DEPARTMENT OF HOMELAND SECURITY

RECORDS MANAGEMENT HANDBOOK

V. 2 January 2005

0550 Publication

Table of Contents

CHAPTER 1: OVERVIEW

1. **Purpose.** This guidance contains mandatory Department of Homeland Security (DHS) procedures for managing records effectively and efficiently throughout their life cycle. These procedures will help DHS successfully accomplish its mission, preserve official records in accordance with applicable statutory and regulatory requirements, and promote access to information by DHS staff and the public as appropriate.

2. **Authority.** The management of Federal records at DHS will comply with 44 U.S.C. Chapters 21, 29, 31, 33 and 35 and 18 U.S.C. Chapter 101, and regulations established by the National Archives and Records Administration (NARA) for managing Federal records as stated in 36 C.F.R. parts 1220, 1222, 1224, 1226, 1228, 1230, 1232, 1234, and 1236.

3. **Policy**

   a. DHS will establish and maintain an active Records Management (RM) program for the economical and efficient management of its records. DHS will establish effective management controls over the creation, maintenance, and use of records in any medium, including electronic and microform media, throughout their life cycle.

   b. The provisions of this directive are mandatory and are applicable to all Organizational Elements of DHS.

   c. All Government employees and contractors are required by law to create and preserve records containing adequate and proper documentation of the organization, functions, policies, decisions, procedures, and essential transactions of the agency. In addition, Federal regulations govern the life cycle of these records: they must be properly stored, preserved, and available for retrieval, and may be disposed of only in accordance with NARA-approved Records Control Schedules.

   d. DHS will cooperate with NARA and other agencies in applying standards, procedures, and techniques to improve the management of records; promote the maintenance of those records of continuing value (permanent); and facilitate the segregation and disposal of temporary records.

   e. All records, including electronic, microform media, and information created will be systematically identified, and appraised, with NARA-approved retention periods published in a Records Control Schedule (RCS).

   f. DHS will establish and maintain a vital records program to ensure continuity of essential DHS activities during and following a national emergency or local natural or technological disaster. DHS vital records will be identified, protected, and secured in locations geographically separated from the original records. Plans for automated information systems will include provisions for reasonable continuity of support through backups and/or duplicate copies should their normal operations be disrupted in an emergency.

   g. Files management standards and procedures will be established for maintaining DHS records in a manner that facilitates ease of use, access and disposition, and that is consistent with the regulations and guidelines promulgated by NARA or other regulatory agencies.

h. The laws, regulations, and policies that apply to records maintained and used by DHS also apply to DHS records maintained and used on behalf of DHS by DHS contractors.

i. DHS will include the life cycle of the records when planning for manual or automated information systems. DHS will incorporate records management and archival functions into the design, development, and implementation of information systems (See OMB Circular A-130). DHS Records Managers must be included in the initial planning to ensure the records created or generated are properly scheduled and that migration strategies are considered for long-term records.

j. Records are broadly defined by statute and regulation to include all recorded information, regardless of medium or format, made or received by DHS under Federal law or in connection with the transaction of public business, either preserved or appropriate for preservation because of their administrative, legal, fiscal or informational value. Records serve as the DHS memory; they are of critical importance in ensuring that DHS continues to function effectively and efficiently.

k. DHS officials are responsible for incorporating into the records of the Department all essential information on their major actions. Significant decisions and commitments reached orally or by informal electronic mail will be documented and included in the record. Minutes will be taken at important meetings, and these, together with a copy of the agenda and all documents considered at or resulting from such meetings, will be made part of the record.

l. The programs, policies and procedures of DHS will be adequately documented in appropriate directives. A record copy of each such directive and supporting documentation, including those superseded, will be maintained as a part of the official files.

m. DHS will take appropriate action, such as training and guidance, to ensure that all staff are capable of identifying Federal records. For electronic mail systems, DHS will ensure that all staff are informed of the potential record status of messages, transmittal and receipt data, directories, and distribution lists.

4. Materials to be managed under this guidance

a. Identifying Federal records.

(1) Documentary materials are records when they meet both of the following conditions:

(a) They are made or received by an agency of the United States Government under Federal law or in connection with the transaction of agency business; and

(b) They are preserved or are appropriate for preservation as evidence of agency organization and activities or because of the value of the information they contain.

(2) Record status. In addition to the two conditions stated above, use the following criteria as a guide for determining whether or not a document, such as an email message, meets the statutory definition of a record. If the material (whether a document, email, or other recorded information) meets any of the following criteria, it is considered a record and should be preserved using established procedures:

(a) It contains unique, valuable information developed in preparing position papers, reports, studies, etc.

(b) It reflects significant actions taken in the course of conducting Department of Homeland Security business.

(c) It conveys unique, valuable information about Department of Homeland Security programs, policies, decisions, or essential actions.

(d) It conveys statements of policy or the rationale for decisions or actions.

(e) It documents oral exchanges (in person or by telephone), during which policy is formulated or other Department of Homeland Security activities are planned or transacted.

(f) It adds to the proper understanding of the formulation or execution of Department of Homeland Security actions or of Department of Homeland Security operations and responsibilities.

(g) It documents important meetings.

(h) It facilitates action by Department of Homeland Security officials and their successors in office.

(i) It makes possible a proper scrutiny by the Congress or other duly authorized agencies of the Government.

(j) It protects the financial, legal, and other rights of the Government and of persons directly affected by the Government's actions.

(k) It documents the persons, places, things, or matters dealt with by the Department.

(l) It documents essential transactions of the Department of Homeland Security such as a scientific research and development case file or an inspection report documenting a shipment of goods to the U.S. from overseas.

