2) Facilitate distinction between record and nonrecord material;
 - (3) Retain the records in a usable format until their authorized disposition date; and
 - (4) *If the media contains permanent records and does not meet the requirements for transferring permanent records to the National Archives and Records Administration (NARA), permit the migration of the permanent records at the time of transfer to a medium which does meet the requirements.* Contact A/ISS/IPS for more information on these transfer requirements.
- b. The following factors are to be considered before selecting a storage medium or converting from one medium to another:
- (1) The authorized life of the records, as determined during the scheduling process;
 - (2) The maintenance necessary to retain the records;
 - (3) The cost of storing and retrieving the records;
 - (4) The record's density;
 - (5) The access time to retrieve records;
 - (6) The portability of the medium (that is, selecting a medium that will run on equipment offered by multiple manufacturers) and the ability to transfer the information from one medium to another

(such as from optical disk to magnetic tape); and

- (7) Whether the medium meets the current applicable Federal Information Processing Standards (FIPS). Contact *A/ISS/IPS* for information and copies of FIP standards.

c. Administrators *and users* of electronic records systems:

- (1) *Should* avoid the use of floppy disks for the exclusive long-term storage of permanent or unscheduled electronic records;
- (2) *Must ensure* that all authorized users can identify and retrieve the information stored on diskettes, removable disks, tapes, or other media by establishing or adopting procedures for external labeling;
- (3) *Must ensure* that information is not lost because of changing technology or deterioration by converting storage media to provide compatibility with the agency's current hardware and software. Before conversion to a different medium, administrators must determine that the authorized disposition of electronic records can be implemented after conversion;
- (4) *Must* back up electronic records on a regular basis to safeguard against loss of information due to equipment malfunctions or human error. Duplicate copies of permanent or unscheduled records *must* be maintained in storage areas separate from the location of the records that have been copied; and
- (5) *Must comply with the requirements at 22 C.F.R. section 1234.30(g) and (h) regarding maintenance and labeling of magnetic computer tape and direct access storage media.*

5 FAH-4 H-218.4 Facsimile Transmissions

(CT:RMH-8; 8-13-2008)

- a. The method of transmitting a document does not relieve sending or receiving offices of their responsibility for adequately and properly documenting official actions and activities and for ensuring the integrity of records.
- b. Personnel using *facsimile (fax)* machines to transmit memorandums, letters, or other documents that fall within the definition of a Federal record are responsible for:
 - (1) Obtaining appropriate clearances;

- (2) Assuring that all appropriate offices receive copies of documents transmitted; and
 - (3) Providing copies of official written documentation, e.g., congressional correspondence, diplomatic notes, general correspondence, memoranda, and intelligence reports to A/ISS/IPS/AAS, for inclusion in the Department's central foreign policy file.
- c. Copies of documents *transmitted by facsimile can qualify as "records" as defined in 5 FAM 415.1 and 5 FAH-4 H-113:*
- (1) *Facsimile materials of merely transitory value need not be filed, however. Transitory documents are those of short term interest (180 days or less) with minimal or no documentary or evidential value, and often relate to matters on which no documented action is taken. They may be destroyed when no longer needed;*
 - (2) This guidance does not apply to advance copies of documents where no action is taken until receipt of the official document. Such advance copies are non-record materials and may be destroyed upon receipt of the official document;
 - (3) This guidance does, *however*, apply to advance copies of documents if the receiving office circulates the advance copy for official purposes such as approval, comment, action, recommendation, or follow-up. In such instances, the advance copy *can constitute an official record that* is to be filed.

5 FAH-4 H-218.5 Oral Histories

(CT:RMH-8; 8-13-2008)

- a. **Content:** Oral history materials refer to all documents, regardless of media, pertaining to interviews developed expressly for historical purposes. Such interviews are initiated with systematic questions and conducted by historians to obtain and record verbatim information from people who have participated in, or been witness to events, situations, and activities that the Department deems historically significant. Planning documents, interview scripts, and indices which may be accumulated in connection with oral histories are part of the Department's documentation.
- b. **File management:** *The Deputy Assistant Secretary for Information Sharing Services (A/ISS)* is responsible for establishing standards for oral histories in conjunction with the Office of the Historian *(PA/HO)*.

- c. **File arrangement and blocking:** There is no special blocking required for these records. It is required only that they be arranged in some logical sequence.

5 FAH-4 H-219 UNASSIGNED