(m) It documents the administration of the Department, such as personnel, procurement, payroll, budget, and other “housekeeping” operations (See the General Records Schedules for many types of administrative records created by the Department).

(3) Working files and similar materials.

Working files, such as preliminary drafts and rough notes, and other similar materials shall be considered Federal records if:

(a) They were circulated or made available to employees, other than the creator, for official purposes such as approval, comment, action, recommendation, follow-up, or to communicate with agency staff about agency business.

(b) They contain unique information, such as substantive annotations or comments that adds to a proper understanding of the agency's formulation and execution of basic policies, decisions, actions, or responsibilities.

(4) Record status of copies. A copy of a document, whether paper, electronic, email, or

otherwise, used in the business of a DHS office is a record for that office, even if another copy is maintained elsewhere in the DHS for other business purposes.

(5) Electronic mail messages. Messages created or received on electronic mail systems may meet the definition of record in 44 U.S.C. 3301. DHS policy and procedures on electronic mail records are contained in Chapter 2 of this guidance.

b. Identifying nonrecord materials. Nonrecord materials are Government-owned informational documents excluded from the definition of "records" or not meeting the requirements of that definition. (see 36 C.F.R. 1222.34(b)). Nonrecord material may be disposed of at any time after its purpose has been served. Nonrecord material will not be interfiled with temporary or permanent record material. The following are specifically excluded from status as records by statute (see 44 U.S.C. 3301):

(1) Library and museum material (but only if such material is made or acquired and preserved solely for reference or exhibition purposes);

(2) Extra copies of documents (but only if the sole reason such copies are preserved is for convenience of reference).

(3) Stocks of publications and of processed documents. (Each agency shall create and maintain serial or record sets of its publications and processed documents, as evidence of agency activities and for the information they contain, including annual reports, brochures, pamphlets, books, handbooks, posters and maps.)

c. Identifying personal papers.

(1) Personal papers are documentary materials of a private or nonpublic character that do not relate to, or have an effect upon, the conduct of agency business. Personal papers are excluded from the definition of Federal records and are not owned by the Government. Examples of personal papers include:

(a) Materials accumulated by an official before joining Government service that are not used subsequently in the transaction of Government business;

(b) Materials relating solely to an individual's private affairs, such as outside business pursuits, professional affiliations, or private political associations that do not relate to agency business.

(c) Diaries, journals, personal correspondence, or other personal notes that are not prepared or used for, or circulated or communicated in the course of, transacting Government business.

(2) If information about private matters and agency business appears in the same document, the document shall be copied at the time of receipt, with the personal information deleted, and treated as a Federal record.

(3) Materials labeled "personal," "confidential," or "private," or similarly designated, and used in the transaction of public business, are Federal records subject to the provisions of pertinent laws and regulations. The use of a label such as "persona" is not sufficient to determine the status of documentary materials in a Federal office.

(4) If personal papers are maintained in a DHS office, they shall be clearly designated as such and filed or otherwise maintained separately from the official records of the office.

(5) In determining whether personal papers may be created and/or maintained in a DHS office, among other things, DHS personnel must comply with the Department's policies on "Personal Use of Government Office Equipment," and "Use of Electronic Mail Systems."

(6) DHS personnel may not remove any Federal records from DHS custody while removing their personal papers and designated nonrecord materials. Before personnel depart from DHS, they shall consult with their designated Records Officer to ensure that official records that may be included in personal papers are returned to DHS files. The Records Officer or General Counsel may approve a request from departing personnel to take extra copies of work-related files if the records do not contain national security-classified information or are otherwise restricted (e.g., Privacy Act, FOIA).

d. Categories of Federal records

(1) Permanent records. Permanent records are those records that NARA appraises as having sufficient value to warrant continued preservation by the Federal Government as part of the National Archives of the United States because the records have continuing value as documentation of the organization and functions of DHS or because the records document the nation's history by containing significant information on persons, things, problems and conditions. DHS records determined by DHS and approved by NARA to be permanent must be available in a medium and format that conforms with the standards for permanent records. DHS permanent records will be transferred to the National Archives of the United States at the time designated on a NARA-approved Request for Records Disposition (SF 115). When permanent records are transferred to National Archives, legal custody of the records is transferred to NARA at this time. NARA takes measures needed to preserve the records and also provides reference service, including service to the creating agency.

(2) Temporary records. Temporary records are records that are designated for either immediate disposal or for disposal after a specified period of time or an event in accordance with a NARA-approved Request for Records Disposition (SF 115) or the General Records Schedule. Temporary records may document DHS business processes or document legal rights of the government or the public, document government accountability, or contain information of administrative or fiscal value. Depending on the type of record, the retention period may range from immediate destruction to as long as 100 years. Temporary records will be maintained and disposed of only in accordance with an approved records control schedule. Records classified as temporary should not be retained beyond their authorized retention period; nor will they be destroyed or otherwise disposed of prior to the end of their authorized retention period.

(3) Unscheduled Records. Records whose final disposition has not been approved by NARA. Unscheduled records are potentially permanent and must be treated as if they are permanent.

e. Additional requirements for certain types of records

(1) Audiovisual, cartographic, architectural, and micrographic records

(a) Audiovisual, cartographic and architectural records designated as permanent will be scheduled for transfer to National Archives as soon as they become inactive or whenever DHS cannot provide the proper care and handling of the materials to guarantee their preservation. Guidelines on special handling, storage and preservation problems can be found in 36 C.F.R. Part 1232

(b) Microform records. Microform records must meets the filming, storage and use standards in 36 C.F.R. part 1230.

(2) Vital records. These types of records are essential to the continued function or reconstruction of an organization during and after an emergency. Refer to the NARA publication entitled “Vital Records and Records Disaster Mitigation and Recovery” for guidance on handling these types of records. The emergency-preparedness needs of DHS will be met through the identification of vital records and pre-positioning copies of them at strategic locations for ready accessibility in the event of a national or local natural or technological disaster.

(3) Contractor Records. Records created or received and maintained for the Government by contractors.

(a) Contractors performing program functions are likely to create or receive records necessary to provide adequate and proper documentation of these programs and to manage them effectively. DHS contracts shall specify the delivery to the Government of all records including data needed for the adequate and proper documentation of contractor-operated programs in accordance with requirements of the Federal Acquisition Regulation (FAR)

(b) When contracts involve the creation of data for the Government's use, in addition to specifying a final product, DHS officials may need to specify the delivery of background data that may have reuse value to the Government. Before specifying the background data that contractors must deliver to the agency, program and contracting officials shall consult with DHS records and information managers and historians and, when appropriate, with other Government agencies to ensure that all agency and Government needs are met, especially when the data deliverables support a new agency mission or a new Government program.

(c) Deferred ordering and delivery-of-data clauses and rights-in-data clauses shall be included in contracts whenever necessary to ensure adequate and proper documentation or because the data have reuse value to the Government.

(d) When data deliverables include electronic records, DHS shall require the contractor to deliver sufficient technical documentation to permit DHS or other Government agencies to use the data.

(e) All data created for Government use and delivered to, or falling under the legal control of, the Government are Federal records and shall be managed in accordance with records management legislation as codified at 44 U.S.C. chapters 21, 29, 31, and 33, the Freedom of Information Act (5 U.S.C. 552), and the Privacy Act (5 U.S.C. 552a), and shall be scheduled for disposition in accordance with 36 C.F.R. part 1228.

CHAPTER 2: DEFINITIONS

1. **Disposal**. Removal of records from DHS control and authority by their physical destruction, sale as waste material, or other forms of savage or transfer; includes erasure of information captured or maintained on electronic media.
2. **Disposal Authority.** The legal authorization obtained only from the Archivist of the United States, NARA, for the disposal of records and recorded information.
3. **Disposition**. An interim or final placement of records and recorded information; the actions taken with regard to records and recorded information to maintain them in a proper place following their appraisal, including the actions of
   a. retaining;
   b. transferring to a records center;
   c. transferring to an archival agency; and
   d. destruction.
4. **Records.** All books, papers, maps, photographs, machine-readable materials, or other documentary materials, regardless of physical form or characteristics, made or received by an agency of the United States Government under Federal law or in connection with the transaction of public business and preserved or appropriate for preservation by that agency or its legitimate successor as evidence of the organization, functions, policies, decisions, procedures, operations, or other activities of the Government or because of the informational value of data in them.
5. **Records Series.** File units or documents arranged according to a filing system or kept together because they relate to a particular subject or function, result from the same activity, document a specific kind of transaction, take a particular physical form, or have some other relationship arising out of their creation, receipt, or use, such as restrictions on access and use.

CHAPTER 3: ELECTRONIC MAIL RECORDS

This section establishes Department of Homeland Security (DHS) policies for managing electronic mail.

1. **Summary.** This section establishes policies and responsibilities for managing the creation, maintenance, use, and disposition of electronic mail. In this section, electronic mail includes the message and all attachments. This section applies in addition to IMD, 4500, the Department's policy on "DHS E-Mail Usage."

2. **Authority.** The management of electronic mail complies with 44 U.S.C. Chapters 21, 29, 31, 33 and 33 and 18 U.S.C. Chapter 101, and regulations established by NARA for managing Federal records as stated in 36 C.F.R. parts 1220, 1222, 1228, and 1234. DHS manages electronic mail in accordance with 36 C.F.R. 1234.24. DHS uses the standards contained in 36 C.F.R. part 1234 to manage Federal electronic mail that is maintained in an electronic recordkeeping system.

3. **General Policy**

   a. All Government employees and contractors are required by law to make and preserve records containing adequate and proper documentation of the organization, functions, policies, decisions, procedures, and essential transactions of the agency. In addition, Federal regulations govern the life cycle of these records: they must be properly stored, preserved, and available for retrieval, and may be disposed of only in accordance with NARA-approved records control schedules.

   b. Employees are encouraged to use electronic mail because it is a cost-effective communications tool. This guidance assists DHS personnel with effectively managing electronic mail.

   c. DHS electronic mail systems are for official use only by authorized personnel. The information in these systems is Departmental, not personal. Utilization of electronic mail for other than official, authorized purposes is prohibited. No expectation of privacy or confidentiality applies.

   d. Users of DHS electronic mail systems will not alter or improperly dispose of any electronic mail message, record of transmission and receipt date, or attachment (such as a document) which meets the definition of a Federal record.

4. **Definitions**

   a. Electronic Mail (Message). A document created or received on an electronic mail system including brief notes, more formal or substantive narrative documents, and any attachments, such as word processing and other electronic documents, which may be transmitted with the message.

   b. Electronic Mail Record. A document created by or received via an electronic mail system which meets the definition of a Federal record as specified in 44 U.S.C. 3301.

c. Electronic Mail System. A computer application used to create, receive, and transmit messages and other documents. Excluded from this definition are file transfer utilities (software that transmits files between users but does not retain any transmission data), data systems used to collect and process data that have been organized into data files or data bases on either personal computers or mainframe computers, and electronically generated documents not transmitted on an electronic mail system.

d. Federal Record. All books, papers, maps, photographs, machine readable materials or other documentary materials, regardless of physical form or characteristics, made or received by an agency of the United States Government under Federal law or in connection with the transaction of public business and preserved or appropriate for preservation by that agency or its legitimate successor as evidence of the organization, functions, policies, decisions, procedures, operations, or other activities of the Government or because of the informational value of data in them. Library and museum material made or acquired and preserved solely for reference or exhibition purposes, extra copies of documents preserved only for convenience of reference, and stocks of publications and of processed documents are not included.

e. Transmission Data. Information in electronic mail systems regarding the identification of sender and addressee(s), and the date and time messages were sent.

f. Receipt Data. Information in electronic mail systems regarding date and time of receipt of a message, and/or acknowledgment of receipt or access by addressee(s).

g. Recordkeeping System. A manual or electronic system in which records are collected, organized, and categorized to facilitate their presentation, retrieval, use, and disposition.

5. Maintaining and preserving electronic mail.

a. Determine if electronic mail is a Federal record. The sender and the person who receives electronic mail independently determine whether or not the message and its attachments meet the definition of a Federal record for their office (See Chapter One, Section Four). The following are examples of electronic mail that constitute Federal records:

(1) Electronic mail that contains substantive information that is necessary to adequately and properly document the activities and functions of the DHS.

(2) Electronic mail that provides key substantive comments on a draft action memorandum if the electronic mail message adds to a proper understanding of the formulation or execution of DHS action.

(3) Electronic mail that provides documentation of significant DHS decisions and commitments reached orally (person-to-person, by telecommunications, or in conference).

(4) Electronic mail that conveys information of value on important DHS activities if the electronic mail message adds to a proper understanding of DHS operations and responsibilities.

(5) Electronic mail that documents the formulation and execution of basic policies and decisions.

(6) Electronic mail that documents important meetings.

(7) Electronic mail that denotes actions taken by DHS officials and their successors.

(8) Electronic mail that makes possible a proper scrutiny by the Congress or other duly authorized agencies of the Government.

(9) Electronic mail that protects the financial, legal, and other rights of DHS and of persons directly affected by the Department's actions.

b. Electronic mail that is a Federal record. Electronic mail determined to be Federal records falls into three categories: permanent records, temporary records, and transitory records.

(1) Permanent electronic mail are those messages that NARA appraises as having sufficient value to warrant continued preservation by the Federal Government as part of the National Archives of the United States. Electronic mail is scheduled as permanent by a NARA-approved Request for Records Disposition (SF 115) because the records have continuing value as documentation of the organization and functions of DHS or because the records document the nation's history by containing significant information on persons, things, problems and conditions. Electronic mail may be scheduled as permanent as part of a larger series or as the electronic mail of a designated agency official, such as, an Under Secretary.

(2) Temporary electronic mail are those messages that NARA approves for either immediate disposal or for disposal after a specified period of time or an event in accordance with a NARA-approved Request for Records Disposition (SF 115) or the General Records Schedule. Temporary records may document DHS business processes or document legal rights of the government or the public, document government accountability, or contain information of administrative or fiscal value. Depending on the type of record, the retention period may range from immediate destruction to as long as 100 years.

(3) Transitory electronic mail are those messages of short-term interest which have no documentary or evidential value and normally need not be kept more than 90 days. Examples of transitory electronic mail messages include:

(a) routine requests for information or publications and copies of replies which require no administrative action, no policy decision, and no special compilation or research for reply;

(b) originating office copies of letters of transmittal that do not add any information to that contained in the transmitted material, and receiving office copy if filed separately from transmitted material;

(c) quasi-official notices including memoranda and other records that do not serve as the basis of official actions, such as notices of holidays or charity and welfare fund appeals, bond campaigns, and similar records. (See General Records Schedule 23, item 7.)

(d) records documenting routine activities containing no substantive information, such as routine notifications of meetings, scheduling of work-related trips and visits, and other scheduling related activities (See GRS 23, item 5b).

c. Maintaining electronic mail.

(1) Electronic mail must be preserved for its appropriate retention period (which may be transitory), along with essential transmission and receipt data (names of sender and addressee(s) and date message was sent) for each electronic mail message in order for the context of the message to be understood. Disposition of all electronic mail records will be made in accordance with an authorized records disposition schedule.

(2) Permanent and temporary electronic mail are maintained and made available for office use by:

(a) Printing the email message (with attachment) and filing, when paper files are used as the recordkeeping system. The printed copy of the electronic mail must be filed in the manual recordkeeping system.

(b) Filing the email electronically, when an electronic recordkeeping system is used as the recordkeeping system. (See 36 C.F.R. 1234.24 (a)-(d)). Note that organizations that choose to manage electronic mail records electronically must either: (1) be able to perform all requirements of preservation, protection, storage, retrieval, and disposition through the electronic mail application system itself, or (2) copy electronic mail records into an electronic recordkeeping system able to perform all the functional requirements of the Federal regulations. "Backups" made as a normal part of electronic mail systems operation and maintenance do not meet these requirements and should not serve as an electronic recordkeeping system.

(3) Transitory electronic mail may be maintained in the "live" email system. These emails with attachments will be deleted after 90 days by the automated delete feature of the email system.

6. Retention and Disposition of electronic mail records

a. When electronic mail is retained as a Federal record, the retention period is governed by the appropriate NARA-approved DHS records control schedule or the General Records Schedule. Temporary records are kept for defined periods of time pending destruction and permanent records are transferred to the National Archives of the United States for permanent preservation.

b. Electronic mail users who are uncertain about the disposition of electronic mail messages should contact their program office Records Officer or the DHS Records Officer for assistance.

c. If an electronic mail item, either sent or received, is a Federal record, it is the responsibility of the DHS employee to ensure that a copy is preserved by making it a part of the official files of DHS, unless it is a transitory record.

d. Besides the text of electronic mail messages, electronic mail systems may provide records transmission and receipt data. Transmission data (such as the identity of the sender and addressee(s) and the date on which the message was sent) must be preserved with all electronic mail items defined as Federal records. Just as with a paper record, this transmission data is necessary for an electronic mail record to be complete and understandable.

e. Electronic mail systems may also provide users with the ability to request acknowledgments or receipts showing that an electronic mail message reached the mailbox or inbox of addressee(s) and was accessed. Electronic mail users should request receipt data when it is needed for adequate and proper documentation of DHS activities, especially when it is necessary to confirm that an electronic mail message was received and accessed. In such instances, receipt data associated with the record copy of the electronic mail message will be preserved.

f. When the recordkeeping copy is maintained in paper, the printed electronic mail message with attachments will be annotated to document that it is the official file copy before being placed in the official files of the responsible organization.

7. **Electronic mail received from external sources.** These procedures also apply to electronic mail received from non-DHS and other outside sources, e.g., through the Internet or other commercial network services.

8. **Compliance Reviews**. Compliance with these procedures will be accomplished through periodic reviews and evaluations to be conducted under the supervision of the DHS Records Officer.

CHAPTER 4: ELECTRONIC RECORDS MANAGEMENT

1. **DHS shall ensure** that the management of electronic records incorporates the following elements:

   a. Integrating the management of electronic records with other DHS records management programs.

   b. Establishing procedures for addressing records management requirements, including recordkeeping requirements and disposition, before approving new electronic information systems or enhancements to existing systems.

   c. Developing and maintaining up-to-date documentation about all electronic information systems that is adequate to: Specify all technical characteristics necessary for reading or processing the records; identify all defined inputs and outputs of the system; define the contents of the files and records; determine restrictions on access and use; understand the purpose(s) and function(s) of the system; describe update cycles or conditions and rules for adding information to the system, changing information in it, or deleting information; and ensure the timely, authorized disposition of the records.

   d. Specifying the location, manner, and media in which electronic records will be maintained to meet operational and archival requirements.

   e. Specifying the methods of implementing controls over national security-classified, sensitive, proprietary, and Privacy Act records stored and used electronically.

   f. Ensuring compliance with applicable Government wide policies, procedures, and standards such as those issued by the Office of Management and Budget, the General Accounting Office, the General Services Administration, the National Archives and Records Administration, and the National Institute of Standards and Technology.

2. **Selection and maintenance of electronic records storage media.**

   a. DHS shall select appropriate media and systems for storing agency records throughout their life (authorized retention period) which meet the following requirements:

      (1) Permit easy retrieval in a timely fashion;

      (2) Facilitate distinction between permanent and temporary records;

      (3) Retain the records in a usable format until their authorized disposition date; and

      (4) Ensure that the format of permanent records and their media at the time of transfer to the National Archives meets NARA requirements in 36 C.F.R. 1228.270.

   b. The following factors shall 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 records density;

(5) The access time to retrieve stored records; and

(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).

c. DHS will 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, agencies must determine that the authorized disposition of the electronic records can be implemented after conversion.

d. DHS will back up electronic records on a regular basis to safeguard against the loss of information due to equipment malfunctions or human error. Duplicate copies of permanent or unscheduled records shall be maintained in storage areas separate from the location of the records that have been copied.

e. Temporary records whose retention standard has been approved by NARA may be stored on any medium, including optical disks, that ensures maintenance of the information until expiration of the authorized retention period. This means that conversion of such temporary records to optical disks and disposal of the original paper records or other media, do not require NARA’s approval.

CHAPTER 5: FEDERAL RECORDS MANAGEMENT ROLES AND RESPONSIBILITIES

1. DHS responsibilities

a. Secretary of the Department of Homeland Security will:

(1) Establish and maintain an active, continuing program for the economical and management of the records of DHS (44 U.S.C. 3101).

b. The Under Secretary for Management will:

(1) Establish policies and procedures for administering the RM program.

(2) Issue changes to this directive that are necessary to implement and manage the RM program.

(3) Establish, coordinate, and maintain a DHS-wide RM program to ensure that all records are received, created, maintained, protected, released, and disposed of as required by the laws and regulations.

(4) Designate an individual(s) to serve as DHS Records Officer.

(5) Ensure that in planning for manual or automated information systems, the life cycle of the records is considered and the records associated are properly scheduled. DHS will include the life cycle of the records when planning for manual or automated information systems. DHS will incorporate records management and archival functions into the design, development, and implementation of information systems (See OMB Circular A-130).

(6) Establish appropriate procedures to ensure that all DHS contracts that result in the creation and maintenance of records to accomplish a Department function include appropriate language to ensure that records created or received and maintained for DHS by contractors are maintained in accordance with NARA regulations (36 C.F.R. 1222.48 and 1234.10(k)).

c. Under Secretaries, Assistant Secretaries, and Other Key Officials will:

(1) Establish, coordinate, and maintain a directorate or organization RM program.

(2) Designate an official(s) and an alternate(s) to serve as Program Records Manager and establish the Records Coordinator position within each program office.

(3) Designate a facility Records Manager in each DHS field facility. These individuals are responsible for assisting the facility Director in ensuring that their facility is in compliance with the provisions of this directive.

d. Program Officials. Program officials have the primary responsibility for creating, maintaining, protecting, and disposing of records of their program area. They will:

(1) Create those records needed to ensure adequate and proper documentation of their area of responsibility:

(2) Appoint a Records Coordinator responsible for records management for the program;

(3) Ensure that adequate recordkeeping requirements are established and implemented for new or revised programs, processes, systems, and procedures;

(4) Implement procedures to protect records from theft, loss, and unauthorized access; and

(5) Ensure that in planning for manual or automated information systems, the life cycle of the records is considered and the records associated are properly scheduled. DHS will include the life cycle of the records when planning for manual or automated information systems. DHS will incorporate records management and archival functions into the design, development, and implementation of information systems (See OMB Circular A-130).

e. DHS Records Officer will:

(1) Lead and manage the DHS records management program.

(2) Establish policy and procedures for administering the records management program.

(3) Issue changes to this guidance that are necessary to implement and manage the program.

(4) Provide technical advice and training, as appropriate, to DHS offices on establishing and maintaining effective records management programs.

(5) Conduct periodic reviews and evaluation of records management programs.

(6) Serve as DHS liaison with NARA and other Government agencies on records management matters.

(7) Periodically conduct DHS-wide reviews of the RM program to ensure that policies and procedures are effectively carried out (44 U.S.C. 3506; 36 C.F.R. 1220.54).

(8) Serve as authorized agency approving official for the SF-115, Request for Records Disposition Authority, and SF-258, Agreement to Transfer Records to the National Archives of the United States.

(9) Develop and implement an agency wide program for the management of all records created, received, maintained, used, or stored on electronic media.

(10) Inventory and schedule records created and maintained by DHS. Provide leadership, guidance, and oversight of inventorying and scheduling activities in program offices.

(11) Develop records management oversight roles and communication networks with all program offices and field facilities to ensure that the records management program is carried out in accordance with DHS policy and procedures.

(12) Developing and disseminating procedures, as needed, to supplement DHS-wide procedures to meet the records management needs of their program offices and to support a records management program within their respective organizations.

f. Records Managers will:

(1) Establish procedures in their area of responsibility to implement the provisions of this directive, NARA regulations, DHS regulations, and related directives.

(2) Ensure that the standards and procedures contained in the NARA regulations are used to manage all electronic records created.

(3) Ensure that all employees are aware of the provisions of this directive and its related handbooks, DHS regulations, and laws governing the creation, receipt, maintenance, and disposition of records.

(4) Identify recordkeeping requirements for programmatic and administrative information systems and record series in all media.

(5) Developing standardized file plans and indexing approaches where appropriate to simplify the use of, access to, and integration of information within the organization.

(6) Inventory and draft records control schedules for records created and maintained in the organization.

(7) Implement approved records dispositions, while ensuring that no records are destroyed without proper authorization as specified in the Federal Records Act.

(8) Systematically review records control schedules, file plans and procedures to ensure that they are current and update them as necessary.

(9) Conduct a program of regular internal records management reviews to assist offices within the organization in implementing appropriate records management procedures.

(10) Assist in the planning and implementing of automated or manual information systems to assure that the systems meet records management and archival requirements.

(11) Implement a vital records program in accordance with the DHS-wide program.

(12) Apprise organizational managers on matters relating to records management activities.

(13) Ensure that adequate recordkeeping requirements are established and implemented for new or revised programs, processes, systems, and procedures.

(14) Designate and maintain a current descriptive list of all official files stations and the name of the responsible official.

(15) Conduct an annual review of all official file stations to ensure adequate and proper documentation is maintained, permanent records are preserved, and other records are disposed of in accordance with applicable schedules. Report to the Department Records Officer on the results of this review.

g. Program Records Coordinators will:

(1) Schedule records created and maintained for their respective organization.

(2) Implement approved records dispositions, while ensuring that no records are destroyed without proper authorization as specified in the Federal Records Act.

(3) Review records control schedules, file plans and procedures to ensure that they are current and updating them as necessary.

(4) Review filing systems and implement procedures to ensure that records are maintained in such a manner that information and documents are readily retrievable.

(5) Transfer or destroy inactive records according to the appropriate schedule.

(6) Cooperate with the Department and Program Records Manager in and the management of records.

(7) Notify the Program Records Manager of organization or program changes that will result in the establishment of new types of records, the transfer or termination of records no longer required, or an increase or decrease in the retention time of the records.

h. Records Liaison Officer

(1) Implement approved records dispositions, while ensuring that no records are destroyed without proper authorization as specified in the Federal Records Act.

(2) Develop file plans to include all records, in any media.

(3) Review records control schedules, file plans and procedures to ensure that they are current and updating them as necessary.

(4) Establish a filing system and implement procedures to ensure that records are maintained in such a manner that information and documents are readily retrievable.

(5) Cut off subject correspondence files on an annual basis and close out case files promptly on the completion of the case.

(6) Transfer or destroy inactive records according to the appropriate schedule.

(7) Report unscheduled records or changes in recordkeeping to the Program Records Coordinator.

i. The Inspector General (IG) will include an analysis of a program's use and implementation of this directive and NARA's regulations in all program audits.

j. The General Counsel (GC) will:

(1) Provide legal advice and assistance to ensure that DHS fully complies with the provisions of the 44 U.S.C. chapters 21, 31 and 33 and 36 C.F.R. parts 1220-1238 relating to records management.

(2) Recommend changes in policies and procedures relating to the RM program.

2. DHS interaction with agencies with Government-wide Records Management responsibilities.

a. National Archives and Records Administration (NARA). NARA is the oversight agency responsible for all Federal records, approving disposition authorities, providing program assistance, evaluating agency records management programs, and serving as the final custodian of permanent records.

b. Office of Budget and Management (OMB). OMB is responsible for:

(1) Developing and implementing uniform and consistent management policies.

(2) Overseeing the development and promotion of the use of management principles, standards and guidelines.

(3) Evaluating agency management practices to determine their adequacy and efficiency.

(4) Determining compliance of such practices with policy, principles, standards, and guidelines that they issue.

c. Government Accountability Office (GAO). GAO issues the GAO Policy and Procedures Manual, Title 8, Records Management, which pertains to accounting and fiscal records. GAO must be included in the approval of records retention schedules and disposal actions for accountable officer's accounts and records relating to claims or demands by or against the Government. GAO also conducts audits and performs evaluations of agency programs.

CHAPTER 6: FILES MANAGEMENT

1. The records created and received by DHS must be maintained in a manner that allows their ready retrieval whenever necessary throughout the approved life cycle of the information. The records maintenance process must include the application of authorized disposal requirements, including the identification and retention of records of permanent value. This is accomplished through the establishment and implementation of files management standards and procedures. Files management includes the following:

b. Establishing procedures for classifying, indexing, labeling, and filing the records to ensure their ready access and retrievability for the conduct of DHS business;

c. Establishing and documenting official file locations to the extent that the maintenance of official files in unofficial locations is not permitted; and

d. Establishing procedures for retrieval, charge-out, and refiling records.

e. Filing personal papers and nonrecord materials separately from official DHS records.

CHAPTER 7: RECORDS DISPOSITION PROGRAM

1. Goals of the Program

An effective records disposition program is essential to successful records management and is an integral part of DHS records management program. The goals of the records disposition program are to:

a. Maintain adequate and proper documentation and evidence of DHS activities for the time required to meet programmatic needs.

b. Retire records requiring longer retention to economical storage facilities, providing savings in space and equipment.

c. Provide timely disposal of records no longer needed for current DHS business.

d. Preserve records of continuing or enduring value through transfer to the National Archives.

2. Records Disposition Authority

The following are the two basic types of records disposition authorities for DHS records:

a. NARA General Records Schedule (GRS). Disposition requirements for administrative or housekeeping records that are common to most Federal agencies are listed in the GRS published by NARA. The disposition requirements of the GRS, including records retention periods, are mandatory DHS-wide unless an exception is obtained from NARA. The GRS does not cover all DHS records.

b. DHS Records Control Schedules. The GRS must be supplemented by DHS-specific schedules covering records that are unique to program administrations and staff offices. NARA-approved disposition requirements authorized for records maintained by DHS are listed in comprehensive records control schedules that are developed and published by Departmental Records Officer. The records series or systems contained in these records schedules are unique to their organization. Disposition instructions and retention periods cited in these schedules are mandatory.

3. Review of Records

b. All records maintained by DHS will be reviewed annually by the office holding them, and action will be taken to:

(1) Remove less-active records to local storage;

(2) Transfer inactive records to an approved records offsite storage facility;

(3) Transfer permanent records to the National Archives; and

(4) Destroy and document the destruction of records which have reached the term of their authorized retention period.

c. Records Coordinators will review their records control schedules annually to ensure they are kept current, accurately reflect program office needs, and meet all statutory requirements. As a result of each review, Records Coordinators will submit changes through the DHS Records Officer for submission to NARA for approval.

d. Any unlawful or accidental destruction, defacing, alteration or removal of DHS records must be reported promptly to the Records Officer. Field facilities will submit reports to their respective Records Coordinators. The penalty for the willful and unlawful destruction, damage, or alienation of Federal records is a fine under the provisions of Title 18, U.S.C., or 3 years in prison, or both (18 U.S.C. 2071).

CHAPTER 8: COMPLIANCE REVIEWS

Compliance with these procedures will be accomplished through periodic reviews and evaluations to be conducted under the Office of Information Resources Management's Review Program as required by Federal regulations.

CHAPTER 9: REMOVAL OF RECORDS BY EMPLOYEES AND POLITICAL APPOINTEES

1. **General.** All employees shall clearly designate as personal, and maintain separately from the records of the office, those papers of a private or nonofficial nature that pertain to their personal affairs. If information about private matters and Department business appears in the same document, the document should be copied at the time of receipt, with the personal information deleted. If the private or nonofficial papers of a Department of Homeland Security (DHS) official are kept in the official's office, they shall be filed separately from the official records of the office. For electronic information it means saving the private information in a separate file without the Federal documentation; and for the paper information it means placing the information in a separate folder.

2. **Responsibilities.** The DHS Records Officers shall:

   a. ensure that nonrecord material being removed by a departing employee or official is examined by the DHS reviewing official for the purpose of providing the appropriate protection for information that is restricted from release under the Privacy Act or other statutes, regulations or executive orders;

   b. obtain signed removal forms as follows: (1) all Presidential appointees with Senate confirmation must complete form DHS 0550-1, "Removal of Documentary Materials by Presidential Appointees with Senate (PAS) Confirmation," and (2) all other employees must complete a signed form DHS 0550-2, "Documentary Materials Removal/Non-removal Certification";

   c. ensure that the signed forms, and related documentation are retained in a centralized file for at least 10 years within the Personnel or Records Management office; and

   d. ensure that no departing official or employee shall remove records or nonrecord materials relating to any pending or contemplated civil, criminal, or administrative proceeding or other program activity when the information, if released, would impair or prejudice the outcome of the proceeding or Government policy determinations, decisions, or other actions. This includes any properly classified national security information.

3. **Procedures for Removal of Papers.**

   a. All records, original and copies, are under the control of DHS, regardless of how and by whom they were created or obtained. Removal of documentary material must be approved in accordance with the provisions of DHS MD 0550.2 (or subsequent versions) to ensure that DHS ability to claim privileges in litigation, to claim FOIA exemptions and to protect sensitive and classified information is not weakened.

   b. No documentary material, even though judged to be nonrecord material, shall be withdrawn if this will create such a gap in the files as to impair the completeness of essential documentation. Indexes, or other finding aids, necessary for the use of the official files may not be removed.

c. Personal diaries, which are really private records of public activities, are private property and may be removed. When the matters dealt with in such work aids as office diaries, logs, memoranda of conferences and telephone calls are covered elsewhere by adequate records, such work aids may be removed provided they do not contain information otherwise prohibited from removal. This applies to personal papers created and/or maintained on paper as well as in electronic format.

d. Extra copies (photocopies, etc.) of records may be removed under certain circumstances. Prior to removal, it must be determined that no legal or policy reason exists that would prevent removal and that the record copy, or other necessary copies, are available in the Department. If the copy is of a document originating with another agency, the requirements of the originating agency must be determined.

e. Notwithstanding paragraphs 3.a. through 3.c. of the handbook, properly classified national security information and sensitive but unclassified (SBU) information may not be removed from U.S. Government control under any circumstances. Such information shall remain classified, controlled or restricted as long as required for national security and/or DHS interests. Subsequent access to such information by former Presidential Appointees and/or historical researchers shall be in accordance with DHS MD 11045, "Protection of Classified National Security Information/Accountability, Control, and Storage," Sections 6.C.3.f. and g.

f. Any violation of the statutory and regulatory limitations placed on removal of documentary material by DHS officials who resign or retire will be forwarded to the DHS Office of Security, who shall confer with the Inspector General regarding such violations.

g. Records will not be disposed of while they are the subject of a pending request, appeal, subpoena, or lawsuit under the Freedom of Information Act or the Privacy Act, as provided for in GRS 14.

4. Review of Papers.

a. The DHS Records Officer should be consulted prior to removing personal papers and the Records Officer will, in turn, consult with NARA if questions arise. The Office of Presidential Libraries is interested in the private papers of high level officials because these papers are an invaluable adjunct to the public records of an Administration. A retiring official may place restrictions on access to papers as deemed necessary if the official decides to make use of these archival depositaries.

b. E.O. 12958, as amended, provides for the declassification of properly classified national security information when the information no longer meets the standards and criteria for continued classification and such declassification is accomplished by an official authorized to do so. Departing officials shall not use the declassification process as a means for allowing the removal of information that would otherwise be prohibited from removal. Declassification actions taken in association with departing senior officials shall be reviewed by appropriate officials having program specific knowledge of the information in coordination with the DHS Office of Security.

DEPARTMENT OF HOMELAND SECURITY

CERTIFICATION FORM

Removal of Document Materials by Presidential Appointees with Senate Confirmation

1. **Documentary Materials that May be Removed: Personal Papers.**

Examples of personal papers include: papers accumulated by an official before joining Government service that are not used subsequently in the transaction of Government business; materials relating solely to an individual's private affairs, such as outside business pursuits, professional affiliations, or private political associations that do not relate to agency business; diaries, journals, personal correspondence, or other personal notes that are not prepared or used for, or circulated or communicated in the course of transacting Government business (36 C.F.R., Section 1222.36(a), (b), and (c)).

2. **Records that May Not be Removed.**

National security information and officially limited information may not be removed from DHS under any circumstances. Such information shall remain classified, controlled or restricted as long as required for national security and/or DHS interests.

3. **Penalties for Unlawful Removal of Records.**

Criminal penalties are provided for the unlawful removal or destruction of Federal records (18 U.S.C. 2071) and for the unlawful disclosure of certain information pertaining to national security (18 U.S.C. 641, 793, 794, 798 and 952).

I certify that I understand the foregoing information and that the documents (paper or electronic media) that I am removing from DHS have been reviewed and approved for removal in accordance with DHS MD 0550 Publication/Handbook.

Name of Departing Official Date	Signature of Departing Official
Name and Title of Reviewing Official Date	Signature of Reviewing Official

DHS Form 550-1 (10/04)

DEPARTMENT OF HOMELAND SECURITY

Documentary Materials Removal/Nonremoval Certification

1. NAME	2. SOCIAL SECURITY NUMBER
3. OFFICE	

4. Are you removing any nonrecord documents (paper or electronic media) from the Department of Homeland Security?

☐ YES Go to 5a.

☐ NO Go to 7a.

5a. I certify that the documents that I am removing from the Department of Homeland Security have been reviewed and approved for removal. They do not include any documents relating to any pending or contemplated civil, criminal, or administrative proceeding or other program information, if released, would impair or prejudice the outcome of the proceeding or Government policy determinations, decisions, or other actions (Examples: classified documents; record copies; documents, even though judged to be nonrecords, that will create a gap in the files; and indexes and finding aids necessary to use of the official files).

5b. SIGNATURE	5c. DATE
6a. TITLE OF REVIEWING OFFICIAL	
6b. SIGNATURE OF REVIEWING OFFICIAL	6c. DATE

7a. By my signature in block number 7b., I certify that I an not removing any documents from the Department of Homeland Security.

7b. SIGNATURE OF EMPLOYEE	7c. DATE

DHS Form 550-2 (10/04)